КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (27), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.27.714
УДК 004.056.5:005.8:336.74

Чикрій Аркадій Олексійович
доктор фізико-математичних наук, професор,
академік НАН України, завідуючий відділом
Інститут кібернетики імені. В.М. Глушкова НАН України, Київ, Україна
ORCID ID: 0000-0001-9665-9085
g.chikrii@gmail.com

Мартинюк Ігор Петрович
аспірант кафедри інженерії програмного забезпечення та кібербезпеки
Державний торговельно-економічний університет, Київ, Україна
ORCID ID: 0009-0005-2815-1104
i.p.martyniuk@gmail.com

Десятко Альона Миколаївна
PhD, доцент, доцент кафедри інженерії програмного забезпечення та кібербезпеки
Державний торговельно-економічний університет, Київ, Україна
ORCID ID: 0000-0002-2284-3418
desyatko@gmail.com

Малюкова Інна Володимирівна
провідний аналітик
рейтингове агентство «Експерт-Рейтинг», Київ, Україна
ORCID ID: 0000-0002-7207-539X
imalyukova82@gmail.com

Ширшов Роман Анатолійович
науковий співробітник
Національна академія Служби безпеки України, Київ, Україна
ORCID ID: 0000-0003-3534-8736
signorum@gmail.com

АКТУАЛЬНІСТЬ СТВОРЕННЯ ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ ЗАХИСТУ ЦИФРОВИХ ВАЛЮТ З НИЗЬКИМ ХЕШРЕЙТОМ

Анотація. Останніми роками цифрові валюти (ЦВ) або криптовалюти стрімко інтегруються у фінансові системи багатьох держав завдяки своїй децентралізованій структурі та високій анонімності. Проте їхня популярність породжує множину вразливостей, пов'язаних із безпекою, особливо для валют із низьким хешрейтом. Хешрейт, як міра обчислювальної потужності мережі, відіграє ключову роль у захисті блокчейна від атак, таких як атака 51%. Відповідно, зі збільшенням кіберзагроз і шахрайства виникає необхідність розроблення адаптивних систем захисту, що враховують унікальні характеристики мережевої інфраструктури цифрових валют (ЦВ). Зростаюча популярність ЦВ серед широких мас і великих фінансових установ привертає увагу зловмисників, насамперед хакерів, що робить ці цифрові активи привабливими мішенями для атак. У цій статті представлено комп'ютерну реалізацію моделі протистояння атакам 51% в умовах нечіткої інформації, з акцентом на фінансовий аспект взаємодії сторін. Модель ґрунтується на динаміці фінансових станів гравців, які захищаються та атакують, описаній через систему диференціальних рівнянь, розроблених професорами В.П. Малюковим і В.А. Лахно. Під час імітаційного експерименту аналізувалися різні співвідношення параметрів, що визначають процес протистояння атакам 51%, враховуючи стратегії обох сторін. Результати експерименту дали змогу виявити множину областей переваги першого гравця, роль якого може виконувати сторона захисту, наприклад, криптовалютної біржі (КВБ). Представлені результати візуалізовано у вигляді гіперплощин у тривимірному просторі, що дало змогу наочно відобразити зони переважності учасників гри залежно від їхніх стратегій і доступних фінансових ресурсів. Дослідження підкреслює важливість адаптації захисних заходів в умовах швидко мінливого цифрового

фінансового ландшафту, а також акцентує увагу на необхідності нових досліджень зі створення інтелектуальних систем для захисту ЦВ з низьким хешрейтом.

Ключові слова: цифрові валюти; криптовалютна біржа; хешрейт; атака; інтелектуальна система; захист.

ВСТУП

Останніми роками спостерігається стрімкий розвиток та інтеграція цифрових валют (ЦВ) або криптовалют у фінансову систему, що зумовлено їхніми унікальними характеристиками, такими як децентралізація та високий ступінь анонімності [1], [2]. Однак, незважаючи на їхню популярність, існує низка вразливостей, пов'язаних із безпекою, особливо для валют із низьким хешрейтом.

Хешрейт, як міра обчислювальної потужності мережі, безпосередньо впливає на захищеність блокчейна від атак, таких як атака 51%. В умовах зростаючої загрози кіберзлочинів і шахрайства виникає потреба в розробленні інтелектуальних систем, здатних адаптивно захищати цифрові валюти, з огляду на специфічні характеристики їхньої мережевої інфраструктури.

Зі збільшенням популярності ЦВ серед широкої аудиторії та великих фінансових установ також спостерігається зростання інтересу до цієї галузі з боку хакерів. Цифрові валюти стають дедалі ціннішими активами, що робить їх привабливими мішенями для зловмисників. Останніми роками зафіксовано велику кількість випадків злому криптовалютних бірж (КВБ), криптогаманців та інших компонентів інфраструктури, що призвело до значних фінансових втрат. Наприклад, атаки на Mt. Gox, Bitfinex і Coincheck обернулися втратою сотень мільйонів доларів [3], [4].

Атака 51% являє собою загрозу, за якої зловмисник або група зловмисників контролюють понад 50% обчислювальних потужностей мережі [5]. Це дає можливість атакувальникам змінювати послідовність транзакцій, блокувати підтвердження нових операцій і здійснювати подвійне витрачання коштів. Розгляд атаки 51% як певної ігрової моделі з використанням фінансових ресурсів (ФР) учасників видається перспективним, тому що дає змогу глибше зрозуміти економічні аспекти безпеки блокчейн-мереж і розробляти ефективні стратегії захисту, які сприятимуть стійкості криптовалютних систем до подібних атак.

У рамках теорії ігор обидві сторони можуть аналізувати стратегії одна одної та прогнозувати дії опонента. Мета кожної зі сторін полягає в максимізації своєї вигоди та мінімізації втрат. Ігрову модель можна подати у вигляді матриці виплат, де різні комбінації стратегій призводять до різних результатів. Аналіз цієї матриці дає змогу визначити рівновагу Неша, за якої жодна сторона не має стимулу відхилятися від своєї стратегії, якщо противник дотримується своєї.

Ключовими стратегіями для атакуючої сторони можуть бути:

- вкладення фінансових ресурсів у збільшення обчислювальних потужностей (ASIC-майнери, GPU тощо) для отримання контролю над більш ніж 51% хешрейту мережі;
- придбання або оренда наявних майнінгових ферм для швидкого нарощування хешрейту;
- узгодження дій з іншими великими майнерами для об'єднання потужностей і спільної атаки;
- пошук дешевих джерел енергії та обладнання для майнінгу з метою максимізації хешрейту за мінімальних витрат.

Основні стратегії захисної сторони можуть включати:

- розподіл майнінгових потужностей серед більшої кількості учасників для зменшення ймовірності контролю над 51% хешрейту;
- створення фінансових стимулів для майнерів, щоб вони залишалися чесними;
- перехід на більш стійкі до атак алгоритми консенсусу, такі як Proof-of-Stake (PoS) і Proof-of-Elapsed Time (PoET);
- введення технічних і економічних бар'єрів для атаки, таких як уповільнення випуску блоків у разі підозри на атаку;
- формування коаліцій серед чесних майнерів для спільного захисту від атак;
- створення резервних фондів для компенсації збитків у разі атаки.

Залежно від обставин як атакуюча, так і захисна сторони можуть розробляти додаткові стратегії або комбінувати наявні. Наприклад, атакуючі можуть диверсифікувати свої вкладення в різні види обладнання, а захисники — впроваджувати освітні програми для підвищення обізнаності майнерів про ризики.

Для розуміння динаміки атаки 51% і розроблення ефективних стратегій захисту доцільно використовувати теорію ігор, адже в блокчейн-мережах взаємодіють учасники з різними інтересами і стратегіями. Атакуючі прагнуть максимізувати свої вигоди, захоплюючи контроль над мережею, тоді як захисники працюють над запобіганням цьому та збереженням цілісності мережі. Теорія ігор дає змогу моделювати ці взаємодії, враховуючи, як конфлікти, так і співпрацю, з акцентом на фінансові ресурси, які можуть використовувати обидві сторони для реалізації своїх стратегій.

У рамках ігрової моделі можна розглянути деяку множину стратегій, доступних як атакувальникам, так і захисникам, беручи до уваги їхні фінансові можливості. Це включає інвестиції в обчислювальні потужності, створення альянсів, застосування різних алгоритмів консенсусу та інші заходи. Пропонована модель дасть змогу оцінити ефективність різних стратегій із погляду витрат і потенційних вигод, а також виявити оптимальні стратегії для кожної сторони, що зрештою посприяє обґрунтованому ухваленню рішень і розробленню ефективніших заходів захисту.

Атака 51% не є лише технічною проблемою, оскільки вона зачіпає також економічні та соціальні аспекти. Теорія ігор враховує вартість ресурсів, мотивацію учасників, ризики та вигоди, що сприяє комплексному аналізу проблеми і є важливим для розроблення довгострокових стійких стратегій захисту, які враховують технічні, економічні та соціальні чинники. Ігрові моделі легко адаптуються до змін умов і параметрів системи, що дає змогу моделювати різні сценарії та враховувати нові загрози, що робить цей підхід гнучким і актуальним у швидко мінливому світі ЦВ і блокчейн-технологій.

Таким чином, використання ігрової моделі для аналізу атаки 51% дасть змогу всебічно оцінити загрозу, розробити оптимальні стратегії захисту і підтримувати стійкість блокчейн-мереж, з акцентом на взаємодію фінансових ресурсів атакувальників і захисників з огляду на складне поєднання технічних, економічних і соціальних чинників. Усе вищесказане підкреслює актуальність роботи та наш інтерес до цього дослідницького завдання.

Постановка проблеми. Важливим практичним завданням є комп'ютерна реалізація ігрової моделі протистояння атакам 51% в умовах нечіткої інформації, що акцентує увагу на фінансовому аспекті такого протистояння сторін, реалізованого за допомогою експерименту імітаційного моделювання. Графічне представлення в тривимірному просторі направлена на ілюстрацію межі області переважності першого гравця, тобто захист від атаки 51%, при цьому важливо акцентувати на адаптації захисних заходів в умовах мінливого цифрового фінансового ландшафту.

Аналіз останніх досліджень і публікацій. Досить детально вплив кібератак на ринок криптовалют було дано в роботі [6]. Основна увага приділяється двом аспектам: ризику закриття КВБ і впливу кібератак на вартість біткойна. Автор досліджує фактори, що сприяють закриттю КВБ, використовуючи передбачувальні моделі, та аналізує, як кібератаки впливають на прибутковість біткойна. Результати показують, що кібератаки можуть призвести до значного зниження ціни біткойна, що підкреслює важливість кібербезпеки (далі КБ) для стійкості криптовалютних ринків.

У [7] аналізуються важливі атрибути мережі біткойна у світлі потенційної загрози атаки 51%, а також пропонуються контрзаходи для запобігання такій атаці. Автори наголошують, що атака 51% характерна для блокчейнів, які використовують алгоритм Proof-of-Work, і для біткойна здійснення такої атаки є малоймовірним через потребу величезного обсягу обчислювальної потужності, який перевищить потужність решти мережі.

У [8] розглядається можливість подвійного витрачання (double spending) у мережі біткойн, яке здійснюється за допомогою атаки 51%. Автор аналізує, як зловмисник, який володіє більшою частиною обчислювальних потужностей мережі (понад 50%), може маніпулювати блокчейном, щоб повторно витрачати одні й ті самі біткойни. Дослідження розглядає ймовірності успіху такої атаки і механізми захисту від неї, роблячи акцент на важливих аспектах безпеки мережі біткойн.

У [9] автори досліджують проектування блокчейнів із застосуванням теорії розв’язання винахідницьких задач (TRIZ). Розглядаються різні аспекти дизайну блокчейнів, включно з безпекою, продуктивністю та стійкістю до атак, таких як атака 51%. Робота пропонує інноваційні підходи та методи для поліпшення архітектури блокчейнів, здатних розв’язувати наявні проблеми та запобігати потенційним загрозам.

Багато авторів [7] – [9] доходять висновку, що атака 51% більш реалізована щодо відносно нових і невеликих ЦВ, таких як альткоїни, які характеризуються низьким хешрейтом. У таких мережах зловмиснику простіше зібрати або орендувати достатні обчислювальні потужності для контролю понад 50% хешрейту, що робить можливими атаки 51%. Це створює значні загрози безпеці для таких блокчейнів, на відміну від більших і усталених криптовалют, таких як біткойн, де атака 51% малоймовірна через високий хешрейт мережі.

У [10] автори досліджують реалізацію і наслідки атаки 51%, обговорюють слабкі місця в консенсусних протоколах блокчейн-мереж і пропонують кілька передових методів захисту. Зроблено висновок про те, що криптовалюти з низьким хешрейтом є більш уразливими для таких атак, оскільки витрати на атаку значно нижчі. Схожий висновок зроблено і [11]. Таким чином, ці роботи зачіпають і аналіз фінансових витрат на атаку 51%. Як і роботи [7] – [9], дослідження [10], [11] підтверджують, що для ЦВ з низьким хешрейтом імовірність успішної атаки 51% вища через менші витрати на виконання такої атаки. Водночас, для великих ЦВ, таких як Bitcoin, витрати на атаку 51% можуть досягати мільярдів доларів, що робить такі атаки вкрай малоймовірними без значних фінансових вкладень або державної підтримки. У той же час на сьогоднішній день існує велика кількість ЦВ з низьким хешрейтом, наприклад, Ravencoin (RVN), що використовує алгоритм майнінгу KawPow [12]. Зауважимо, що хешрейт Ravencoin значно нижчий, ніж у Litecoin, що робить його більш вразливим для атак 51%. Можна згадати і Beam (BEAM), приватну криптовалюту, що використовує алгоритм MimbleWimble [13]. Хешрейт Beam також відносно низький, що робить її потенційною мішенню для зловмисників. До цієї категорії можна віднести і Dogecoin (DOGE) [14]. Хоча хешрейт Dogecoin вищий, ніж у Ravencoin і Beam, він все ж залишається відносно

низьким порівняно з Bitcoin і Ethereum. Це робить Dogecoin більш вразливим для атак 51%, особливо якщо його ціна значно зросте [15]. Згадаємо також, Horizen (ZEN) [16] і Monero (XMR) [17], які потенційно можуть стати мішенями для атак 51%. Провідні компанії в галузі КБ поки що тільки почали формувати для себе новий ландшафт кіберзагроз, пов'язаних із ЦВ і КВБ. А творці КВБ поки що до кінця не готові інвестувати в КБ, віддаючи перевагу швидкому прибутку за угодами з ЦВ. Усе вище сказане і зумовило релевантність нових досліджень у напрямі розвитку нових методів і моделей оцінки фінансових ресурсів, які можуть бути спрямовані на реалізацію атаки 51% для нових ЦВ. Цей аспект вивчення проблематики, пов'язаної з ЦВ, викликає особливий інтерес у розрізі завдань дослідження. І, відповідно, заслуговує на всебічне вивчення в рамках поточного дослідження.

Мета статті. Вивчення можливості реалізації на мовах високого рівня застосунків, що реалізують математичні моделі, які призначені для аналізу кібернетичної безпеки криптовалют із низьким хешрейтом і, відповідно, криптовалютних бірж, коли за умов нечіткої інформації відбувається протидія атаці 51 % при наявних фінансових ресурсах сторін подібної атаки.

МЕТОДИКА ДОСЛІДЖЕННЯ

За методику дослідження прийнято положення теорії ігор, а також результати досліджень, опублікованих у роботах [4], [18], [19]. Відповідно до цих робіт вважаємо, що для забезпечення кібербезпеки (КБ) цифрових валют (ЦВ) необхідне фінансове забезпечення. Або іншими словами фінансові ресурси (ФР). Сторона захисту ЦВ потребує ФР для виконання своїх завдань, таких як розподіл майнінгових потужностей серед більшої кількості учасників, створення фінансових стимулів для майнерів, перехід на стійкі до атак алгоритми консенсусу та інші заходи із забезпечення безпеки мережі. Атакуючій стороні ресурси також потрібні для розробки та реалізації атаки 51%, яка включає збільшення обчислювальних потужностей, оренду наявних майнінгових ферм, пошук дешевих джерел енергії та обладнання та інші подібні заходи. Взаємодію між двома сторонами протистояння — стороною, що захищається, та стороною, що атакує, — можна розглядати як гру з двома гравцями. Перший гравець — сторона захисту ЦВ. Другий гравець — сторона, що атакує ЦВ або криптовалютну біржу (КВБ).

Відповідно до праць [4], [18], [19] така взаємодія під час реалізації програми для імітаційного експерименту розглядалася з фінансової точки зору. Це справедливо, оскільки така взаємодія залежить від кореляції їхніх витрат на досягнення поставлених цілей. Взаємодія між гравцями відбувається безперервно в часі. Це підкреслює динамічний характер їхніх стратегій захисника й атакуючого. Протистояння відбувається так. Перший гравець має різні технологічні стратегії n (штук) для захисту від атаки 51%. Наприклад, такі стратегії включають розподіл майнінгових потужностей серед більшої кількості учасників, створення фінансових стимулів для майнерів, перехід на стійкі до атак алгоритми консенсусу, запровадження технічних бар'єрів для атак, розробку та впровадження систем моніторингу та попередження атак на ЦВ та/або КВБ, а також організацію кампаній з підвищення обізнаності серед учасників мережі. Другий гравець, навпаки, має свої стратегії m (штук) для здійснення атаки 51%. Ці стратегії можуть включати, наприклад, збільшення обчислювальних потужностей, оренду наявних майнінгових ферм, кооперацію з іншими великими майнерами, пошук дешевих джерел енергії та обладнання, проведення атак у моменти найменшої активності мережі,

а також використання вразливостей у програмному забезпеченні для управління майнінговими фермами. Застосування другим гравцем своїх стратегій веде до фінансових збитків першого гравця, і навпаки. Якщо витрати на захист від атаки 51% ефективні, атакуючий не досягає своїх цілей і зазнає збитків. Таким чином, результат протистояння залежить від того, чиї стратегії будуть більш ефективними і економічно виправданими в умовах поточної фінансової та технічної ситуації.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

В рамках наших міркувань, вважаємо, що i технологічна стратегія другого гравця, призводить до фінансових збитків першого гравця в розмірі χ_i^1. Тоді j технологічна стратегія першого гравця приносить йому фінансовий дохід у розмірі χ_j^2. Позначимо чере p_{ij}^1 відношення ω_j^2 / ω_i^1, а через p_{ij}^2 відношення ω_j^2 / ω_i^1. Якщо $\chi_i^1 = 0$ при деякому i або $\chi_j^2 = 0$ при деякому j, то такі стратегії виключаємо з розгляду.

Фінансові ресурси гравців у момент часу $t \in [0, +\infty)$ задовольняють такій системі диференціальних рівнянь [18], [19]:

$$\begin{aligned} d\alpha(t)/dt &= -\alpha(t) + K \cdot \alpha(t) - U(t) \cdot K \cdot \alpha(t) - \Theta \cdot P_2 \cdot V(t) \cdot N \cdot \beta^{\xi}(t); \\ d\beta^{\xi}(t)/dt &= -\beta(t) + N \cdot \beta^{\xi}(t) - V(t) \cdot N \cdot \beta^{\xi}(t) - \Xi \cdot P_1 \cdot U(t) \cdot K \cdot \alpha(t). \end{aligned} \quad (1)$$

В рамках даної статті ми не зупиняємося детально на розв’язанні цієї системи диференціальних рівнянь, оскільки розв’язання аналогічних задач, було детально розібрано в публікаціях проф. Малюкова В.П. та проф. Лахно В.А. [4], [18], [19], а лише наведемо опис програмної реалізації такої моделі.

Мета гри — аналіз витрат сторін на фінансування процесів захисту та атаки 51% з боку хакерів. Під час обчислювального експерименту ми оцінюємо ФР обох сторін і їхнє використання для різних стратегій: у захисників — на розподіл майнінгових потужностей, створення фінансових стимулів для майнерів і перехід на стійкі до атак алгоритми консенсусу; в атакувальників — на збільшення обчислювальних потужностей, оренду наявних майнінгових ферм та пошук дешевих джерел енергії й обладнання.

Модель реалізовано алгоритмічною мовою Python у середовищі програмування VS Code (див. рис. 1). Візуалізацію результатів гри представлено на рис. 2.

План експерименту включав такі етапи:

1. Визначити початкові стани гравців у тривимірному просторі та візуалізувати множину переваг першого гравця.
2. Побудувати гіперплощини різного кольору, що ілюструють межі області переважності першого гравця.
3. Визначити множину станів гравців (множину переважності першого гравця), яка розташована нижче гіперплощин у позитивному ортанті (ця множина має властивість, що якщо взаємодія починається з цих станів, то в першого гравця є стратегія, що приводить його до бажаного результату).
4. Знайти перетин гіперплощин і визначити промінь збалансованості, на якому стани гравців перебувають у рівновазі.
5. Провести аналіз витрат сторін на реалізацію своїх стратегій — для захисника: розподіл майнінгових потужностей, створення фінансових стимулів для майнерів, перехід на стійкі до атак алгоритми консенсусу. Для

ISSN 2663 - 4023

атакуючого: збільшення обчислювальних потужностей, оренда майнінгових ферм, пошук дешевих джерел енергії та обладнання.

6. Оцінити, наскільки ефективно гравці досягають своїх цілей за обраних стратегій, і проаналізувати траєкторії руху станів гравців щодо променя збалансованості.

```
import matplotlib.pyplot as plt
from mpl_toolkits.mplot3d import Axes3D


# Визначення функції правої частини системи рівнянь
def system(y, t, L1, L2, U, V):
    z, w = y[:M], y[M:]  # разделение вектора y на компоненты z и w
    dzdt = -z + L1 @ z - np.diag(U) @ (L1 @ z) - np.diag(V) @ (L2 @ w)
    dwdt = -w + L2 @ w - np.diag(V) @ (L2 @ w) - np.diag(U) @ (L1 @ z)
    return np.concatenate((dzdt, dwdt))


# Параметри системи
M = 3  # ккількість стратегій у кожного гравця

# Матриці перетворення ресурсів
L1 = np.array([[1.1, 0, 0], [0, 1.2, 0], [0, 0, 1.3]])
L2 = np.array([[1.0, 0, 0], [0, 1.1, 0], [0, 0, 1.2]])

# Інвестиційні стратегії гравців
U = np.array([0.1, 0.2, 0.3])
V = np.array([0.2, 0.1, 0.4])

# Початкові умови (фінансові ресурси гравців)
z0 = np.array([10, 15, 20]) # початкові ресурси захисника
w0 = np.array([8, 12, 18]) # початкові ресурси хакера
y0 = np.concatenate((z0, w0))

# Тимчасовий діапазон інтегрування
t = np.linspace(0, 10, 100)

# Розв'язання системи диференціальних рівнянь
solution = odeint(system, y0, t, args = (L1, L2, U, V))

# Побудова тривимірних графіків
fig = plt.figure()
ax = fig.add_subplot(111, projection='3d')
```

Рис. 1. Реалізація розв'язання системи диференціальних рівнянь у середовищі програмування VS Code

ISSN 2663 - 4023

Слід зазначити, що наша модель зосереджена виключно на фінансових аспектах протистояння атаці 51%. Ми не розглядаємо технічні деталі та реалізацію стратегій, як-от розробка і впровадження специфічного ПЗ, посилення обчислювальних потужностей, або створення нових алгоритмів консенсусу. Це обмеження моделі має на увазі, що результати нашого аналізу мають бути доповнені технічними дослідженнями для комплексного розуміння і забезпечення кібербезпеки ЦВ і КВБ.

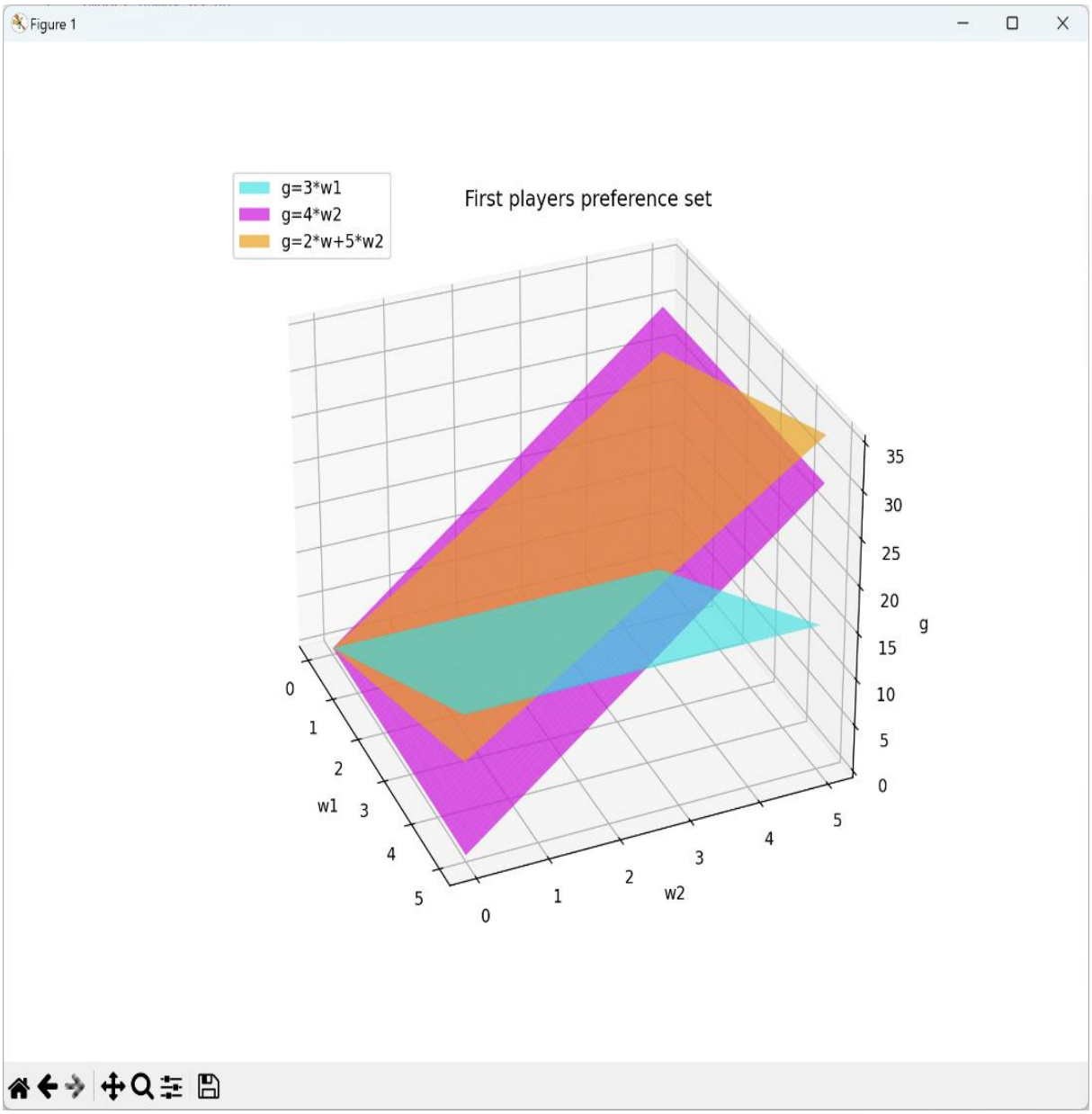

Рис. 2. Множина переважності першого гравця

На рис. 2 змінні $w1$ і $w2$ — фінансові ресурси сторони захисту в умовних одиницях на реалізацію своїх стратегій захисту, які були описані вище. Відповідно Delta — ФР атакуючої сторони, які вона витрачає в рамках своїх стратегій з подолання захисних контурів КВБ.

Множину переважності першого гравця зображено в тривимірному просторі. Вона являє собою множину станів гравців, які перебувають у тривимірному позитивному

ортанті тривимірного простору і які знаходяться «під гіперплощинами» різного кольору. Перетин гіперплощин ілюструє межі області переваги першого гравця. Крім того, перетин цих трьох гіперплощин дає змогу визначити промені збалансованості, тобто, при знаходженні станів гравців на таких променях у гравців існують стратегії, за застосування яких траєкторія руху гравців залишатиметься на цих променях як завгодно довго.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У роботі представлено комп'ютерну реалізацію ігрової моделі протистояння атакам 51% в умовах нечіткої інформації, що акцентує увагу на фінансовому аспекті такого протистояння сторін. Модель ґрунтується на припущенні, що динаміка фінансових станів, гравця, який захищається від атак 51%, та гравця, який атакує, описується системою диференціальних рівнянь, представлених у роботах проф. Малюкова В.П. і проф. Лахна В.А., що моделюють зміну багатовимірних змінних.

Наведено результати імітаційного експерименту, під час якого аналізувалися різні співвідношення параметрів, що характеризують процес протистояння атакам 51%. Експеримент дав змогу отримати множину переважності першого гравця. Вона зображена в тривимірному просторі. При цьому перетин гіперплощин ілюструє межі області переважності першого гравця, тобто захист від атаки 51%.

Дослідження підкреслює важливість адаптації захисних заходів в умовах цифрового фінансового ландшафту, що швидко змінюється, а також акцентує увагу на необхідності нових досліджень зі створення інтелектуальних систем для захисту ЦВ з низьким хешрейтом.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Чубенко, В. Ю. (2023). Вплив криптовалют на фінансову безпеку країни. *Збірник наукових праць Державного податкового університету, (1),* 188–204. https://doi.org/10.33244/2617-5940.1.2022.188-204
2. Слобода, Л., & Родіонова, Е. (2021). ІНВЕСТИЦІЙНІ РІШЕННЯ НА РИНКУ КРИПТОВАЛЮТ ТА ЇХНІЙ ВПЛИВ НА ФІНАНСОВУ БЕЗПЕКУ КРАЇНИ. *Socio-Economic Relations in the Digital Society, 1(40),* 25–33. https://doi.org/10.18371/2221-755X1(40)2021237576
3. Гребельний, А. (2024). КІБЕРРИЗИКИ НА КРИПТОВАЛЮТНИХ БІРЖАХ: ПРИЧИНИ, НАСЛІДКИ ТА ЇХ МІНІМІЗАЦІЯ. *Modern Engineering and Innovative Technologies, 1(34–01),* 106–113. https://doi.org/10.30890/2567-5273.2024-34-00-036
4. Лахно, В., Малюков, В., Малюкова, І., Аткелди, О., Криворучко, О., Десятко, А., & Степашкіна, К. (2023). МОДЕЛЬ АНАЛІЗУ СТРАТЕГІЙ ПРИ ДИНАМІЧНІЙ ВЗАЄМОДІЇ УЧАСНИКІВ ФІШИНГОВИХ АТАК. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(20),* 124–141. https://doi.org/10.28925/2663-4023.2023.20.124141
5. Гаврилова А. (2019). Аналіз стану захищеності бкокчейн-проектів на ринку українських сервісів. *Інтелектуальні системи та інформаційні технології,* 62–64.
6. Lee, S. A. (2022). *Investigating the Impact of Cyber Security Attacks on Cryptocurrency Markets* [Macquarie University]. https://doi.org/https://doi.org/10.25949/21598905.v1
7. Baruwa, Z., Bhattacherjee, S., Chandnani, S.R., & Zhu, Z. (2023). Social Media Perceptions of 51% Attacks on Proof-of-Work Cryptocurrencies: A Natural Language Processing Approach. *ArXiv, abs/2310.14307*.
8. Ramos, S., Pianese, F., Leach, T., & Oliveras, E. (2021). A great disturbance in the crypto: Understanding cryptocurrency returns under attacks, Blockchain. *Research and Applications, 2(3).* https://doi.org/10.1016/j.bcra.2021.100021

9. Kim, S. K., Yeun, C. Y., Damiani, E., & Al-Hammadi, Y. (2019). Various perspectives in new blockchain design by using theory of inventive problem solving. *In: IEEE International Conference on Blockchain and Cryptocurrency*.
10. Sayeed, S., & Marco-Gisbert, H. (2019). Assessing blockchain consensus and security mechanisms against the 51% attack. *Applied Sciences, 9(9)*. https://doi.org/10.3390/app9091788
11. Taylor, K. (2021). *What Happens in 51% Attacks? | CoinMarketCap*. CoinMarketCap Academy. https://coinmarketcap.com/academy/article/what-happens-in-51-attacks
12. Yi, X., Fang, Y., Wu, D., & Jiang, L. (2022). *BlockScope: Detecting and investigating propagated vulnerabilities in forked blockchain projects.* https://doi.org/10.14722/ndss.2023.24222
13. Shaikh, M., Munir, S., Wiil, U. K., & Shaikh, A. (2024). A Blockchain-Based Renewable Energy Authenticated Marketplace: BEAM of Flexibility. *Advances in Emerging Information and Communication Technology. ICIEICT 2023. Signals and Communication Technology. Springer, Cham*. https://doi.org/10.1007/978-3-031-53237-5_31
14. La Morgia, M., Mei, A., Sassi, F., & Stefa, J. (2023). The doge of wall street: Analysis and detection of pump and dump cryptocurrency manipulations. *ACM Transactions on Internet Technology, 23(1)*, 1–28. https://doi.org/10.1145/3561300
15. Lansiaux, E., Tchagaspanian, N., & Forget, J. (2022) Community Impact on a Cryptocurrency: Twitter Comparison Example Between Dogecoin and Litecoin. *Front. Blockchain, 5:829865*. https://doi.org/10.3389/fbloc.2022.829865
16. Hilmola, O.-P. (2021). On Prices of Privacy Coins and Bitcoin. *Journal of Risk and Financial Management, 14(8),* 361. https://doi.org/10.3390/jrfm14080361
17. Wang, Z., Li, X., Ruan, J., & Kou, J. (2019). Prediction of Cryptocurrency Price Dynamics with Multiple Machine Learning Techniques. *In Proceedings of the 2019 4th International Conference on Machine Learning Technologies (ICMLT '19). Association for Computing Machinery*. https://doi.org/10.1145/3340997.3341008
18. Lakhno, V., Malyukov, V., Malyukova, I., Akhmetov, B., Alimseitova, Z., & Ogan, A. (2024). A neuro-game model for analyzing strategies in the dynamic interaction of participants of phishing attacks. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*. http://doi.org/10.12928/telkomnika.v22i3.25938
19. Malyukov, V., Lakhno, V., Bebeshko, B., Malyukova, I., & Zhumadilova, M. (2023). Multifactor Model of the Digital Cryptocurrency Market as a Computational Core of the Information System. *CPITS II*, vol. 3550, 200–208.
20. Chikrii, A. A. (2013). *Conflict controlled processes*. Dordrecht. https://doi.org/10.1007/978-94-017-1135-7
21. Hulak, H. M., Zhiltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2024). *Information and cyber security of the enterprise. Textbook.* Lviv: Publisher Marchenko T. V.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (27), 2025
ISSN 2663 - 4023

Arkadii Chikrii
Doctor of Physical and Mathematical Sciences, Professor,
Academician of the National Academy of Sciences of Ukraine, Head of Department
Institute of Cybernetics named after. V.M. Glushkov Institute of
Cybernetics of the National Academy of Sciences of Ukraine, Kyiv, Ukraine
ORCID ID: 0000-0001-9665-9085
g.chikrii@gmail.com

Ihor Martyniuk
Doctor of Philosophy Degree Candidate,
Department of Software Engineeringand Cyber Security
State University of Trade and Economics, Kyiv, Ukraine
ORCID ID: 0009-0005-2815-1104
i.p.martyniuk@gmail.com

Alona Desiatko
PhD in Computer Sciences, Associate Professorof Department of
Software Engineeringand Cyber Security
State University of Trade and Economics, Kyiv, Ukraine
ORCID ID: 0000-0002-2284-3418
desyatko@gmail.com

Inna Malyukova
Lead Analyst
Rating agency “Expert-rating”, Kyiv, Ukraine
ORCID ID: 0000-0002-7207-539X
imalyukova82@gmail.com

Roman Shyrshov
Researcher
National Academy of Security Service of Ukraine, Kyiv, Ukraine
ORCID ID: 0000-0003-3534-8736
signorum@gmail.com

THE RELEVANCE OF CREATING AN INTELLIGENT SYSTEM FOR PROTECTION OF DIGITAL CURRENCIES WITH LOW HASHRATE

Abstract. In the modern digital world, where information technology is an integral part of life, cybersecurity issues are becoming increasingly relevant. One of the key aspects of protecting information systems is managing the attack surface, which includes all possible entry points for malicious actors. Forming and managing the attack surface is a complex task that requires constant attention and improvement. Malicious actors (“Threat actors”) play a crucial role in this process. They constantly seek new ways to penetrate systems, using various methods and techniques. These “actors” can vary in their origins and motivations: from cybercriminals seeking financial gain to state actors conducting espionage and sabotage activities. Understanding the types of “malicious actors” and their methods is essential for effective attack surface management. This understanding helps to timely detect and eliminate vulnerabilities, improve system and network configurations, and raise staff awareness of modern cyber threats. This article examines the key aspects of forming the attack surface, focusing on the role of “malicious actors”. It explores the types of “malicious actors”, their methods and techniques, and provides practical recommendations for reducing risks and improving the protection of information systems. Additionally, conducting regular security audits and implementing modern protection technologies such as intrusion detection systems, data encryption, and multi-factor authentication are important. Thus, a comprehensive approach to managing the attack surface, which includes understanding “Threat actors”, utilizing modern protection technologies, and continuously training personnel, is crucial for effectively protecting the information systems of critical infrastructure.

Keywords: malicious actor; threat actor; attack surface; critical infrastructure object (CIO); Internet of Things (IoT).

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Chubenko, V. Y. (2023). The influence of cryptocurrencies on the financial security of the country. *Collection of scientific papers of the University of the State Fiscal Service of Ukraine, (1),* 188–204. https://doi.org/10.33244/2617-5940.1.2022.188-204
2. Sloboda, L., & Rodionova, E. (2021). INVESTMENT DECISIONS ON THE CRYPTOCURRENCY MARKET AND THEIR IMPACT ON THE COUNTRY'S FINANCIAL SECURITY. *Socio-Economic Relations in the Digital Society*, *1(40)*, 25–33. https://doi.org/10.18371/2221-755X1(40)2021237576
3. Grebelny, A. (2024). CYBER RISKS ON CRYPTOCURRENCY EXCHANGES: CAUSES, CONSEQUENCES, AND THEIR MITIGATION. *Modern Engineering and Innovative Technologies*, *1(34–01)*, 106–113. https://doi.org/10.30890/2567-5273.2024-34-00-036
4. Lakhno, V., Malyukov, V., Malyukova, I., Atkeldi, O., Kryvoruchko, O., Desiatko, A., & Stepashkina, K. (2023). A MODEL OF STRATEGY ANALYSIS DURING THE DYNAMIC INTERACTION OF PHISHING ATTACK PARTICIPANTS. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*, *4(20)*, 124–141. https://doi.org/10.28925/2663-4023.2023.20.124141
5. Gavrylova, A. (2019). Analysis of the state of security of bccchain projects in the market of Ukrainian services. *Intelligent systems and information technologies*, 62–64.
6. Lee, S. A. (2022). *Investigating the Impact of Cyber Security Attacks on Cryptocurrency Markets* [Macquarie University]. https://doi.org/https://doi.org/10.25949/21598905.v1
7. Baruwa, Z., Bhattacherjee, S., Chandnani, S.R., & Zhu, Z. (2023). Social Media Perceptions of 51% Attacks on Proof-of-Work Cryptocurrencies: A Natural Language Processing Approach. *ArXiv*, *abs/2310.14307*.
8. Ramos, S., Pianese, F., Leach, T., & Oliveras, E. (2021). A great disturbance in the crypto: Understanding cryptocurrency returns under attacks, Blockchain. *Research and Applications*, *2(3).* https://doi.org/10.1016/j.bcra.2021.100021
9. Kim, S. K., Yeun, C. Y., Damiani, E., & Al-Hammadi, Y. (2019). Various perspectives in new blockchain design by using theory of inventive problem solving. *In: IEEE International Conference on Blockchain and Cryptocurrency*.
10. Sayeed, S., & Marco-Gisbert, H. (2019). Assessing blockchain consensus and security mechanisms against the 51% attack. *Applied Sciences*, *9(9)*. https://doi.org/10.3390/app9091788
11. Taylor, K. (2021). *What Happens in 51% Attacks? | CoinMarketCap*. CoinMarketCap Academy. https://coinmarketcap.com/academy/article/what-happens-in-51-attacks
12. Yi, X., Fang, Y., Wu, D., & Jiang, L. (2022). *BlockScope: Detecting and investigating propagated vulnerabilities in forked blockchain projects.* https://doi.org/10.14722/ndss.2023.24222
13. Shaikh, M., Munir, S., Wiil, U. K., & Shaikh, A. (2024). A Blockchain-Based Renewable Energy Authenticated Marketplace: BEAM of Flexibility. *Advances in Emerging Information and Communication Technology. ICIEICT 2023. Signals and Communication Technology. Springer, Cham*. https://doi.org/10.1007/978-3-031-53237-5_31
14. La Morgia, M., Mei, A., Sassi, F., & Stefa, J. (2023). The doge of wall street: Analysis and detection of pump and dump cryptocurrency manipulations. *ACM Transactions on Internet Technology*, *23(1)*, 1–28. https://doi.org/10.1145/3561300
15. Lansiaux, E., Tchagaspanian, N., & Forget, J. (2022) Community Impact on a Cryptocurrency: Twitter Comparison Example Between Dogecoin and Litecoin. *Front. Blockchain*, *5:829865*. https://doi.org/10.3389/fbloc.2022.829865
16. Hilmola, O.-P. (2021). On Prices of Privacy Coins and Bitcoin. *Journal of Risk and Financial Management*, *14(8)*, 361. https://doi.org/10.3390/jrfm14080361
17. Wang, Z., Li, X., Ruan, J., & Kou, J. (2019). Prediction of Cryptocurrency Price Dynamics with Multiple Machine Learning Techniques. *In Proceedings of the 2019 4th International Conference on Machine Learning Technologies (ICMLT '19). Association for Computing Machinery*. https://doi.org/10.1145/3340997.3341008
18. Lakhno, V., Malyukov, V., Malyukova, I., Akhmetov, B., Alimseitova, Z., & Ogan, A. (2024). A neuro-game model for analyzing strategies in the dynamic interaction of participants of phishing attacks. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*. http://doi.org/10.12928/telkomnika.v22i3.25938

19. Malyukov, V., Lakhno, V., Bebeshko, B., Malyukova, I., & Zhumadilova, M. (2023). Multifactor Model of the Digital Cryptocurrency Market as a Computational Core of the Information System. *CPITS II*, vol. 3550, 200–208.
20. Chikrii, A. A. (2013). *Conflict controlled processes*. Dordrecht. https://doi.org/10.1007/978-94-017-1135-7
21. Hulak, H. M., Zhiltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2024). *Information and cyber security of the enterprise. Textbook.* Lviv: Publisher Marchenko T. V.