КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.32.1150
УДК 004.056.55: 003.26

Грищук Ольга Михайлівна
доктор філософії, підполковник
Слухачка Національного університету оборони України
Національний університет оборони України, Київ, Україна
ORCID: 0000-0001-6957-4748
Hry.Olga@gmail.com

Грищук Руслан Валентинович
Лауреат Національної премії України імені Бориса Патона,
Заслужений діяч науки і техніки України,
доктор технічних наук, професор полковник
Заступник начальника Військової академії (м. Одеса)
Військова академія (м. Одеса), Одеса, Україна
ORCID: 0000-0001-9985-8477
Prof.Hry@gmail.com

ОЦІНЮВАННЯ ЗАХИЩЕНОСТІ БЛОКЧЕЙН-ВУЗЛА ВІД ЕКЛІПС-АТАКИ ТА ТРОЯНСЬКОГО ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА ОСНОВІ ДИФЕРЕНЦІАЛЬНО-ІГРОВИХ МОДЕЛЕЙ

Анотація. Технологія блокчейн як новітня проривна інформаційна технологія суттєво вплинула на розвиток банківського сегменту, трансформувавши класичні підходи до здійснення операцій з грошовими активами, де банк виступав обов'язковим посередником фінансових транзакцій. На сьогодні технологія блокчейн утвердилася як базис цифрової економіки. Вона також вже знайшла практичне застосування в оборонній та соціальній сферах. Висока ринкова вартість блокчейн-активів – різноманітних токенів та криптовалют, – останнім часом почала привертати значний інтерес як з боку урядових (як правило підсанкційних держав), так і неурядових кіберугруповань, а також окремих хакерів, які прагнуть незаконного збагачення. З цією метою ними реалізовуються різноманітні кібератаки як на окремі блокчейн-вузли, так і цілі блокчейн-мережі. Також непоодинокими є спроби інфікування блокчейну за допомогою шкідливого програмного забезпечення. Зважаючи на зазначене, у даній статті як об'єкт дослідження обрано процес оцінювання захищеності блокчейн-вузла від Екліпс-атак та троянського шкідливого програмного забезпечення. Предметом дослідження є диференціально-ігрові моделі оцінювання захищеності блокчейн-вузла, які побудовано на основі ланцюгів Маркова. Така інтерпретація дала змогу формалізувати ймовірності станів блокчейн-вузла під впливом Екліпс-атаки та троянського шкідливого програмного забезпечення у вигляді систем диференціальних рівнянь Колмогорова-Чепмена. Для отримання оцінок рівня захищеності в аналітичному та числовому виглядах в статті було використано відомий диференціально-ігровий підхід на основі нетейлорівських диференціальних перетворень академіка Г. Пухова. Наукова новизна одержаних у статті результатів полягає в подальшому розвитку механізмів забезпечення кібербезпеки технології блокчейн за рахунок вибору оптимальних стратегій кіберзахисту блокчейн-вузлів, які підпали під вплив Екліпс-атаки або троянського шкідливого програмного забезпечення. Одержані оцінки захищеності блокчейн-вузла є науковим підґрунтям для вироблення практичних рекомендацій щодо захисту технології блокчейн і від інших не менш небезпечних типів кібератак та видів шкідливого програмного забезпечення.

Ключові слова: блокчейн-вузол; рівень захищеності; Екліпс-атака; троянське шкідливе програмне забезпечення; модель; кібербезпека; диференціальна гра; диференціальні перетворення.

ВСТУП

Теологія блокчейн в апріорі вважається захищеною [1]. Саме ця аксіома становить її сутність та зміст. Разом із тим, висока ринкова капіталізація [2] токенів та криптовалют, створених на основі технології блокчейн, є одним з головних чинників, які розширюють коло бажаючих заволодіти ними і перш за все в незаконний спосіб [3]. Тому номенклатура застосовуваних для цього технологічних інструментів суттєво відрізняється. Це обумовлено рядом обставин. З одного боку, об'єктом впливу може виступати блокчейн-вузол і блокчейн-мережа, з іншого – загрозу кібербезпеці блокчейн-вузла, або блокчейн-мережі може становити або один з типів кібератак, або один з видів шкідливого програмного забезпечення (ШПЗ).

Кібератаки різняться між собою методами, об'єктами та цілями впливу [4]. Найбільш відомими кібератаками на блокчейн-мережі є атака маршрутизації [5] та атака-51% [6]. На рівні блокчейн-вузла такими кібератаками є атака Сівілли [7], атака відмови від обслуговування [8], атака підміни часових міток [9], Екліпс-атака [10] та ін. З наведених кібератак Екліпс-атака для окремих блокчейн-вузлів становить найбільшу небезпеку [11]. З поміж усього спектру ШПЗ такого як віруси, хробаки та трояни, практичний інтерес становить останнє [11], особливо для банківських застосунків [12]. Це обумовлено тим, що троянське ШПЗ є найбільш поширеним серед названих вище видів [13], а тому залишається в тренді головних кіберзагроз банківському сегменту [14], [15]. Також сімейство троянського ШПЗ достатньо гнучке до оновлень як самих мобільних операційних систем, так і їх безпекових механізмів [16]. Наприклад, особливо небезпечними на сьогодні є найновітніші зразки троянського ШПЗ, а саме Vultur, DroidBot, Errorfather, BlankBot [17], а також Android Trojan Crocodilus [18]. Не зважаючи на їх різноманіття всіх їх між собою пов'язують спільні поведінкові ознаки [19]. Саме ця особливість у перспективі відкриває можливість розроблення проактивних механізмів забезпечення кіберзахисту блокчейн-вузлів. Таким чином, всебічне дослідження блокчейн-вузлів на їх захищеність від Екліс-атак та троянського ШПЗ на основі математичних моделей, може стати дієвим інструментом на шляху вироблення дієвих механізмів їх кіберзахисту.

Постановка проблеми. У цій роботі на основі диференціально-ігрового підходу [20] оцінюється захищеність блокчейн-вузла від Екліпс-атаки та троянського ШПЗ.
Об'єкт дослідження – процес оцінювання захищеності блокчейн-вузла від Екліпс-атак та троянського ШПЗ.

Предметом дослідження є диференціально-ігрові моделі оцінювання захищеності блокчейн-вузла під впливом Екліпс-атаки та троянського ШПЗ.

Аналіз останніх досліджень і публікацій. З [21] відомо, що математичний базис диференціально-ігрових моделей становить теорія ігор [22], яка Сатоші Накамото вперше використана для вирішення проблеми візантійських генералів під час знаходження механізму консенсусу "доказу роботи" (Proof of Work) [23]. Аналіз останніх наукових досліджень за темою статті показав, що за останні роки в світі відмічається сплеск наукових досліджень, присвячених вивченню безпекових властивостей технології блокчейн на основі теорії ігор в цілому [24] та диференціальних ігор зокрема. Тому серед усіх відомих робіт до критичного огляду включено лише ті, які є предметом даного дослідження.

Диференціальні ігри в технології блокчейн вперше використано для моделювання, імітації та проєктування мережевих токенів [25]. Запропонована в [25] диференціально-ігрова модель в умовах невизначеності стратегій кіберзахисту та

кібернападу дозволяє максимізувати гравцям власні функції плати. Дана ідея набула подальшого розвитку у відомій праці [26]. У публікації [27] для дослідження стратегій поведінки гравців в умовах невизначеності під час кібератаки в блокчейн-мережах використано математичний апарат диференціальних ігор зі стохастичною динамікою. В основу розрахунку виграшу та програшу гравців кіберзахисту та гравців кібернападу в [27] покладено відомий алгоритм Рунге-Кутта. У результаті на основі рівноваги Неша запропонована в [27] диференціально-ігрова модель дозволяє знаходити числові оцінки виграшу та програшу кожного з гравців під час кібератаки, яка моделюється. Разом із тим дані оцінки втрачають свою достовірність у разі відхилення гравцями від оптимальних стратегій, що є недоліком даного підходу.

Вперше Екліпс-атаку на блокчейн-вузол на основі методів теорії диференціальних ігор змодельовано в [28], а в серії фундаментальних робіт [29], [30], [31] та [32] для цього закладено відповідне математичне підґрунтя. У формалізованому вигляді ймовірнісні стани надійності блокчейн-вузла в [29] описано математичною моделлю, що являє собою систему диференціальних рівнянь. Кількість рівнянь в такій системі є рівною кількості станів блокчейн-вузла під час Екліпс-атаки в одноранговій мережі, що являє собою ланцюг Маркова. В [29], [30], [31] та [32] також показано, що залежно від обраних гравцями стратегій кіберзахисту або кібернападу на блокчейн-вузол значення цільової функції яка є показником стану безпеки системи в реальному часі варіює. Виходячи з одержаних в цих роботах результатів можна констатувати – основною перевагою застосування диференціальних ігор при дослідженні технології блокчейн є можливість прогнозування майбутнього стану їх безпеки. Оцінений стан безпеки технології блокчейн під впливом кібератак в кінцевому рахунку впливатиме на рівень капіталізації криптовалют. Однак ні в згаданих наукових працях, ні в інших відомих публікаціях не розроблені паттерни Екліпс-атаки на блокчейн-вузол в аналітичному вигляді, придатні для оцінювання їх захищеності.

Однією з перших оглядових робіт, присвячених моделюванню ШПЗ є стаття [33]. При цьому більшість з розглянутих у [33] моделей таких як SIR, SEIR, SEIRS та ін., мають епідеміологічну природу та описуються системами диференціальних рівнянь. Але для їх розв’язання у такій постановці, як відомо на сьогодні, методи теорії диференціальних ігор не застосовувалися. Інколи, як також показано в [33], для моделювання ШПЗ, у т.ч. й троянського, використовуються методи теорії клітинних автоматів. Абстрактна природа таких моделей ставить під сумнів достовірність оцінок рівня захищеності об’єктів захисту, що моделюються. У монографії [34] теоретичний базис моделювання ШПЗ становлять такі методи як методи теорії масового обслуговування, варіаційного числення та теоретико-ігрові методи. Згаданий математичний інструментарій також накладається на класичні епідеміологічні моделі, про що згадувалося вище. Одержані оцінки захищеності на основі запропонованих в [34] моделей дозволили авторам запропонувати ряд ефективних стратегій кіберзахисту технології блокчейн від ШПЗ. Зокрема до таких стратегій в [34] автори віднесли стратегію своєчасного встановлення патчів, коректного налаштування фаєрволів, стратегію ізоляції інфікованих хостів тощо. Попри наявність у [34] прикладних сценаріїв, більшість представлених результатів мають переважно абстрактний характер, адже при появі нових зразків троянського ШПЗ запропоновані в [34] моделі потребуватимуть постійного оновлення й верифікації. У дисертації [35], опираючись на властивості Марківських процесів з неперервним часом та напівмарківських процесів, дисертантом досліджено лише поширення троянського ШПЗ у банківських додатках без надання відповідних оцінок їх захищеності. Кількісні оцінки одержані в [35]

стосуються лише ймовірнісних характеристик успішності досягнення цілей троянським ШПЗ, а також оцінок ризиків для безпеки, залежно від його складності та інтенсивності поширення. Слід зазначити, що всі рішення для ймовірностей в [35] одержано з використанням перетворень Лапласа. Тому моделі розроблені в [35] не дозволяють знаходити оптимальні стратегії кіберзахисту банківських додатків, зокрема й блокчейн-вузлів та оцінювати їх захищеність.

У [36] запропоновано моделювати динаміку поширення ШПЗ у кіберпросторі на основі баєсівських структурних часових рядів, які верифіковані на класичних епідеміологічних моделях SIS та SIR, а також на двох реальних зразках троянського ШПЗ, а саме Conficker Worm та Code Red Worm. Перевагою такого підходу є можливість одержання ймовірнісних оцінок захищеності без попередніх знань про задіяні безпекові механізми, але за умови відомих апріорних даних про вид троянського ШПЗ. Неврахування топології блокчейн-мережі, яка складається з окремих блокчейн-вузлів у [36], є недоліком такого підходу, адже не дозволяє одержувати достовірні оцінки захищеності окремого блокчейн-вузла у разі появи нових зразків троянського ШПЗ. Аналогічні недоліки притаманні і працям [37] та [38]. Відмінністю [37] та [38] від [36] є лише математичний базис. Наприклад, у [37] в якості такого базису обрано математичний апарат булевої алгебри.

Останні наукові розробки, наприклад [39], ґрунтуються на методології машинного навчання. При цьому підходи, які покладаються в основу моделей оцінювання захищеності в [39] залишилися застарілими. Вони ґрунтуються на звичайних диференціальних рівняннях (ODEs), універсальних диференціальних рівняннях (UDEs) та нейронних звичайних диференціальних рівняннях (Neural ODEs). На практиці це дозволяє отримувати лише оцінки захищеності для відомих видів троянського ШПЗ, не враховуючи ефект “нульового дня”. Інші відомі сучасні наукові публікації та темою статті як правило ґрунтуються на комплексуванні описаних вище підходів. Наприклад, у [40] комплексуються моделі броунівського руху та детермінованого підходу. Таке комплексування дозволяє отримувати оцінки захищеності інформаційних сервісів в багатохмарних середовищах без прив’язки до конкретного виду ШПЗ. Таким чином, спектр робіт, як показано вище є дуже різноманітним та неоднозначним.

На відміну від відомих робіт, метою даного дослідження є оцінювання захищеності блокчейн-вузла від Екліпс-атаки та троянського ШПЗ на основі диференціально-ігрових моделей, теоретичний базис яких становлять методи теорії диференціальних ігор та диференціально-експоненціальні перетворення нетейлорівського типу.

МЕТОДИКА ДОСЛІДЖЕННЯ

У [29] показано, що кібератаки на блокчейн-вузли для їх систем безпеки протікають в умовах невизначеності за невідомого вектору атаки, а природа поширення ШПЗ має нелінійний характер [41]. На практиці задачі такого класу зводяться до теоретико-ігрових задач, динаміка процесів у блокчейн-вузлах в яких описується системами диференціальних рівнянь [35]. Однак до сьогодні й надалі невирішеним залишалося питання розроблення таких диференціально-ігрових моделей Екліпс-атаки та троянського ШПЗ, застосування яких дозволяло б одержувати достовірні оцінки рівня захищеності блокчейн-вузла та інших його безпекових метрик, наприклад таких як рівень довіри, рівень толерантності до ризику, рівень залишкового ризику тощо. Вирішити цю проблему пропонується на основі відомого методу диференціально-ігрового моделювання процесів кібернападу [42], який вже знайшов широке

застосування в галузі кібербезпеки [43]. Основу згаданого методу становлять диференціальні перетворення академіка НАН України Г. Пухова [44] та їх модифікація – диференціально-експоненціальні перетворення нетейлорівського типу [45]. Такі перетворення дозволять в реальному часі отримувати точні, у рамках нетейлорівської теорії, диференціально-ігрові моделі Екліпс-атаки та троянського ШПЗ у вигляді відрізка ряду по експоненціальних функціях.

Загальний вигляд таких перетворень, які пропонується покласти в основу розроблюваних диференціально-ігрових моделей можна описати виразом [45]

$$X_0(k)=\begin{cases}\dfrac{T^k}{k!}\left[\dfrac{d^k x_0(t)}{dt^k}\right]_{t=0}; \\ \sum\limits_{s=0}^{s=n} A_s q_s^k \text{ при } A_0=0;\end{cases} \quad \underline{\cdot} \quad x_0(t)=\begin{cases}\sum\limits_{k=0}^{k=m}\left(\dfrac{t}{T}\right)^k X_0(k); \\ \sum\limits_{s=0}^{s=n} A_s e^{q_s t} \text{ при } A_0=0,\end{cases} \tag{1}$$

де $X_0(k)$ – диференціальне зображення оригіналу $x_0(t)$, що становить дискретну функцію цілочислового аргументу k, $k=0,\ldots,m$, $m\to\infty$;

$x_0(t)$ – оригінал, являє собою безперервну, диференціюється нескінченну кількість разів і обмежену разом з усіма своїми похідними функцію дійсного аргументу t;

T – масштабна стала, яка має розмірність аргументу t і обирається з відрізку $0\le t\le T$, на якому розглядається функція $x_0(t)$;

$\underline{\cdot}$ – символ відповідності між оригіналом $x_0(t)$ та його диференціальним зображенням $X_0(k)$;

A_s, q_s – параметри апроксимуючої експоненціальної функції, які підлягають знаходженню одним з відомих методів, наприклад методом спектральних рівнянь, $s=0,\ldots,n$.

Диференціальні зображення $X_0(k)$ називаються диференціальними спектрами, а значення функції $x_0(t)$ при конкретних значеннях аргументу k – дискретами. Ліворуч від символу $\underline{\cdot}$ у перетвореннях (1) стоїть пряме перетворення, що дозволяє за оригіналом $x_0(t)$ знайти зображення $X_0(k)$, а праворуч – зворотне, що дозволяє за зображенням $X_0(k)$ отримати оригінал $x_0(t)$ у формі ряду по експоненціальним функціям. Одержані на основі (1) диференціально-ігрові моделі Екліпс-атаки та троянського ШПЗ є математичним підґрунтям для оцінювання захищеності блокчейн-вузла у вигляді декого рівня. Під час оцінювання зазначеного рівня захищеності в диференціально-ігровій постановці далі по тексту дослідження пропонується оперувати наступними категоріями:

– суб’єкти конфлікту під час атаки на блокчейн-вузол називатимуться гравцями кіберзахисту та кібернападу відповідно;

– правила поведінки гравців називатимуться стратегіями;

– стратегії гравців обиратимуться за умови оптимізації деякого критерію – рівня захищеності блокчейн-вузла, який називатиметься платою;

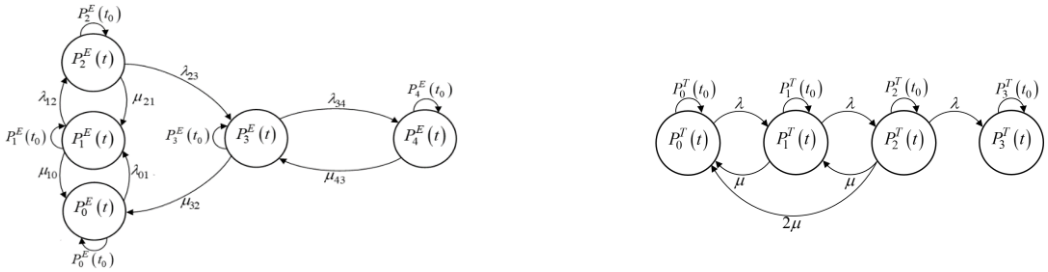
– ціна гри – це плата, за якої гравці одночасно обирають свої оптимальні стратегії;

– рішення диференціального рівняння яке підлягає розв'язанню є траєкторією гри (партії), тобто паттерном Екліпс-атаки на блокчейн-вузол або паттером троянського ШПЗ у залежності від того, який процес моделюється.

Під час здійснення Екліпс-атаки чи під час атаки троянського ШПЗ на блокчейн-вузол інтереси гравців різняться. Вони є антагоністичними. Гравець кіберзахисту намагається максимізувати захищеність блокчейн-вузла, а гравець кібернападу навпаки – мінімізувати. За таких умов задача з диференціально-ігровим базисом набуває безкоаліційного характеру.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Побудова графів Екліпс-атаки та троянського ШПЗ. Опираючись на основні положення теорії ланцюгів Маркова з безперервним часом, а також беручи до уваги відомі дослідження [29], [46] та [47] на рис. 1 приведемо графи Екліпс-атаки та троянського ШПЗ відповідно.



а) *б)*

Рис. 1. Графові моделі атак на блокчейн-вузол:а – граф Екліпс-атаки; б – граф троянського ШПЗ

Позначення вжиті на рис. 1 приведено у табл. 1.

Таблиця 1

Фізична сутність параметрів графових моделей

Познач	Фізична сутність	Од. вимір.
1	2	3
$P_0^E(t)$	ймовірність перебування блокчейн-вузла у нормальному (захищеному) стані	
$P_1^E(t)$	ймовірність зламу гравцем нападу таблиці маршрутизації блокчейн-вузла	
$P_2^E(t)$	ймовірність перезапуску таблиці маршрутизації блокчейн-вузлом	
$P_3^E(t)$	ймовірність віддаленого підключення гравцем нападу до блокчейн-вузла	
$P_4^E(t)$	ймовірність адміністрування блокчейн-вузла гравцем нападу під час якого він перебуває у незахищеному стані	
λ_{01}	інтенсивність кібератаки на таблицю маршрутизації блокчейн-вузла з повідомленням їй хибних IP-адрес для перепідключення	c^{-1}
λ_{12}	інтенсивність кібератаки, спрямованої на ініціювання перезапуску таблиці маршрутизації блокчейн-вузла	c^{-1}
λ_{23}	інтенсивність кібератаки, унаслідок якої перезапускається таблиця маршрутизації і блокчейн-вузол підключається до хибних IP-адрес	c^{-1}
λ_{34}	інтенсивність кібератаки, унаслідок якої блокчейн-вузол підключається до хибних IP-адрес з пулу IP-адрес зламаної таблиці маршрутизації	c^{-1}
μ_{10}	інтенсивність виявлення та видалення повідомлень з хибними IP-адресами	c^{-1}

Продовження таблиці 1

Фізична сутність параметрів графових моделей

1	2	3
μ_{21}	інтенсивність очищення таблиці маршрутизації блокчейн-вузла від пулу хибних IP-адрес	c^{-1}
μ_{32}	інтенсивність відновлення нормальних з'єднань з легітимними IP-адресами за рахунок проведення заходів технічного обслуговування	c^{-1}
μ_{43}	інтенсивність часткового відновлення нормальних з'єднань з легітимними IP-адресами	c^{-1}
$P_0^T(t)$	ймовірність перебування блокчейн-вузла у захищеному стані	
$P_1^T(t)$	ймовірність отримання блокчейн-вузлом файлів, інфікованих троянським ШПЗ	
$P_2^T(t)$	ймовірність запуску власником блокчейн-вузла файлів, інфікованих троянським ШПЗ	
$P_3^T(t)$	ймовірність перебування блокчейн-вузла в незахищеному стані під контролем троянського ШПЗ	
λ	інтенсивність поширення троянського ШПЗ в блокчейн-вузлі (стратегія гравця кібернападу)	c^{-1}
μ	інтенсивність виявлення та видалення файлів, інфікованих троянським ШПЗ (стратегія гравця кіберзахисту)	c^{-1}
t	час перебування блокчейн-вузла в одному зі станів $\left\{P_0^E(t), P_1^E(t),\ldots,P_4^E(t)\right\}$ під час Екліпс-атаки або в одному зі станів $\left\{P_0^T(t), P_1^T(t),\ldots,P_3^T(t)\right\}$ під час атаки троянським ШПЗ відповідно, $t\in[t_0,T]$	c
t_0	час початку кібератаки на блокчейн-вузол	c
T	час завершення кібератаки на блокчейн-вузол	c

Вербальний опис Екліпс-атаки та троянського ШПЗ на основі їх графових моделей. З рис. 1 а випливає, що Екліпс-атака розпочинається з моменту ініціації гравцем кібернападу процедури з'єднання блокчейн-вузла з хибною IP-адресою з пулу IP-адрес таблиці маршрутизації. Таке підключення можливе у разі планового або примусового перезапуску програмного забезпечення блокчейн-вузла. У разі перезапуску програмного забезпечення вузол-жертва з'єднується з хибною IP-адресою з метою отримання віддаленого контролю над ним та подальшої його компрометації. У разі збільшення кількості скомпрометованих блокчейн-вузлів на основі Екліпс-атаки створюються передумови для ініціації інших більш небезпечних кібератак на блокчейн-вузли на рівні мережі.

Поширення троянського ШПЗ у блокчейн-вузлі починається в момент отримання цим вузлом інфікованих файлів (див. рис. 1 б). У разі запуску цих файлів власником блокчейн-вузла даний вузол переходить під контроль власника троянського ШПЗ й перебуває в незахищеному стані. Для уникнення цієї ситуації з метою переведення блокчейн-вузла у захищений стан гравець кіберзахисту на кожному кроці поширення троянського ШПЗ здійснює контрзаходи, спрямовані на підвищення рівня захищеності.

Формалізована постановка задачі оцінювання захищеності блокчейн-вузла від Екліпс-атаки та троянського ШПЗ.

Виходячи з графової моделі (див. рис. 1 а) та вербального опису приведеного вище, процес Екліпс-атаки на блокчейн-вузол у формалізованому вигляді можна описати системою диференціальних рівнянь Колмогорова-Чепмена

$$\begin{cases} \frac{dP_0^E(t)}{dt} = -\lambda_{01}P_0^E(t) + \mu_{10}P_1^E(t) + \mu_{32}P_3^E(t); \\ \frac{dP_1^E(t)}{dt} = -(\lambda_{12} + \mu_{10})P_1^E(t) + \lambda_{01}P_0^E(t) + \mu_{21}P_2^E(t); \\ \frac{dP_2^E(t)}{dt} = -(\lambda_{23} + \mu_{21})P_2^E(t) + \lambda_{12}P_1^E(t); \\ \frac{dP_3^E(t)}{dt} = -(\lambda_{34} + \mu_{32})P_3^E(t) + \lambda_{23}P_2^E(t) + \mu_{43}P_4^E(t); \\ \frac{dP_4^E(t)}{dt} = -\mu_{43}P_4^E(t) + \lambda_{34}P_3^E(t). \end{cases} \quad (2)$$

Система диференціальних рівнянь Колмогорова-Чепмена, які описують процес поширення троянського ШПЗ у блокчейн-вузлі з урахуванням графової моделі (див. рис. 1 б) набуває вигляду

$$\begin{cases} \frac{dP_0^T(t)}{dt} = -\lambda P_0^T(t) + \mu\left(P_1^T(t) + 2P_2^T(t)\right); \\ \frac{dP_1^T(t)}{dt} = -(\lambda + \mu)P_1^T(t) + \lambda P_0^T(t) + \mu P_2^T(t); \\ \frac{dP_2^T(t)}{dt} = -(\lambda + 3\mu)P_2^T(t) + \lambda P_1^T(t); \\ \frac{dP_3^T(t)}{dt} = \lambda P_2^T(t). \end{cases} \quad (3)$$

Системи диференціальних рівнянь (2) та (3) справедливі за початкових умов та умов нормування відповідно:

$$\left[\begin{array}{l} \left[\begin{array}{l} P_0^E(t_0) = 1; \\ P_1^E(t_0) = \ldots = P_4^E(t_0) = 0; \\ P_0^E(t) + P_1^E(t) + \ldots + P_4^E(t) = 1; \end{array}\right. \\ \left[\begin{array}{l} P_0^T(t_0) = 1; \\ P_1^T(t_0) = \ldots = P_3^T(t_0) = 0; \\ P_0^T(t) + P_1^T(t) + \ldots + P_3^T(t) = 1. \end{array}\right. \end{array}\right. \quad (4)$$

Стратегії гравців кібернападу та кіберзахисту під час Екліпс-атаки та троянського ШПЗ відповідно варіюють в межах

$$\left[\begin{array}{ll} \begin{cases} 0 < \lambda_{ij} \le \lambda_{ij\max}; \\ 0 < \mu_{ji} \le \mu_{ji\max}; \end{cases} & \begin{cases} 0 < \lambda \le \lambda_{\max}; \\ 0 < \mu \le \mu_{\max}, \end{cases} \end{array}\right. \quad (5)$$

де $\lambda_{ij\max}$ – максимальна інтенсивність Екліпс-атаки на блокчейн-вузол, $i = 0,\ldots,3$, $j = 1,\ldots,4$;

$\mu_{ji\max}$ – максимальна інтенсивність кіберзахисту блокчейн-вузла від Екліпс-атаки;

$\lambda_{\max}$ – максимальна інтенсивність поширення троянського ШПЗ в блокчейн-вузлі;

$\mu_{\max}$ – максимальна інтенсивність кіберзахисту блокчейн-вузла від троянського ШПЗ.

Обґрунтування показника оцінювання рівня захищеності. Показником захищеності блокчейн-вузла від Екліпс-атаки та троянського ШПЗ є його рівень захищеності –

Security Level (SL) [48]. У диференціально-ігровій постановці рівень захищеності SL є платою гри за довільних стратегій, які обираються гравцями [42]. Для досліджуваних кібератак плати у загальному вигляді, з урахуванням відомої формули інтегрування в області зображень [44], можуть бути визначені згідно виразів відповідно

$$\begin{cases} SL^E\left(\mu_{ji},\lambda_{ij}\right)=\dfrac{1}{T}\int\limits_{t_0}^{T}P_0^E\left(t\right)dt \quad \div \quad SL^E\left(\mu_{ji},\lambda_{ij}\right)\Big|_k=\sum\limits_{k=0}^{k=\infty}\dfrac{P_0^E\left(k\right)}{k+1}; \\ SL^T\left(\mu,\lambda\right)=\dfrac{1}{T}\int\limits_{t_0}^{T}P_0^T\left(t\right)dt \quad \div \quad SL^T\left(\mu,\lambda\right)\Big|_k=\sum\limits_{k=0}^{k=\infty}\dfrac{P_0^T\left(k\right)}{k+1}, \end{cases} \tag{6}$$

де SL^E – рівень захищеності блокчейн-вузла від Екліпс-атаки;
SL^T – рівень захищеності блокчейн-вузла від троянського ШПЗ.

Крім довільних стратегій під час кібератаки на блокчейн-вузол гравці можуть обирати інші типи стратегій відповідно до умов (5). У такому разі рівень захищеності *SL* блокчейн-вузла (6) змінюватиметься. Зв'язок між рівнем захищеності *SL* та відповідними метриками в диференціально-ігровій та безпековій постановках на прикладі кібератаки троянським ШПЗ на блокчейн-вузол наведено в табл. 2.

Таблиця 2

Таблиця співвідношення між рівнем захищеності Security Level та відповідними метриками в диференціально-ігровій та безпековій постановках

	Тип стратегії							
Диференціально-ігрова постановка [47]	**оптимальна**		**змішана**				**довільна**	
	$\mu^{opt}{}_{extr}$	$\lambda^{opt}{}_{extr}$	μ	$\lambda^{opt}{}_{extr}$	$\mu^{opt}{}_{extr}$	λ	μ	λ
	$AL^{T\,\mu^{opt}{}_{extr}}_{\lambda^{opt}{}_{extr}}$		$RT^T\left(\mu,\lambda^{opt}{}_{extr}\right)$		$RR^T\left(\mu^{opt}{}_{extr},\lambda\right)$		$SL^T\left(\mu,\lambda\right)$	
Безпекова постановка [48]	*Assurance Level*/ Рівень гарантій		*Risk Tolerance*/ Допустимий рівень ризику		*Residual Risk* / Залишковий ризик		*Security Level* / Рівень захищеності	

У табл. 2 вжито такі позначення: $\mu^{opt}_{ji\ extr}$, $\mu^{opt}{}_{extr}$ та $\lambda^{opt}_{ij\ extr}$, $\lambda^{opt}{}_{extr}$ – оптимальні стратегії гравців кіберзахисту та кібернападу в їх екстремальних (граничних) значеннях відповідно. Для Екліпс-атаки наведені в табл. 2 метрики є тотожними та зберігають аналогічний фізичний зміст. Обґрунтування критерію оцінювання рівня захищеності. При визначенні критерію для оцінювання рівня захищеності блокчейн-вузла опиратимемось на логіку за якою гравці обиратимуть свої стратегії. Так гравці кіберзахисту обиратимуть такі стратегії μ_{ji} та μ, які максимізуватимуть рівні захищеності SL^E та SL^T відповідно, при умові їх мінімізації іншими гравцями, тобто

$$\begin{cases} SL^E\left(\mu_{ji},\lambda_{ij}\right)=\max\limits_{\mu_{ji}\in E_{\mu_{ji}}}\min\limits_{\lambda_{ij}\in E_{\lambda_{ij}}}SL^E\left(\mu_{ji},\lambda_{ij}\right)\Big|_k; \\ SL^T\left(\mu,\lambda\right)=\max\limits_{\mu\in E_{\mu}}\min\limits_{\lambda\in E_{\lambda}}SL^T\left(\mu,\lambda\right)\Big|_k, \end{cases} \tag{7}$$

де $SL^E\left(\mu_{ji},\lambda_{ij}\right)\Big|_k$ та $SL^T\left(\mu,\lambda\right)\Big|_k$ – плати за обраних гравцями стратегій μ_{ji}, μ та λ_{ij}, λ у замкнених обмежених у евклідових просторах $E_{\mu_{ji}}$, E_{μ} та $E_{\lambda_{ij}}$, E_{λ} з відповідних $R_{\mu_{ji}}$, R_{μ} та $R_{\lambda_{ij}}$, R_{λ} множин, які визначають можливі стратегії гравців. Гравці кібернападу,

навпаки, на відміну від стратегій гравців кіберзахисту (7), обиратимуть такі стратегії λ_{ij} й λ, які мінімізуватимуть згадані рівні, тобто

$$\begin{cases} SL^E\left(\mu_{ji},\lambda_{ij}\right)=\min\limits_{\lambda_{ij}\in E_{\lambda_{ij}}}\max\limits_{\mu_{ji}\in E_{\mu_{ji}}} SL^E\left(\mu_{ji},\lambda_{ij}\right)\Big|_k; \\ SL^T\left(\mu,\lambda\right)=\min\limits_{\lambda\in E_\lambda}\max\limits_{\mu\in E_\mu} SL^T\left(\mu,\lambda\right)\Big|_k. \end{cases} \tag{8}$$

Закономірним також є припущення про те, що всі гравці в даних диференціальних іграх намагатимуться дотримуватися своїх оптимальних стратегій і прагнутимуть гарантованого результату: одні з позицій кіберзахисту, інші – з позицій кібернападу. У такому разі плати (6) вироджуватимуться в ціну гри, яка в теорії диференціальних ігор є гарантованою оцінкою [42]. У безпековій постановці, як показано в табл. 2, ці метрики називатимуться рівнем гарантій – Assurance Level (AL) [48]:

$$\begin{cases} AL^{E\,\mu_{ji}^{opt}{}_{extr}}_{\lambda_{ij}^{opt}{}_{extr}}=\max\limits_{\mu_{ji}\in E_{\mu_{ji}}}\min\limits_{\lambda_{ij}\in E_{\lambda_{ij}}} SL^E\left(\mu_{ji},\lambda_{ij}\right)\Big|_k=\min\limits_{\lambda_{ij}\in E_{\lambda_{ij}}}\max\limits_{\mu_{ji}\in E_{\mu_{ji}}} SL^E\left(\mu_{ji},\lambda_{ij}\right)\Big|_k; \\ AL^{T\,\mu^{opt}{}_{extr}}_{\lambda^{opt}{}_{extr}}=\max\limits_{\mu\in E_\mu}\min\limits_{\lambda\in E_\lambda} SL^T\left(\mu,\lambda\right)\Big|_k=\min\limits_{\lambda\in E_\lambda}\max\limits_{\mu\in E_\mu} SL^T\left(\mu,\lambda\right)\Big|_k. \end{cases} \tag{9}$$

Виконання умови (9) – умови існування сідлової точки [42], свідчить про недоцільність відхилення гравцями від своїх оптимальних стратегій, оскільки в усіх інших випадках кожен з них зазнає втрат у платі – рівні захищеності блокчейн-вузла, тобто

$$\begin{cases} \begin{cases} RR^E\left(\mu_{ji}^{opt}{}_{extr},\lambda_{ij}\right)\le\max\limits_{\mu_{ji}\in E_{\mu_{ji}}} SL^E\left(\mu_{ji},\lambda_{ij}\right)\Big|_k; \\ RT^E\left(\mu_{ji},\lambda_{ij}^{opt}{}_{extr}\right)\ge\min\limits_{\lambda_{ij}\in E_{\lambda_{ij}}} SL^E\left(\mu_{ji},\lambda_{ij}\right)\Big|_k; \end{cases} \\ \begin{cases} RR^T\left(\mu^{opt}{}_{extr},\lambda\right)\le\max\limits_{\mu\in E_\mu} SL^T\left(\mu,\lambda\right)\Big|_k; \\ RT^T\left(\mu,\lambda^{opt}{}_{extr}\right)\ge\min\limits_{\lambda\in E_\lambda} SL^T\left(\mu,\lambda\right)\Big|_k. \end{cases} \end{cases} \tag{10}$$

Таким чином, оцінювання захищеності блокчейн-вузла від Екліпс-атаки та троянського ШПЗ на основі приведених вище моделей зведено до класичних диференціально-ігрових задач, в яких знаходженню підлягають такі їх параметри як

$$\begin{cases} \left\langle P_0^{E\,opt}\left(t\right),\mu_{ji}^{opt}{}_{extr},\lambda_{ij}^{opt}{}_{extr},AL^{E\,\mu_{ji}^{opt}{}_{extr}}_{\lambda_{ij}^{opt}{}_{extr}}\right\rangle; \\ \left\langle P_0^{T\,opt}\left(t\right),\mu^{opt}{}_{extr},\lambda^{opt}{}_{extr},AL^{T\,\mu^{opt}{}_{extr}}_{\lambda^{opt}{}_{extr}}\right\rangle. \end{cases} \tag{11}$$

Результати розв'язання диференціальних ігор. Скориставшись описаною вище методологією на основі прямого перетворення (1) для $m=3$ і $n=2$ отримаємо диференціальні спектри для ймовірності перебування блокчейн-вузла у нормальному (захищеному) стані під час Екліпс-атаки $P_0^E\left(k=m\right)$. Скориставшись при цьому методом спектральних на основі методу ітерацій одразу визначимо невідомі параметри апроксимуючої експоненціальної функції $\left\langle\left\{A_1^E,A_2^E\right\};\left\{q_1^E,q_2^E\right\}\right\rangle$. У результаті отримаємо:

$$\begin{cases} P_0^E(0)=1; \\ P_0^E(1)=-\lambda_{01}T; \\ P_0^E(2)=\frac{1}{2}\lambda_{01}(\lambda_{01}+\mu_{10})T^2; \\ P_0^E(3)=-\frac{1}{6}\lambda_{01}\left((\lambda_{01}+\mu_{10})^2+\lambda_{12}\mu_{10}\right)T^3; \end{cases} \Rightarrow \begin{cases} P_0^E(0)=A_1^E+A_2^E; \\ P_0^E(1)=q_1^E A_1^E+q_1^E A_2^E; \\ P_0^E(2)=q_1^{E^2} A_1^E+q_2^{E^2} A_2^E; \\ P_0^E(3)=q_1^{E^3} A_1^E+q_2^{E^3} A_2^E; \end{cases}$$

$$\left\langle \begin{matrix} \{A_1^E, A_2^E\}; \\ \{q_1^E, q_2^E\} \end{matrix} \right\rangle \Rightarrow \left\langle \begin{matrix} \left\{\frac{9}{2}\left(\frac{\lambda_{01}}{\lambda_{01}+\mu_{10}}\right), 1-\frac{9}{2}\left(\frac{\lambda_{01}}{\lambda_{01}+\mu_{10}}\right)\right\}; \\ \left\{-\frac{1}{3}(\lambda_{01}+\mu_{10})T, \frac{1}{2}\frac{\lambda_{01}}{\left(1-\frac{9}{2}\left(\frac{\lambda_{01}}{\lambda_{01}+\mu_{10}}\right)\right)}T\right\} \end{matrix} \right\rangle \Bigg|_{\lambda_{12}\approx 0}. \quad (12)$$

Аналогічно до (12) за диференціальними спектрами ймовірності перебування блокчейн-вузла в захищеному стані під час атаки на нього троянського ШПЗ $P_0^T(k=m)$ знайдемо невідомі параметри апроксимуючої експоненціальної функції $\left\langle \{A_1^T, A_2^T\}; \{q_1^T, q_2^T\} \right\rangle$:

$$\begin{cases} P_0^T(0)=1; \\ P_0^T(1)=-\lambda T; \\ P_0^T(2)=\frac{1}{2}\lambda(\lambda+\mu)T^2; \\ P_0^T(3)=-\frac{1}{6}\lambda\left(\lambda^2+\lambda\mu+\mu^2\right)T^3; \end{cases} \Rightarrow \begin{cases} P_0^T(0)=A_1^T+A_2^T; \\ P_0^T(1)=q_1^T A_1^T+q_2^T A_2^T; \\ P_0^T(2)=q_1^{T^2} A_1^T+q_2^{T^2} A_2^T; \\ P_0^T(3)=q_1^{T^3} A_1^T+q_2^{T^3} A_2^T; \end{cases} \quad (13)$$

$$\left\langle \begin{matrix} \{A_1^T, A_2^T\}; \\ \{q_1^T, q_2^T\} \end{matrix} \right\rangle \Rightarrow \left\langle \begin{matrix} \left\{\frac{9}{2}\frac{\lambda(\lambda+\mu)^3}{\left(\lambda^2+\lambda\mu+\mu^2\right)^2}, \frac{-7\lambda^4-23\lambda^3\mu-21\lambda^2\mu^2-5\lambda\mu^3+2\mu^4}{2\left(\lambda^2+\lambda\mu+\mu^2\right)^2}\right\}; \\ \left\{-\frac{1}{3}\frac{\left(\lambda^2+\lambda\mu+\mu^2\right)}{(\lambda+\mu)}T, \frac{\lambda\left(\lambda^2+\lambda\mu+\mu^2\right)\left(\lambda^2+4\lambda\mu+\mu^2\right)}{-7\lambda^4-23\lambda^3\mu-21\lambda^2\mu^2-5\lambda\mu^3+2\mu^4}T\right\} \end{matrix} \right\rangle.$$

Провівши зворотне диференціально-експоненціальне перетворення (1) з урахуванням визначених параметрів апроксимуючих експоненціальних функцій $\left\langle \{A_1^E, A_2^E\}; \{q_1^E, q_2^E\} \right\rangle$ (12) і $\left\langle \{A_1^T, A_2^T\}; \{q_1^T, q_2^T\} \right\rangle$ (13), отримаємо шукані ймовірності $P_0^E(t)$ і $P_0^T(t)$ в загальному вигляді відповідно

$$P_0^E(t)=\frac{9}{2}\left(\frac{\lambda_{01}}{\lambda_{01}+\mu_{10}}\right)\exp\left(-\frac{1}{3}(\lambda_{01}+\mu_{10})t\right)+ +\left(1-\frac{9}{2}\left(\frac{\lambda_{01}}{\lambda_{01}+\mu_{10}}\right)\right)\exp\left(\frac{1}{2}\frac{\lambda_{01}}{\left(1-\frac{9}{2}\left(\frac{\lambda_{01}}{\lambda_{01}+\mu_{10}}\right)\right)}t\right),$$

$$P_0^T(t)=\frac{9}{2}\frac{\lambda(\lambda+\mu)^3}{\left(\lambda^2+\lambda\mu+\mu^2\right)^2}\exp\left(-\frac{1}{3}\frac{\left(\lambda^2+\lambda\mu+\mu^2\right)}{(\lambda+\mu)}t\right)+ \quad (14)$$

$$+\left(\frac{-7\lambda^4-23\lambda^3\mu-21\lambda^2\mu^2-5\lambda\mu^3+2\mu^4}{2\left(\lambda^2+\lambda\mu+\mu^2\right)^2}\right)\exp\left(\frac{\lambda\left(\lambda^2+\lambda\mu+\mu^2\right)\left(\lambda^2+4\lambda\mu+\mu^2\right)}{-7\lambda^4-23\lambda^3\mu-21\lambda^2\mu^2-5\lambda\mu^3+2\mu^4}t\right).$$

Отримавши в аналітичному вигляді (14) вирази для ймовірностей перебування блокчейн-вузла в захищених станах під впливом Екліпс-атаки та троянського ШПЗ, а

також скориставшись відомою формулою інтегрування [44] з (6), оцінимо його рівень захищеності для довільних стратегій гравців, визначених в межах (5):

$$\begin{cases} SL^E\left(\mu_{ji},\lambda_{ij}\right) \approx 1-\frac{1}{2}\lambda_{01}T+\frac{1}{6}\lambda_{01}\left(\lambda_{01}+\mu_{10}\right)T^2-\frac{1}{24}\lambda_{01}\left(\left(\lambda_{01}+\mu_{10}\right)^2+\lambda_{12}\mu_{10}\right)T^3; \\ SL^T\left(\mu,\lambda\right) \approx 1-\frac{1}{2}\lambda T+\frac{1}{6}\lambda\left(\lambda+\mu\right)T^2-\frac{1}{24}\lambda\left(\lambda^2+\lambda\mu+\mu^2\right)T^3, \end{cases} \tag{15}$$

де $P_0^E\left(k=m\right)$, $P_0^T\left(k=m\right)$, $m=3$.

Для знаходження оптимальних стратегій дослідимо знайдені в аналітичному вигляді вирази рівнів захищеності (15) на екстремум, тобто

$$\begin{cases} \left.\frac{\partial SL^E\left(\mu_{ji},\lambda_{ij}\right)}{\partial\mu_{ji}}\right|_{\lambda_{12}\approx 0}=0; \\ \left.\frac{\partial SL^E\left(\mu_{ji},\lambda_{ij}\right)}{\partial\lambda_{ij}}\right|_{\lambda_{12}\approx 0}=0; \\ \frac{\partial SL^T\left(\mu,\lambda\right)}{\partial\mu}=0; \\ \frac{\partial SL^T\left(\mu,\lambda\right)}{\partial\lambda}=0; \end{cases} \Rightarrow \begin{cases} \begin{cases} \mu_{10\ extr}^{opt}=\frac{1}{T}; \\ \lambda_{01\ extr}^{opt}=\frac{1}{T}; \end{cases} \\ \begin{cases} \mu^{opt}{}_{extr}=\frac{5}{3T}; \\ \lambda^{opt}{}_{extr}=\frac{2}{3T}. \end{cases} \end{cases} \tag{16}$$

Визначення знаку екстремуму (16) здійснимо на основі дослідження (15) на виконання достатніх умов:

$$\begin{cases} \left.\frac{\partial^2 AL^E\left(\mu_{ji\ extr}^{opt},\lambda_{ij\ extr}^{opt}\right)}{\partial\left(\mu_{ji\ extr}^{opt}\right)^2}\right|_{\lambda_{12}\approx 0}<0; \\ \left.\frac{\partial^2 AL^E\left(\mu_{ji\ extr}^{opt},\lambda_{ij\ extr}^{opt}\right)}{\partial\left(\lambda_{ij\ extr}^{opt}\right)^2}\right|_{\lambda_{12}\approx 0}>0; \\ \frac{\partial^2 AL^T\left(\mu^{opt}{}_{extr},\lambda^{opt}{}_{extr}\right)}{\partial\left(\mu^{opt}{}_{extr}\right)^2}<0; \\ \frac{\partial^2 AL^T\left(\mu^{opt}{}_{extr},\lambda^{opt}{}_{extr}\right)}{\partial\left(\lambda^{opt}{}_{extr}\right)^2}>0; \end{cases} \Rightarrow \begin{cases} \begin{cases} \mu_{10\ extr}^{opt}=\mu_{10\ \max}^{opt}; \\ \lambda_{01\ extr}^{opt}=\lambda_{01\ \min}^{opt}; \end{cases} \\ \begin{cases} \mu^{opt}{}_{extr}=\mu^{opt}{}_{\max}; \\ \lambda^{opt}{}_{extr}=\lambda^{opt}{}_{\min}. \end{cases} \end{cases} \tag{17}$$

Таким чином, урахувавши (14), (17) та (9), розв’язками диференціальних ігор в постановці (11) будуть:

$$\begin{cases} \left\langle P_0^{E\,opt}\left(t\right)=\frac{9}{4}e^{-\frac{2}{3}t}-\frac{5}{4}e^{-\frac{2}{5}t},\ \mu_{10\ \max}^{opt}=\frac{1}{T},\ \lambda_{01\ \min}^{opt}=\frac{1}{T},\ AL^{E\,\mu_{10\ \max}^{opt}}_{\lambda_{01\ \min}^{opt}}\approx 0.667\right\rangle; \\ \left\langle P_0^{T\,opt}\left(t\right)=\frac{343}{169}e^{-\frac{13}{21}t}-\frac{174}{169}e^{-\frac{299}{522}t},\ \mu^{opt}{}_{\max}=\frac{5}{3T},\ \lambda^{opt}{}_{\min}=\frac{2}{3T},\ AL^{T\,\mu^{opt}_{\max}}_{\lambda^{opt}_{\min}}\approx 0.806\right\rangle. \end{cases} \tag{18}$$

Верифікація та аналіз результатів. Верифікацію знайдених рішень проведено засобами математичного моделювання з використанням онлайн-пакета символьної математики Maple [49]. Матриці верифікації метрик оцінок захищеності блокчейн-вузла від досліджуваних кібератак за різних стратегій гравців приведено в табл. 2 та табл. 3. При проведенні верифікації крок дискретизації у зміні стратегій

гравців для кожної кібератаки обрано у 25% в бік зменшення або збільшення, залежно від знайдених екстремумів (17).

Таблиця 3

Безпекові метрики блокчейн-вузла під час Екліпс-атаки

Матриця безпекових метрик

Екліпс-атака		*стратегія кіберзахисту, c^{-1}*			
		$0.25\mu_{10\ \max}^{opt}$	$0.5\mu_{10\ \max}^{opt}$	$0.75\mu_{10\ \max}^{opt}$	$\mu_{10\ \max}^{opt}$
стратегія кібернападу, c^{-1}	$\lambda_{01\ \min}^{opt}$	RT_{11}^{E}	RT_{12}^{E}	RT_{13}^{E}	AL_{14}^{E}
	$1.25\lambda_{01\ \min}^{opt}$	SL_{21}^{E}	SL_{22}^{E}	SL_{23}^{E}	RR_{24}^{E}
	$1.5\lambda_{01\ \min}^{opt}$	SL_{31}^{E}	SL_{32}^{E}	SL_{33}^{E}	RR_{34}^{E}
	$1.75\lambda_{01\ \min}^{opt}$	SL_{41}^{E}	SL_{42}^{E}	SL_{43}^{E}	RR_{44}^{E}

Мнемонічні правила

$$\Rightarrow \begin{cases} RT_{11}^{E} \geq SL_{21}^{E} \geq RR_{24}^{E}; \\ RT_{12}^{E} \geq SL_{22}^{E} \geq RR_{24}^{E}; \\ RT_{13}^{E} \geq SL_{23}^{E} \geq RR_{24}^{E}; \end{cases} \begin{cases} RT_{11}^{E} \geq SL_{31}^{E} \geq RR_{34}^{E}; \\ RT_{12}^{E} \geq SL_{32}^{E} \geq RR_{34}^{E}; \\ RT_{13}^{E} \geq SL_{33}^{E} \geq RR_{34}^{E}; \end{cases} \begin{cases} RT_{11}^{E} \geq SL_{41}^{E} \geq RR_{44}^{E}; \\ RT_{12}^{E} \geq SL_{42}^{E} \geq RR_{44}^{E}; \\ RT_{13}^{E} \geq SL_{43}^{E} \geq RR_{44}^{E}; \end{cases}$$

Результати верифікації

$\Downarrow$

Екліпс-атака		*стратегія кіберзахисту, c^{-1}*			
		$0.25\mu_{10\ \max}^{opt}$	$0.5\mu_{10\ \max}^{opt}$	$0.75\mu_{10\ \max}^{opt}$	$\mu_{10\ \max}^{opt}$
стратегія кібернападу, c^{-1}	$\lambda_{01\ \min}^{opt}$	0.643	0.656	0.644	0.667
	$1.25\lambda_{01\ \min}^{opt}$	0.570	0.580	0.583	0.580
	$1.5\lambda_{01\ \min}^{opt}$	0.496	0.500	0.496	0.484
	$1.75\lambda_{01\ \min}^{opt}$	0.417	0.412	0.398	0.376

Таблиця 4

Безпекові метрики блокчейн-вузла під час атаки троянським ШПЗ

Матриця безпекових метрик

Троянське ШПЗ		*стратегія кіберзахисту, c^{-1}*			
		$0.25\mu^{opt}{}_{\max}$	$0.5\mu^{opt}{}_{\max}$	$0.75\mu^{opt}{}_{\max}$	$\mu^{opt}{}_{\max}$
стратегія кібернападу, c^{-1}	$\lambda^{opt}{}_{\min}$	RT_{11}^{T}	RT_{12}^{T}	RT_{13}^{T}	AL_{14}^{T}
	$1.25\lambda^{opt}{}_{\min}$	SL_{21}^{T}	SL_{22}^{T}	SL_{23}^{T}	RR_{24}^{T}
	$1.5\lambda^{opt}{}_{\min}$	SL_{31}^{T}	SL_{32}^{T}	SL_{33}^{T}	RR_{34}^{T}
	$1.75\lambda^{opt}{}_{\min}$	SL_{41}^{T}	SL_{42}^{T}	SL_{43}^{T}	RR_{44}^{T}

Мнемонічні правила

$$\Rightarrow \begin{cases} RT_{11}^{T} \geq SL_{21}^{T} \geq RR_{24}^{T}; \\ RT_{12}^{T} \geq SL_{22}^{T} \geq RR_{24}^{T}; \\ RT_{13}^{T} \geq SL_{23}^{T} \geq RR_{24}^{T}; \end{cases} \begin{cases} RT_{11}^{T} \geq SL_{31}^{T} \geq RR_{34}^{T}; \\ RT_{12}^{T} \geq SL_{32}^{T} \geq RR_{34}^{T}; \\ RT_{13}^{T} \geq SL_{33}^{T} \geq RR_{34}^{T}; \end{cases} \begin{cases} RT_{11}^{T} \geq SL_{41}^{T} \geq RR_{44}^{T}; \\ RT_{12}^{T} \geq SL_{42}^{T} \geq RR_{44}^{T}; \\ RT_{13}^{T} \geq SL_{43}^{T} \geq RR_{44}^{T}; \end{cases}$$

Результати верифікації

$\Downarrow$

Троянське ШПЗ		*стратегія кіберзахисту, c^{-1}*			
		$0.25\mu^{opt}{}_{\max}$	$0.5\mu^{opt}{}_{\max}$	$0.75\mu^{opt}{}_{\max}$	$\mu^{opt}{}_{\max}$
стратегія кібернападу, c^{-1}	$\lambda^{opt}{}_{\min}$	0.762	0.786	0.801	0.806
	$1.25\lambda^{opt}{}_{\min}$	0.715	0.743	0.758	0.762
	$1.5\lambda^{opt}{}_{\min}$	0.670	0.700	0.716	0.718
	$1.75\lambda^{opt}{}_{\min}$	0.626	0.658	0.673	0.672

У табл. 3 та табл. 4 праворуч від кожної з матриць формалізовано мнемонічні правила. Дані правила в аналітичному вигляді узагальнюють співвідношення між оцінюваними метриками за обраного кроку дискретизації зміни стратегій гравців. Також для спрощення математичних викладок у згаданих таблицях використано такі умовні скорочення:

$$AL^E = AL^{E\,\mu_{10}^{opt}\,\max}_{\lambda_{01}^{opt}\,\min};\qquad AL^T = AL^{T\;\mu^{opt}\,\max}_{pq\;\lambda^{opt}\,\min};$$

$$RR^E_{pq} = RR^E_{pq}\left(\mu_{10}^{opt}\,\max, \lambda_{01}\right);\qquad RR^T_{pq} = RR^T_{pq}\left(\mu^{opt}\,\max, \lambda\right);$$

$$RT^E_{pq} = RT^E_{pq}\left(\mu_{10}, \lambda_{01}^{opt}\,\min\right);\qquad RT^T_{pq} = RT^T_{pq}\left(\mu, \lambda^{opt}\,\min\right);$$

$$SL^E_{pq} = SL^E_{pq}\left(\mu_{10}, \lambda_{01}\right);\qquad SL^T_{pq} = SL^T_{pq}\left(\mu, \lambda\right),$$

де $p = \overline{1,4}$, $q = \overline{1,4}$.

Для повноти оцінювання й встановлення загальних тенденцій зміни захищеності блокчейн-вузла під досліджуваними кібератаками на рис. 2 та рис. 3 приведені відповідні графіки, одержані на основі знайдених аналітичних рішень (14) та (18).

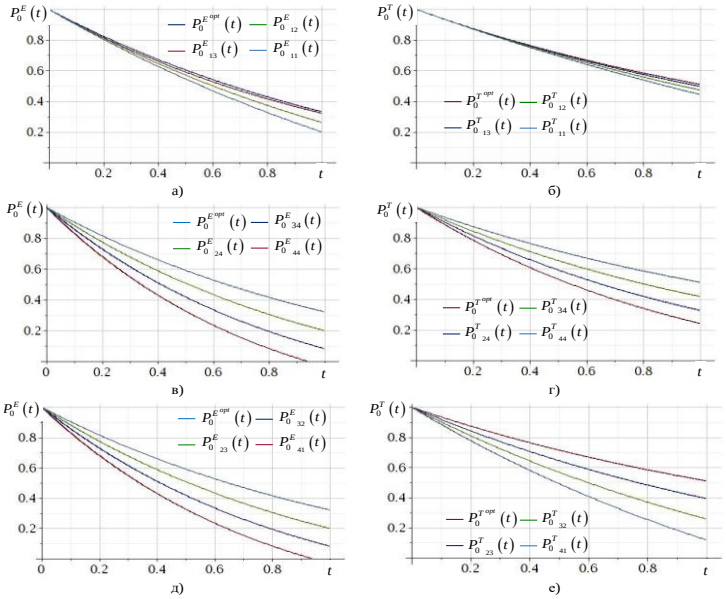


Рис. 2. Ймовірності перебування блокчейн-вузла в захищеному стані: а, в, д – під впливом Екліпс-атаки; б, г, е – під впливом атаки троянським ШПЗ

Аналіз результатів оцінювання рівня захищеності, приведених в табл. 3 та табл. 4 показує, що для блокчейн-вузла за однакових вихідних умов з досліджуваних кібератак найбільш небезпечною є Екліпс-атака. При її реалізації рівень гарантій за оптимальних стратегій гравців не перевищує 0.677, що на 16% нижче ніж при атаці троянським ШПЗ. При відхиленні гравцями від оптимальних стратегій рівень захищеності блокчейн-вузла під час Екліпс-атаки знижується. Найбільш суттєво на його зміну впливає стратегія гравця кібернападу. При відхиленні таким гравцем від своєї оптимальної стратегії більш ніж на 25% у бік нарощення інтенсивності кібератаки блокчейн-вузол переходить в незахищений стан та потенційно підпадає під адміністрування атакуючим гравцем. Слід зауважити, що у разі додержання гравцем кібернападу своєї оптимальної стратегії, вибір стратегії кіберзахисту блокчейн-вузла

відмінної від оптимальної призведе до відхилення його рівня захищеності від максимально можливого рівня гарантій, але й надалі залишатиметься в межах допустимого рівня ризику.

Таким чином, результати аналізу даних верифікації рівня захищеності блокчейн вузла дозволяють стверджувати про адекватність запропонованих вище математичних моделей, а одержані оцінки рівня захищеності блокчейн-вузла під час Екліпс-атаки можуть із заданим ступенем достовірності (залежить від кількості дискрет диференціального спектра, які враховуються під час оцінювання) визначатися такими математичними моделями:

$$\begin{cases} AL^{E}{}_{\lambda_{01}^{opt}}^{\mu_{10}^{opt}{}_{\max}} \approx 0.667; \\ RT^{E}\left(\mu_{10}, \lambda_{01}^{opt}{}_{\min}\right) \approx 1 - \frac{1}{2}\lambda_{01}^{opt}{}_{\min} T + \frac{1}{6}\lambda_{01}^{opt}{}_{\min}\left(\lambda_{01}^{opt}{}_{\min} + \mu_{10}\right)T^2 - \\ \qquad - \frac{1}{24}\lambda_{01}^{opt}{}_{\min}\left(\left(\lambda_{01}^{opt}{}_{\min} + \mu_{10}\right)^2\right)T^3; \\ RR^{E}\left(\mu_{10}^{opt}{}_{\max}, \lambda_{01}\right) \approx 1 - \frac{1}{2}\lambda_{01} T + \frac{1}{6}\lambda_{01}\left(\lambda_{01} + \mu_{10}^{opt}{}_{\max}\right)T^2 - \\ \qquad - \frac{1}{24}\lambda_{01}\left(\left(\lambda_{01} + \mu_{10}^{opt}{}_{\max}\right)^2\right)T^3; \\ SL^{E}\left(\mu_{ji}, \lambda_{ij}\right) \approx 1 - \frac{1}{2}\lambda_{01} T + \frac{1}{6}\lambda_{01}\left(\lambda_{01} + \mu_{10}\right)T^2 - \frac{1}{24}\lambda_{01}\left(\left(\lambda_{01} + \mu_{10}\right)^2\right)T^3. \end{cases} \quad (19)$$

Рівень захищеності блокчейн-вузла під час кібератаки його троянським ШПЗ також варіює, залежно від стратегій, які обираються гравцями. Так рівень гарантій у разі вибору гравцями оптимальних стратегій є відносно високим, порівняно з рівнем гарантій за того ж розподілу стратегій гравців під час Екліпс-атаки. Він складає 0.806, що свідчить про високу стійкість блокчейн-вузлів до кібератак троянським ШПЗ. Навіть відхилення гравцями від оптимальних стратегій не дозволить гравцю кібернападу перевести блокчейн-вузол у не захищений стан. Однак, справедливо слід зазначити, що у такому разі ймовірності отримання блокчейн-вузлом інфікованих файлів та їх запуску його власником, зростають. Відповідно зростають і ризики, що автоматично відображається на зниженні рівня захищеності.

Таким чином, розподіл метрик безпеки для блокчейн-вузла під впливом троянського ШПЗ може бути поданий комплексом моделей вигляду:

$$\begin{cases} AL^{T}{}_{\lambda^{opt}{}_{\min}}^{\mu^{opt}{}_{\max}} \approx 0.806; \\ RR^{T}\left(\mu^{opt}{}_{\max}, \lambda\right) \approx 1 - \frac{1}{2}\lambda T + \frac{1}{6}\lambda\left(\lambda + \mu^{opt}{}_{\max}\right)T^2 - \\ \qquad - \frac{1}{24}\lambda\left(\lambda^2 + \lambda\,\mu^{opt}{}_{\max} + \mu^{opt}{}_{\max}{}^2\right)T^3; \\ RT^{T}\left(\mu, \lambda^{opt}{}_{\min}\right) \approx 1 - \frac{1}{2}\lambda^{opt}{}_{\min} T + \frac{1}{6}\lambda^{opt}{}_{\min}\left(\lambda^{opt}{}_{\min} + \mu\right)T^2 - \\ \qquad - \frac{1}{24}\lambda^{opt}{}_{\min}\left(\lambda^{opt}{}_{\min}{}^2 + \lambda^{opt}{}_{\min}\,\mu + \mu^2\right)T^3; \\ SL^{T}\left(\mu, \lambda\right) \approx 1 - \frac{1}{2}\lambda T + \frac{1}{6}\lambda\left(\lambda + \mu\right)T^2 - \frac{1}{24}\lambda\left(\lambda^2 + \lambda\,\mu + \mu^2\right)T^3. \end{cases} \quad (20)$$

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Отримані результати становлять одне з перших узагальнень у галузі кібербезпеки щодо масштабування диференціально-ігрових моделей, побудованих на основі диференціальних перетворень, для оцінювання захищеності блокчейн-вузла під впливом Екліпс-атаки та атаки троянським ШПЗ. Верифікація моделей засобами математичного моделювання підтвердила їх адекватність, оскільки теоретичні положення збігаються з результатами числових розрахунків.

Знайдені аналітичні вирази (19) та (20), які описують метрики безпеки блокчейн-вузла, дають змогу робити обґрунтовані висновки про вплив стратегій гравців на його рівень захищеності. Серед важливих результатів встановлено, що Екліпс-атака на блокчейн-вузол є більш небезпечною, ніж атака троянським ШПЗ. Такий висновок обумовлює потребу розширення спектра засобів і заходів кіберзахисту для забезпечення його кіберстійкості.

Запропоновані диференціально-ігрові моделі у реальному та прискореному масштабах часу дозволяють оцінювати й прогнозувати рівень захищеності блокчейн-вузла залежно від стратегій гравців, які обираються гравцями.

Перспективним напрямом подальших досліджень є розширення кола диференціально-ігрових моделей для аналізу впливу інших, недосліджених у цій роботі, кібератак. Це створить підґрунтя для розроблення практичних рекомендацій із забезпечення кібербезпеки блокчейн-технологій у різних прикладних сферах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Guo, H., & Yu, X. (2022). A survey on blockchain technology and its security. Blockchain: Research and Applications, 3(2), 100067. https://doi.org/10.1016/j.bcra.2022.100067
2. Pessa, A. A. B., Perc, M., & Ribeiro, H. V. (2023). Age and market capitalization drive large price variations of cryptocurrencies. Scientific Reports, 13, 3351. https://doi.org/10.1038/s41598-023-30431-3
3. Krause, D. S. (2025). The $1.4 billion Bybit hack: Cybersecurity failures and the risks of cryptocurrency deregulation. International Journal of Cryptocurrency Research, 5(1), 52–62. https://doi.org/10.51483/IJCCR.5.1.2025.52-62
4. Barj, S., & Youjil, A. (2024). Blockchain and cryptocurrency security from a layered perspective using MITRE ATT&CK. International Journal of Engineering Trends and Technology, 72(4), 1–14. https://doi.org/10.14445/22315381/IJETT-V72I4P101
5. Hassija, V., Zeadally, S., Jain, I., Tahiliani, A., Chamola, V., & Gupta, S. (2021). Framework for determining the suitability of blockchain. Transactions on Emerging Telecommunications Technologies, 32(10), e4334. https://doi.org/10.1002/ett.4334
6. Aggarwal, S., & Kumar, N. (2021). Attacks on blockchain. In P. Raj (Ed.), Advances in computers (Vol. 121, pp. 399–410). Elsevier. https://doi.org/10.1016/bs.adcom.2020.08.020
7. Alachkar, K., & Gaastra, D. (2018). Blockchain-based Sybil attack mitigation: A case study of the I2P network. In Proceedings of the International Conference on Network Protocols (ICNP) (pp. 1–13).
8. Chaganti, R., Boppana, R. V., Ravi, V., Munir, K., Almutairi, M., Rustam, F., Lee, E., & Ashraf, I. (2022). Denial-of-service attacks in blockchain ecosystem: A review. IEEE Access, 10, 96538–96555. https://doi.org/10.1109/ACCESS.2022.3205019
9. Aghili, S. (2024). Leveraging blockchain technology: Governance, risk, compliance, security, and use cases. CRC Press. https://doi.org/10.1201/9781003462033
10. Heilman, E., Kendler, A., Zohar, A., & Goldberg, S. (2015). Eclipse attacks on Bitcoin's peer-to-peer network. In Proceedings of the 24th USENIX Security Symposium (pp. 129–144).
11. Marcus, Y., Heilman, E., & Goldberg, S. (2018). Low-resource eclipse attacks on Ethereum's peer-to-peer network. IACR Cryptology ePrint Archive. https://eprint.iacr.org/2018/236
12. Hryshchuk, R., Yevseiev, S., & Shmatko, A. (2018). Construction methodology of information security systems of banking information. Premier Publishing

13. Alasmary, W., Alhaidari, F., Alharthi, A., & Alsubhi, K. (2024). Malware trends: Detection and mitigation strategies. Journal of Cybersecurity and Digital Forensics, 6(1), 45–62. https://doi.org/10.1109/JCDF.2024.0006
14. Hadikosyah, G. A., Zannah, N. F., Yulistia, S., Febrian, M. R., Maulana, F., & Sulthan, R. (2026). Trojan malware propagation and impact. JIKUM: Jurnal Ilmu Komputer, 2(1), 47–52. https://doi.org/10.62671/jikum.v2i1.153
15. McElroy, S. (2024). Identifying Android banking malware through UI complexity. In IEEE International Conference on Cyber Security and Resilience (CSR) (pp. 348–353). https://doi.org/10.1109/CSR61664.2024.10679403
16. Reijonen, A. (2024). The evolution of mobile malware (Master's thesis, JAMK University). https://surl.lu/vicrdm
17. Zimperium Inc. (2025). 2025 global mobile threat report. https://surl.li/kzmhnq
18. The Hacker News. (2025). New Android Trojan Crocodilus abuses accessibility. https://thehackernews.com/2025/03/new-android-trojan-crocodilus-abuses.html
19. Rieck, K., Holz, T., Willems, C., Düssel, P., & Laskov, P. (2008). Malware behavior classification. In DIMVA 2008 (pp. 108–127). https://doi.org/10.1007/978-3-540-70542-0_6
20. Hryshchuk, R. (2021). Differential transformations in cybersecurity. In CEUR Workshop Proceedings (Vol. 3200, pp. 223–227).
21. Hryshchuk, R., & Korchenko, O. (2012). Differential game models of cyber attacks. Ukrainian Information Security Research Journal, (3), 115–122. https://doi.org/10.18372/2410-7840.14.3418
22. Myerson, R. B. (1991). Game theory: Analysis of conflict. Harvard University Press
23. Stifter, N., Judmayer, A., Schindler, P., Zamyatin, A., & Weippl, E. R. (2018). Formalization of Nakamoto consensus. IACR Cryptology ePrint Archive. https://eprint.iacr.org/2018/400
24. Liu, Z., Luong, N. C., Wang, W., Niyato, D., Wang, P., Liang, Y.-C., & Kim, D. I. (2019). Blockchain from game theory perspective. IEEE Access, 7, 47615–47643. https://doi.org/10.1109/ACCESS.2019.2909924
25. Zhang, Z. (2019). Engineering token economy. arXiv. https://doi.org/10.48550/arXiv.1907.00899
26. Zhang, Z., Zargham, M., & Preciado, V. M. (2020). Blockchain-enabled economic networks. Applied Network Science, 5, 19. https://doi.org/10.1007/s41109-020-0254-9
27. Wang, H., & An, J. (2023). Game-based blockchain security. The Journal of Supercomputing, 79, 15894–15926. https://doi.org/10.1007/s11227-023-05289-x
28. Zhiyong, L., Shuyi, W., Weiwei, S., Jiahui, L., & Jianming, W. (2023). Blockchain security situation awareness. Journal of China Universities of Posts and Telecommunications, 30(4), 105–120. https://doi.org/10.19682/j.cnki.1005-8885.2023.2020
29. Zhou, C., Xing, L., Liu, Q., & Wang, H. (2021). Bitcoin reliability under eclipse attacks. IJMEMS, 6(2), 480–492. https://doi.org/10.33889/IJMEMS.2021.6.2.029
30. Zhou, C., Xing, L., Guo, J., & Liu, Q. (2022). Bitcoin selfish mining analysis. IJMEMS, 7(1), 16–27.
31. Zhou, C., Xing, L., Liu, Q., & Li, Y. (2023). Bitcoin dependability under attacks. IJMEMS, 8(4), 547–559.
32. Zhou, C., Xing, L., Liu, Q., & Wang, H. (2023). Defense strategies for selfish mining. Applied Sciences, 13(1), 422. https://doi.org/10.3390/app13010422
33. del Rey, A. M. (2015). Malware propagation modeling. Security and Communication Networks, 8(15), 2561–2579. https://doi.org/10.1002/sec.1186
34. Karyotis, V., & Khouzani, M. (2016). Malware diffusion models. Morgan Kaufmann
35. Liu, Q. (2021). Security risk assessment (Doctoral dissertation). https://doi.org/10.62791/19801
36. Fang, Z., Zhao, P., Xu, M., Xu, S., Hu, T., & Fang, X. (2022). Statistical malware modeling. Journal of Applied Statistics, 49(4), 858–883.
37. Signes-Pont, M. T., Castillo, A. C., Mora, H. M., & Szymanski, J. (2018). Mobile malware propagation. Computers & Security. https://doi.org/10.1016/j.cose.2018.08.004
38. Quiroga-Sánchez, L., Montoya, G., & Lozano-Garzon, C. (2025). Malware propagation in IoT. Cybersecurity, 8, 2.
39. Pappu, K., et al. (2025). Malware propagation dynamics. arXiv.
40. Omar, O. A. M., et al. (2025). Malware propagation in cloud systems. Mathematics and Computers in Applications, 30(1), 8.
41. Zhou, Y., et al. (2023). Epidemic models for malware. Frontiers in Physics, 11, 1198410.
42. Hryshchuk, R. V. (2010). Theoretical foundations of cyber attack modeling. Ruta
43. Pukhov, G. E. (1978). Differential transformations. Cybernetics and Systems Analysis, 14, 383–390
44. Stasiuk, O. I., & Baranov, H. V. (2006). Differential transformations for computer modeling.

45. ISO/IEC. (2022). Information security risk management (ISO/IEC 27005:2022). https://www.iso.org/standard/80585.html
46. Maplesoft. (2025). Maple for students. https://www.maplesoft.com/products/Maple/student.aspx

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023

Olha Hryshchuk
PhD, Lieutenant Colonel
Officer of the National Defence University of Ukraine
National Defence University of Ukraine, Kyiv, Ukraine
ORCID: 0000-0001-6957-4748
Hry.Olga@gmail.com

Ruslan Hryshchuk
Laureate of the Borys Paton National Prize of Ukraine
Honored Science and Technology Figure of Ukraine
DSc (Engineering), Professor, Colonel
Deputy Commandant of the Odesa Military Academy
Odesa Military Academy, Odesa, Ukraine
ORCID: 0000-0001-9985-8477
Prof.Hry@gmail.com

EVALUATION OF BLOCKCHAIN NODE SECURITY AGAINST ECLIPSE ATTACKS AND TROJAN MALWARE USING DIFFERENTIAL GAME MODELS

Abstract. Blockchain technology is a modern breakthrough in information systems. It has significantly influenced the banking sector by transforming classical approaches to financial transactions, where banks acted as mandatory intermediaries. Today, blockchain has become a foundation of the digital economy. It is also applied in defense and social domains. The high market value of blockchain assets, such as tokens and cryptocurrencies, has recently attracted strong interest from both governmental actors (often from sanctioned states) and non-governmental cyber groups, as well as individual hackers seeking illegal profit. To achieve this, they conduct cyberattacks against blockchain nodes and entire networks. Attempts to infect blockchain systems with malicious software are also common. This article focuses on evaluating the security of blockchain nodes against Eclipse attacks and Trojan malware. The study applies differential game models based on Markov chains. This approach allows formalizing the probabilities of blockchain node states under the influence of Eclipse Attacks and Trojan Malware using Kolmogorov-Chapman differential equations. To obtain analytical and numerical estimates of security levels, the article employs a differential game method based on non-Taylor differential transformations developed by academician G. Pukhov. The novelty of the results lies in advancing mechanisms of blockchain cybersecurity by selecting optimal defense strategies for nodes exposed to Eclipse Attacks or Trojan Malware. The obtained security estimates provide a scientific basis for practical recommendations on protecting blockchain technology from other dangerous types of cyberattacks and malicious software.

Keywords: blockchain node; security level; Eclipse Attack; Trojan Malware; model; cybersecurity; differential game; differential transformations.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Guo, H., & Yu, X. (2022). A survey on blockchain technology and its security. Blockchain: Research and Applications, 3(2), 100067. https://doi.org/10.1016/j.bcra.2022.100067
2. Pessa, A. A. B., Perc, M., & Ribeiro, H. V. (2023). Age and market capitalization drive large price variations of cryptocurrencies. Scientific Reports, 13, 3351. https://doi.org/10.1038/s41598-023-30431-3
3. Krause, D. S. (2025). The $1.4 billion Bybit hack: Cybersecurity failures and the risks of cryptocurrency deregulation. International Journal of Cryptocurrency Research, 5(1), 52–62. https://doi.org/10.51483/IJCCR.5.1.2025.52-62
4. Barj, S., & Youjil, A. (2024). Blockchain and cryptocurrency security from a layered perspective using MITRE ATT&CK. International Journal of Engineering Trends and Technology, 72(4), 1–14. https://doi.org/10.14445/22315381/IJETT-V72I4P101

5. Hassija, V., Zeadally, S., Jain, I., Tahiliani, A., Chamola, V., & Gupta, S. (2021). Framework for determining the suitability of blockchain. Transactions on Emerging Telecommunications Technologies, 32(10), e4334. https://doi.org/10.1002/ett.4334
6. Aggarwal, S., & Kumar, N. (2021). Attacks on blockchain. In P. Raj (Ed.), Advances in computers (Vol. 121, pp. 399–410). Elsevier. https://doi.org/10.1016/bs.adcom.2020.08.020
7. Alachkar, K., & Gaastra, D. (2018). Blockchain-based Sybil attack mitigation: A case study of the I2P network. In Proceedings of the International Conference on Network Protocols (ICNP) (pp. 1–13).
8. Chaganti, R., Boppana, R. V., Ravi, V., Munir, K., Almutairi, M., Rustam, F., Lee, E., & Ashraf, I. (2022). Denial-of-service attacks in blockchain ecosystem: A review. IEEE Access, 10, 96538–96555. https://doi.org/10.1109/ACCESS.2022.3205019
9. Aghili, S. (2024). Leveraging blockchain technology: Governance, risk, compliance, security, and use cases. CRC Press. https://doi.org/10.1201/9781003462033
10. Heilman, E., Kendler, A., Zohar, A., & Goldberg, S. (2015). Eclipse attacks on Bitcoin's peer-to-peer network. In Proceedings of the 24th USENIX Security Symposium (pp. 129–144).
11. Marcus, Y., Heilman, E., & Goldberg, S. (2018). Low-resource eclipse attacks on Ethereum's peer-to-peer network. IACR Cryptology ePrint Archive. https://eprint.iacr.org/2018/236
12. Hryshchuk, R., Yevseiev, S., & Shmatko, A. (2018). Construction methodology of information security systems of banking information. Premier Publishing
13. Alasmary, W., Alhaidari, F., Alharthi, A., & Alsubhi, K. (2024). Malware trends: Detection and mitigation strategies. Journal of Cybersecurity and Digital Forensics, 6(1), 45–62. https://doi.org/10.1109/JCDF.2024.0006
14. Hadikosyah, G. A., Zannah, N. F., Yulistia, S., Febrian, M. R., Maulana, F., & Sulthan, R. (2026). Trojan malware propagation and impact. JIKUM: Jurnal Ilmu Komputer, 2(1), 47–52. https://doi.org/10.62671/jikum.v2i1.153
15. McElroy, S. (2024). Identifying Android banking malware through UI complexity. In IEEE International Conference on Cyber Security and Resilience (CSR) (pp. 348–353). https://doi.org/10.1109/CSR61664.2024.10679403
16. Reijonen, A. (2024). The evolution of mobile malware (Master's thesis, JAMK University). https://surl.lu/vicrdm
17. Zimperium Inc. (2025). 2025 global mobile threat report. https://surl.li/kzmhnq
18. The Hacker News. (2025). New Android Trojan Crocodilus abuses accessibility. https://thehackernews.com/2025/03/new-android-trojan-crocodilus-abuses.html
19. Rieck, K., Holz, T., Willems, C., Düssel, P., & Laskov, P. (2008). Malware behavior classification. In DIMVA 2008 (pp. 108–127). https://doi.org/10.1007/978-3-540-70542-0_6
20. Hryshchuk, R. (2021). Differential transformations in cybersecurity. In CEUR Workshop Proceedings (Vol. 3200, pp. 223–227).
21. Hryshchuk, R., & Korchenko, O. (2012). Differential game models of cyber attacks. Ukrainian Information Security Research Journal, (3), 115–122. https://doi.org/10.18372/2410-7840.14.3418
22. Myerson, R. B. (1991). Game theory: Analysis of conflict. Harvard University Press
23. Stifter, N., Judmayer, A., Schindler, P., Zamyatin, A., & Weippl, E. R. (2018). Formalization of Nakamoto consensus. IACR Cryptology ePrint Archive. https://eprint.iacr.org/2018/400
24. Liu, Z., Luong, N. C., Wang, W., Niyato, D., Wang, P., Liang, Y.-C., & Kim, D. I. (2019). Blockchain from game theory perspective. IEEE Access, 7, 47615–47643. https://doi.org/10.1109/ACCESS.2019.2909924
25. Zhang, Z. (2019). Engineering token economy. arXiv. https://doi.org/10.48550/arXiv.1907.00899
26. Zhang, Z., Zargham, M., & Preciado, V. M. (2020). Blockchain-enabled economic networks. Applied Network Science, 5, 19. https://doi.org/10.1007/s41109-020-0254-9
27. Wang, H., & An, J. (2023). Game-based blockchain security. The Journal of Supercomputing, 79, 15894–15926. https://doi.org/10.1007/s11227-023-05289-x
28. Zhiyong, L., Shuyi, W., Weiwei, S., Jiahui, L., & Jianming, W. (2023). Blockchain security situation awareness. Journal of China Universities of Posts and Telecommunications, 30(4), 105–120. https://doi.org/10.19682/j.cnki.1005-8885.2023.2020
29. Zhou, C., Xing, L., Liu, Q., & Wang, H. (2021). Bitcoin reliability under eclipse attacks. IJMEMS, 6(2), 480–492. https://doi.org/10.33889/IJMEMS.2021.6.2.029
30. Zhou, C., Xing, L., Guo, J., & Liu, Q. (2022). Bitcoin selfish mining analysis. IJMEMS, 7(1), 16–27.
31. Zhou, C., Xing, L., Liu, Q., & Li, Y. (2023). Bitcoin dependability under attacks. IJMEMS, 8(4), 547–559.

32. Zhou, C., Xing, L., Liu, Q., & Wang, H. (2023). Defense strategies for selfish mining. Applied Sciences, 13(1), 422. https://doi.org/10.3390/app13010422
33. del Rey, A. M. (2015). Malware propagation modeling. Security and Communication Networks, 8(15), 2561–2579. https://doi.org/10.1002/sec.1186
34. Karyotis, V., & Khouzani, M. (2016). Malware diffusion models. Morgan Kaufmann
35. Liu, Q. (2021). Security risk assessment (Doctoral dissertation). https://doi.org/10.62791/19801
36. Fang, Z., Zhao, P., Xu, M., Xu, S., Hu, T., & Fang, X. (2022). Statistical malware modeling. Journal of Applied Statistics, 49(4), 858–883.
37. Signes-Pont, M. T., Castillo, A. C., Mora, H. M., & Szymanski, J. (2018). Mobile malware propagation. Computers & Security. https://doi.org/10.1016/j.cose.2018.08.004
38. Quiroga-Sánchez, L., Montoya, G., & Lozano-Garzon, C. (2025). Malware propagation in IoT. Cybersecurity, 8, 2.
39. Pappu, K., et al. (2025). Malware propagation dynamics. arXiv.
40. Omar, O. A. M., et al. (2025). Malware propagation in cloud systems. Mathematics and Computers in Applications, 30(1), 8.
41. Zhou, Y., et al. (2023). Epidemic models for malware. Frontiers in Physics, 11, 1198410.
42. Hryshchuk, R. V. (2010). Theoretical foundations of cyber attack modeling. Ruta
43. Pukhov, G. E. (1978). Differential transformations. Cybernetics and Systems Analysis, 14, 383–390
44. Stasiuk, O. I., & Baranov, H. V. (2006). Differential transformations for computer modeling.
45. ISO/IEC. (2022). Information security risk management (ISO/IEC 27005:2022). https://www.iso.org/standard/80585.html
46. Maplesoft. (2025). Maple for students. https://www.maplesoft.com/products/Maple/student.aspx

Отримано редакцією журналу / Received: 21.01.26
Прорецензовано / Revised: 15.02.26
Схвалено до друку / Accepted: 26.03.26