НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

ІНСТИТУТ ПРОБЛЕМ МОДЕЛЮВАННЯ В ЕНЕРГЕТИЦІ ІМ. Г.Є. ПУХОВА

НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

«ВИКОРИСТАННЯ БЛОКЧЕЙН ТЕХНОЛОГІЙ В ЕНЕРГЕТИЦІ – 2025»

Збірник матеріалів конференції
26 березня 2025 р.

Київ – 2025

УДК 620.9 + 349 + 004 + 003.26

Рекомендовано до друку Вченою радою
Інституту проблем моделювання в енергетиці
ім. Г.Є. Пухова НАН України
(протокол № 3 від 27.03.2025)

Організаційний комітет:
В.В. Мохор, В.О. Артемчук та ін.

Програмний комітет:
В.В. Мохор, В.О. Артемчук та ін.

Відповідальний за випуск:
В.О. Артемчук

Usage of blockchain technologies in energetics – 2025: collection of materials of the scientific and practical conference, Kyiv, March 26, 2025, PIMEE of NAS of Ukraine. - 2025. - 84 p.

Використання блокчейн технологій в енергетиці – 2025 : збірник матеріалів науково-практичної конференції, м. Київ, 26 березня 2025 р., ІПМЕ ім. Г.Є. Пухова НАН України. – 2025. – 84 с.

ЗМІСТ

М.Ю. Кузнєцов, Л.В. Ковальчук, А.А. Шумська, І.М. Кузнєцов **ОБЧИСЛЕННЯ ІМОВІРНОСТІ АТАКИ РОЗГАЛУЖЕННЯ НА БЛОКЧЕЙН З ВИКОРИСТАННЯМ МЕТОДУ ПРИСКОРЕНОГО МОДЕЛЮВАННЯ** 5

Л.В. Ковальчук, М.С. Кондратенко **ВИЗНАЧЕННЯ КІЛЬКОСТІ БЛОКІВ ПІДТВЕРДЖЕННЯ У ДВОРІВНЕВОМУ БЛОКЧЕЙНІ З ПРОТОКОЛОМ КОНСЕНСУСУ PROOF-OF-PROOF ПРИ РІЗНИХ ТИПАХ КОНСЕНСУСУ У МЕЙНЧЕЙНІ/САЙДЧЕЙНІ ДЛЯ ЗАПОБІГАННЯ АТАКИ ПОДВІЙНОЇ ВИТРАТИ** 10

В.М. Горбачук, Т.О. Бардадим, М.С. Дунаєвський, В.В. Годлюк, Д.О. Рибачок **ОСНОВИ ДЕЦЕНТРАЛІЗОВАНИХ РИНКІВ ЕЛЕКТРОЕНЕРГІЇ** 15

З.Х. Борукаєв, В.А. Євдокімов, К.Б. Остапченко **КОНЦЕПТУАЛЬНА МОДЕЛЬ ОРГАНІЗАЦІЇ ДЕЦЕНТРАЛІЗОВАНОЇ ТОРГІВЛІ ЕЛЕКТРИЧНОЮ ЕНЕРГІЄЮ В УКРАЇНІ** 19

А.В. Полухін, В.А. Євдокімов, Я.П. Лукашевич **СМАРТ-КОНТРАКТИ НА ОСНОВІ БЛОКЧЕЙНУ ЯК ШЛЯХ ДО РОЗВИТКУ ДЕЦЕНТРАЛІЗОВАНОГО РИНКУ ЕЛЕКТРИЧНОЇ ЕНЕРГІЇ В УКРАЇНІ** 23

В.А. Євдокімов, Д.Р. Цвілій **КОНЦЕПТ ПОБУДОВИ ПЛАТФОРМИ ДЛЯ УКЛАДАННЯ P2P КОНТРАКТІВ НА РИНКУ ЕЛЕКТРИЧНОЇ ЕНЕРГІЇ УКРАЇНИ** 26

В.З. Чіхладзе, А.М. Кудін **ВИРІШЕННЯ ЗАДАЧІ БАЛАНСУВАННЯ КРИПТОВАЛЮТНОГО ПОРТФЕЛЮ В СЕРЕДОВИЩІ СМАРТ-КОНТРАКТІВ ТА DeFi** 30

І.А. Кудін **ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН, ДЛЯ ОБ'ЄДНАННЯ МАЛИХ ГОСПОДАРСТВ З МЕТОЮ P2P ТОРГІВЛІ ЕЛЕКТРОЕНЕРГІЄЮ ТА СПІЛЬНОГО ПРОДАЖУ ЕЛЕКТРОЕНЕРГІЇ ТРЕТІМ СТОРОНАМ** 31

О.С. Кушнір **МОДЕЛЬ БАЛАНСУЮЧИХ ТОРГІВ АКУМУЛЬОВАНОЇ ЕЛЕКТРИЧНОЇ ЕНЕРГІЇ ДЛЯ РОЗПОДІЛЕНИХ ЕНЕРГЕТИЧНИХ МЕРЕЖ** 32

С.В. Матвєєв, І.В. Івченко **БЛОКЧЕЙН-ТЕХНОЛОГІЇ ДЛЯ ОПТИМІЗАЦІЇ ЕНЕРГОСПОЖИВАННЯ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ** 35

Б.М. Плескач, В.Д. Самойлов, Є.В.Новак **ВИКОРИСТАННЯ БЛОК-ЧЕЙН ТЕХНОЛОГІЇ В ЛОКАЛЬНІЙ ЕЛЕКТРИЧНІЙ МЕРЕЖІ З МОДУЛЬНОЮ СОНЯЧНО-ВІТРЯНОЮ ЕЛЕКТРОСТАНЦІЄЮ** 37

Д.І. Симонов, Б.Ю. Заіка, Є.Д. Симонов **ВИКОРИСТАННЯ МАШИННОГО НАВЧАННЯ ДЛЯ ПІДВИЩЕННЯ БЕЗПЕКИ БЛОКЧЕЙН-ПРОЄКТІВ У СФЕРІ ЕНЕРГЕТИКИ**.....41

П.С. Чернишов, М.М. Ковальов **ЄCITY: БЛОКЧЕЙН-АРХІТЕКТУРА ЯК ОСНОВА ДЕЦЕНТРАЛІЗОВАНОГО УПРАВЛІННЯ ЕНЕРГОСПОЖИВАННЯМ ТА МОБІЛЬНІСТЮ У СМАРТ-МІСТАХ**.....45

К.В. Васильєв **МЕТОДИ КІБЕРЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЗА ДОПОМОГОЮ ШІ**.....47

A. Davydiuk, S. Kulyk **CLOUD DATA MIGRATION SECURITY**.....50

Я.Ю. Дорогий, В.В. Цуркан, В.Ю. Колісніченко **ПОКРАЩЕНИЙ МЕТОД ВИЯВЛЕННЯ ТА ІДЕНТИФІКАЦІЇ ВУЗЛІВ БЛОКЧЕЙН–МЕРЕЖІ ROOTSTOCK**.....56

Я.Ю. Дорогий, В.В. Цуркан, В.С. Кравчук **ТЕНЗОРНА МОДЕЛЬ ОЦІНКИ РЕЗУЛЬТАТИВНОСТІ ПЕНТЕСТУ НА РІЗНИХ ЕТАПАХ РОЗГОРТАННЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ**.....59

М.С. Дунаєвський **ІНФОРМАЦІЙНІ МОДЕЛІ ТОРГІВЛІ НА ВНУТРІШНЬОДОБОВИХ РИНКАХ ЕЛЕКТРОЕНЕРГІЇ**.....63

Н.В. Заїка, О.С. Верховець, М.Ю. Комаров, О.М. Дроботун **МЕТОДИ ОБФУСКАЦІЙНОГО ЗАХИСТУ ПЗ ДЛЯ КІБЕРБЕЗПЕКИ ОКІ**.....67

Є.О. Застьола, О.Б. Білоцерківський **РЕАЛІЗАЦІЯ БЛОКЧЕЙН-ПРОЕКТІВ У ЕНЕРГЕТИЧНОМУ СЕКТОРІ ТА СПЕКУЛЯЦІЇ НА КРИПТОВАЛЮТНИХ РИНКАХ ЯК ШЛЯХ ДО ФІНАНСОВОЇ НЕЗАЛЕЖНОСТІ ПІДПРИЄМЦЯ**.....70

Г.В. Неласа, О.В. Неласий, С.С. Самойлик **ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ СМАРТ-КОНТРАКТІВ В ДЕЦЕНТРАЛІЗОВАНИХ ЗАСТОСУНКАХ**.....72

В.О. Побережник, В.С. Балацька **КОНЦЕПЦІЯ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН ДЛЯ ПІДТВЕРДЖЕННЯ ЦІЛІСНОСТІ ТА АВТЕНТИЧНОСТІ ДАНИХ**.....75

А.О. Попова, О.М. Любименко, Н.О. Маслова, О.А. Штепа **БЕЗПЕКА СМАРТ-КОНТРАКТІВ: КОМПЛЕКСНИЙ ПІДХІД ДО ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ АТАКАМ**.....77

М.Б.Фесенко **КЛІЄНТ-СЕРВЕРНА АРХІТЕКТУРА ДОСТУПУ ДО БАЗИ ЗНАНЬ З ВИКОРИСТАННЯМ БЛОКЧЕЙН ТЕХНОЛОГІЇ**.....81

М.Ю. Кузнєцов, Л.В. Ковальчук, А.А. Шумська, І.М. Кузнєцов

ОБЧИСЛЕННЯ ІМОВІРНОСТІ АТАКИ РОЗГАЛУЖЕННЯ НА БЛОКЧЕЙН З ВИКОРИСТАННЯМ МЕТОДУ ПРИСКОРЕНОГО МОДЕЛЮВАННЯ

У цій роботі ми розглядаємо одну з найважливіших атак на блокчейн – так звану атаку розгалуження (Splitting Attack) [1]. Метою цієї атаки є створення невизначеності в мережі, коли лінійний блокчейн розщеплюється на дві гілки, з яких то одна, то інша вважається валідною. Така невизначеність створює проблеми з виконанням транзакцій, що неминуче знижує вартість відповідної криптовалюти. Це зниження зловмисник може використати для свого збагачення за наступним сценарієм: взяти кредит у цій криптовалюті; перевести отриману суму у фіатну валюту (наприклад, в долари); виконати атаку, внаслідок якої ціна криптовалюти суттєво знизиться; перевести частину доларів назад у відповідну криптовалюту і повернути борг, отримавши прибуток за рахунок падіння ціни.

На даний час не існує явних аналітичних формул для обчислення імовірності її успіху, що викликає певну недовіру до блокчейн-технологій. У даній роботі такий результат отримано для спрощеної (але все одно достатньо складної з математичної точки зору) моделі атаки розгалуження, коли зловмисник притримується певного чіткого алгоритму, який можна формалізувати і проаналізувати. У цій роботі отримано рекурентні формули, які дозволяють знаходити точні значення ймовірності того, що зловмисник зможе побудувати розгалуження заданої довжини. Ця ж імовірність оцінюється і методом Монте-Карло із заданими достовірністю та відносною похибкою.

У роботі [2] розглядалась спрощена модель, у якій ознакою початку розгалуження є поява послідовності 0–1–0 (символ "1" означає, що відповідний таймслот належить чесному слотлідеру, а "0" – зловмиснику). Якщо ж розглядати більш складні сценарії початку розгалуження, то застосування аналітичних чи асимптотичних формул для знаходження вказаної імовірності є дуже проблематичним, якщо взагалі можливим.

Ця робота узагальнює роботу [2] та пропонує більш загальний алгоритм, який зловмисник застосовує для початку розгалуження. Для обчислення вказаної ймовірності застосовується прискорене моделювання, яке використовує як елементи стандартного методу Монте-Карло, так і рекурентні формули.

Модель атаки розгалуження

Як і в роботі [2], будемо розглядати модель зловмисника, у якій його дії описуються простими правилами:

- у випадку наявності двох гілок різної довжини зловмисник під час свого таймслоту продовжує коротшу;

- у випадку наявності двох гілок однакової довжини зловмисник продовжує обидві, створюючи два блоки під час одного свого таймслоту;
- у випадку відсутності можливості створити або продовжити розгалуження поведінка зловмисника може бути довільною.

Розглянемо випадкову послідовність $\overline{\xi} = (\xi_1, \ldots, \xi_n)$ фіксованої довжини n, яка характеризує розподіл стейкхолдеров по таймслотам. Припустимо, що всі випадкові величини $\{\xi_i\}$ є незалежними та можуть приймати лише два значення: 0 (відповідний блок формується зловмисником) та 1 (блок формується чесним слотлідером). Нехай p – імовірність того, що $\xi_i = 1$, та $q = 1 - p$ – імовірність того, що $\xi_i = 0$. Цілком природньо припустити, що $q < 0.5$, хоча для запропонованого нижче методу це не має суттєвого значення.

У певному таймслоті (алгоритм визначення цього таймслота буде наведено нижче) зловмисник може почати будувати альтернативну послідовність блоків, в результаті чого утворюється розгалуження. Метою зловмисника є побудова розгалуження максимально можливої довжини. Припустимо, що у деякому наступному таймслоті обидві гілки мають однакову довжину (яка визначається кількістю блоків від розгалуження), причому це останній таймслот з рівними довжинами гілок. Тоді *довжина розгалуження* – це кількість блоків, які входять до однієї з цих гілок.

Метою запропонованої нижче моделі є моделювання дій зловмисника під час атаки розгалуження, направлених на утворення розгалуження максимально можливої довжини. В цій моделі досліджується ймовірність того, що довжина розгалуження перевищить деяке задане значення r.

Припустимо, що зловмисник вже почав атаку розгалуження. Тоді алгоритм приєднання блоків до гілок розгалуження є наступним. Якщо надходить блок, який формується чесним слотлідером (символ “1”), то він завжди приєднується до гілки, яка на даний момент є довшою. Якщо ж обидві гілки мають однакову довжину, то блок приєднується до будь-якої з них (імовірність приєднання блоку до тієї чи іншої гілки ролі не грає і може бути будь-якою). У випадку, коли надходить блок, який формується зловмисником (символ “0”), він приєднується до більш короткої гілки (спрацьовує принцип вирівнювання довжин гілок). Якщо ж гілки мають однакову довжину, то зловмисник під час відповідного таймслоту створює два блоки (з посиланням на відповідні попередні блоки) та приєднує по кожному блоку до обох гілок.

У подальшому знадобиться допоміжне твердження, яке дозволяє обчислювати ймовірність того, що розгалуження досягне певної довжини протягом заданої кількості таймслотів. Припустимо, що розгалуження починається у нульовому таймслоті, а блокчейн складається з m блоків. Потрібно обчислити ймовірність того, що розгалуження буде мати довжину, не меншу за γ. Цю ймовірність позначимо $Q(m, \gamma)$.

Якщо у l-му таймслоті довжина довшої гілки розгалуження становить i блоків, а коротшої гілки – j блоків, то пару (i, j) назвемо станом розгалуження у таймслоті l. Введемо допоміжні ймовірності $\{a(l,i,j)\}$, а саме $a(l,i,j)$ – ймовірність того, що у l-му таймслоті розгалуження знаходиться у стані (i, j). Ці ймовірності обчислюються за додаткової умови: якщо $j \le \gamma - 1$, то при переході із l-го таймслота до $(l+1)$-го допускається потрапляння у стани, коли обидві гілки мають однакову довжину ($i = j$); якщо ж $j \ge \gamma$, то переходи у такі стани вважаються неможливими. Таке визначення ймовірностей $\{a(l,i,j)\}$ дозволить у подальшому, скориставшись формулою повної ймовірності, знайти таймслоти, де відбулось *перше* потрапляння розгалуження у стани з довжиною розгалуження, не меншою γ.

Оскільки блокчейн складається з m блоків, то $1 \le l \le m$. Хоча розгалуження починається у нульовому таймслоті, але довжину розгалуження будемо рахувати, починаючи з першого таймслоту. Тому як початкове значення візьмемо $a(0,0,0) = 1$. Встановимо межі для кількості блоків у довшій та коротшій гілках розгалуження. Очевидно, що кількість блоків у довшій гілці у l-му таймслоті не може перевищувати l (це станеться, коли всі l блоків надходили від чесного слотлідера). Якщо ж одиниці та нулі чергуються, то довша гілка буде мати найменшу довжину $\lceil (l+1)/2 \rceil$, де $[\cdot]$ означає цілу частину. Коротша ж гілка може мати довжину від 0 до i (поточна довжина довшої гілки розгалуження у таймслоті l). Наступна лема встановлює рекурентні співвідношення для обчислення $\{a(l,i,j)\}$, а також формулу для обчислення ймовірності $Q(m,\gamma)$.

Лема. При початковій умові $a(0,0,0) = 1$ імовірності $\{a(l,i,j),\ 1 \le l \le m-1,\ \lceil (l+1)/2 \rceil \le i \le l,\ 0 \le j \le i\}$ визначаються так:

$$a(l,l,0) = p \cdot a(l-1,l-1,0),$$
$$a(l,i,j) = q \cdot a(l-1,i,j-1) + p \cdot a(l-1,i-1,j),\ \ j = 1,\ldots,\gamma-1,\ \ j < i,$$
$$a(l,j,j) = q \cdot a(l-1,j-1,j-1) + q \cdot a(l-1,j,j-1),\ \ j = 1,\ldots,r-1,$$
$$a(l,i,j) = q \cdot a(l-1,i,j-1) + p \cdot a(l-1,i-1,j),\ \ i \ge \gamma+2,\ \ \gamma \le j \le i-2,$$
$$a(l,i,i-1) = q \cdot a(l-1,i,i-2),\ \ i \ge \gamma+1.$$

Ймовірність $Q(m,\gamma)$ обчислюється за формулою:

$$Q(m,\gamma) = q \sum_{l=\gamma-1}^{m-1} a(l,\gamma-1,\gamma-1) + q \sum_{l=\gamma}^{m-1} \sum_{j=\gamma}^{l} a(l,j,j-1).$$

Дана лема дозволяє сформулювати метод прискореного моделювання ймовірності $P(n,r;L,s)$, який наведемо у вигляді алгоритму побудови незміщеної оцінки $\hat{P}_1(n,r;L,s)$ вказаної імовірності в одній реалізації.

1. Методом Монте-Карло моделюємо номер блоку, з якого зловмисник починає розгалуження. Необхідною умовою появи розгалуження з довжиною не меншою за s блоків є наявність щонайменше s нулів у послідовності з n символів. Тому здійснюємо наступні дії:

- обчислюємо $P_s = \sum_{k=s}^{n} C_n^k \, q^k \, p^{n-k}$;
- моделюємо випадкову величину ν, яка приймає значення k з імовірністю $C_n^k \, q^k \, p^{n-k} \big/ P_s$; нехай $\nu = k$;
- моделюємо випадкову послідовність $\overline{\xi} = (\xi_1, \ldots, \xi_n)$ за умови, що вона містить рівно k нулів та $n-k$ одиниць;
- послідовно, починаючи з кожного блока i, для якого $\xi_i = 0$, за наведеними вище правилами будуємо розгалуження; припустимо, що для деякого $i \le n-r$ існує таке $\mu_i \le \min\{i+L-1, n\}$, що після надходження блоку μ_i довжина розгалуження буде не меншою за s (μ_i – це перший блок із такою властивістю); якщо таке i існує, то знаходимо $m = n - \mu_i$ та $\gamma = r - \theta_i$, де θ_i – довжина розгалуження після надходження блоку μ_i; якщо такого i не існує, то це відповідає випадку, коли зловмисник не має наміру розпочати розгалуження у цій реалізації, і тому $\hat{P}_1(n,r;L,s) = 0$.

2. Якщо $\gamma \le 0$, то методом Монте-Карло вже побудовано розгалуження з довжиною не меншою за r, і в цьому випадку $\hat{P}_1(n,r;L,s) = P_s$. Нехай $\gamma > 0$. Якщо $m \ge \gamma$, то за рекурентними формулами, наведеними у Лемі, обчислюємо $Q(m,\gamma)$ і в якості оцінки маємо $\hat{P}_1(n,r;L,s) = P_s \cdot Q(m,\gamma)$. Якщо ж $m < \gamma$, то довжина розгалуження не може досягнути r, і тому $\hat{P}_1(n,r;L,s) = 0$.

Дослідження здійснено в рамках проекту «Розвиток розподіленої енергетики в умовах ринку електричної енергії України з використанням технологій та систем цифровізації», що виконується за напрямом використання бюджетних коштів «підтримка пріоритетних для держави наукових досліджень і науково-технічних (експериментальних) розробок» бюджетної програми КПКВК 6541230 в НАН України.

1. Kovalchuk L., Kaidalov D., Shevtsov O., Nastenko A., Rodinko M., Oliynykov R. Analysis of splitting attacks on Bitcoin and GHOST consensus protocols. *9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*. Bucharest, Romania, 2017. P. 978–982. https://doi:10.1109/IDAACS.2017.8095233 .

2. Кузнєцов М., Ковальчук Л., Шумська А. Моделювання спрощеного варіанту атаки розгалуження на блокчейн, який грунтується на протоколі консенсусу proof-of-stake. // *Кібернетика і системний аналіз* (прийнято до друку).

Л.В. Ковальчук, М.С. Кондратенко

ВИЗНАЧЕННЯ КІЛЬКОСТІ БЛОКІВ ПІДТВЕРДЖЕННЯ У ДВОРІВНЕВОМУ БЛОКЧЕЙНІ З ПРОТОКОЛОМ КОНСЕНСУСУ PROOF-OF-PROOF ПРИ РІЗНИХ ТИПАХ КОНСЕНСУСУ У МЕЙНЧЕЙНІ/САЙДЧЕЙНІ ДЛЯ ЗАПОБІГАННЯ АТАКИ ПОДВІЙНОЇ ВИТРАТИ

Ця робота продовжує дослідження роботи [1] і завершує серію досліджень стійкості дворівневого протоколу консенсусу Proof-of-Proof (PoP) до атаки подвійної витрати у блокчейні, *який наслідує стійкість (security inherited blockchain)*.

У наших попередніх роботах, що розглядали стійкість протоколу консенсусу PoP до атаки подвійної витрати, були отримані явні вирази для імовірності атаки у таких випадках:

- протоколи консенсусу Proof-of-Work(з урахуванням часу синхронізації) в обох блокчейнах ([2]);
- протокол консенсусу Proof-of- Stake в обох блокчейнах (робота [3]);
- протокол консенсусу Proof-of-Stake в основному блокчейні та Proof-of-Work в другорядному [1].

У цій роботі мистецтв отримаємо оцінки імовірності успіху атаки подвійної витрати для протоколу PoP у випадку, коли основний блокчейн реалізує протокол консенсусу Proof-of-Work, а другорядний – Proof-of-Stake. Таким чином, ця робота завершує дослідження імовірності успіху атаки для всіх випадків PoP, що базуються на найбільш поширених протоколах, якими є PoW та PoS.

Зазначимо, що при отриманні оцінки імовірності успіху атаки ми будемо також враховувати можливий час синхронізації у основному блокчейні (ОБ), а також можливість того, що зловмисник у другорядному блокчейні (ДБ) може ігнорувати випуск блоків у тих таймслотах, в яких він є слотлідером. Ці припущення дозволяють отримати оцінки у реальній моделі функціонування блокчейну, але з іншого боку створюють суттєві аналітичні складнощі при отриманні таких оцінок.

2. Позначення та допоміжні твердження.

У цій роботі ми використовуємо таку математичну модель дворівневого блокчейну. У основному блокчейні, який забезпечує стійкість до атак (зокрема до атаки подвійної витрати), використовується протокол консенсусу Proof-of-Work – наприклад, в якості основного блокчейну вибрано мережу Bitcoin. Ми також вважаємо, що в мережі присутній зловмисник, який порушує правила створення блоків та може намагатись виконати різні атаки на блокчейн, зокрема атаку подвійної витрати, яку ми тут розглядаємо. Також ми робимо припущення на користь зловмисника стосовно часу синхронізації мережі (тобто часу між моментом надсилання нового блоку і моментом, коли цей блок отримали всі учасники мережі). Надалі

припускаємо, що час синхронізації зловмисника є нульовим, а час синхронізації чесних майнерів вважаємо ненульовим і обмеженим зверху деякою величиною D_H. Позначимо α загальний гешрейт мережі, α_M – загальний гешрейт зловмисника, $\alpha_H = \alpha - \alpha_M$ – загальний гешрейт чесних майнерів. Позначимо $p_H = \frac{\alpha_H}{\alpha}$ та $p_M = \frac{\alpha_M}{\alpha}$ відповідно долю гешрейту чесних майнерів та зловмисника.

У другорядному блокчейні використовується протокол консенсусу Proof-of-Stake, отже що процес випуску блоків розбивається на *епохи*, кожна з яких, в свою чергу, розбивається на *таймслоти* – фіксовані відрізки часу, відведені на створення блоку слотлідером (слотлідерами) цього таймслоту. Позначимо N кількість таймслотів у одній епосі, а τ – тривалість одного таймслоту. Тоді час, відведений на одну епоху, дорівнює $N \cdot \tau$. Згідно з протоколом вибору слотлідера, в одному таймслоті може бути більше одного слотлідера, а може взагалі не бути слотлідерів. Але в будь-якому випадку буде виконуватись наступна вимога: *за один таймслот до блокчейну можна додати не більше одного блоку*. Позначимо β загальний стейк мережі, β_M – загальний стейк зловмисника, $\beta_H = \beta - \beta_M$ – загальний стейк чесних майнерів. Позначимо $q_H = \frac{\beta_H}{\beta}$ та $q_M = \frac{\beta_M}{\beta}$ відповідно долю стейку чесних майнерів та зловмисника.

Зазначимо, що більш детальний опис протоколів консенсусу PoW та PoS, а також алгоритм виконання зловмисником атаки подвійної витрати можна знайти у першій частині [1] цього дослідження.

Постановка задачі.

Задача, що вирішується у цій роботі, полягає в наступному. Нехай зловмисник виконує атаку подвійної витрати, намагаючись змінити деякий блок B_0 з вибраною транзакцією на альтернативний блок з альтернативною транзакцією, створивши розгалуження блокчейну та більш довгу альтернативну гілку. В рамках визначеної тут моделі, для заданого маленького значення $\varepsilon \in (0, 1)$, потрібно визначити таку найменшу кількість z блоків підтвердження у сайдчейні, що після їх виходу імовірність атаки подвійної витрати на блок B_0 не перевищує задане $\varepsilon \in (0, 1)$.

Лема 1 [9] (імовірність успіху атаки подвійної витрати за умови z блоків підтвердження у мережі з протоколом PoW та ненульовим часом синхронізації).

Позначимо

$$p'_M = 1 - e^{-\alpha_M D_H} \cdot \frac{\alpha_H}{\alpha_M + \alpha_H} = 1 - e^{-\alpha_M D_H} \cdot p_H;$$

$$p'_H = e^{-\alpha_M D_H} \cdot \frac{\alpha_H}{\alpha_M + \alpha_H} = e^{-\alpha_M D_H} \cdot p_H.$$

Також для заданих $k, z \in \mathbf{N}$ позначимо $P_z(k)$ імовірність того, що протягом часу, за який чесні майнери створять z блоків, зловмисник створить рівно k блоків.

Далі, позначимо P_z імовірність успіху атаки подвійної витрати, за умови створення чесними майнерами z блоків підтвердження (після блоку, на який направлена атака).

Тоді:

1) $P_z(k) = \frac{p_H^z}{(n-1)!} \cdot \frac{e^{-\alpha_M z D_H} \cdot (\alpha_M z D_H)^k}{k!} \cdot \sum_{i=0}^{k} \frac{(z-i+1)! \cdot C_k^i}{(\alpha z D_H)^i}$;

2) $P_z = \begin{cases} 1, & \text{if } p'_M \geq p'_H; \\ 1 - \sum_{k=0}^{z} P_z(k) \left(1 - \left(\frac{p'_M}{p'_H}\right)^{z-k}\right), & \text{else.} \end{cases}$

Введемо випадкові величини $T_H(i)$, $i \in \mathbf{N}$, де $T_H(i)$ дорівнює часу до створення i-го блоку підтвердження (після блоку, на який направлена атака) чесними майнерами. Ці величини розподілені експоненційно з параметром α_H для всіх значень i. Тоді час, що потрібен чесним майнерам на створення і розповсюдження i-го блоку підтвердження, визначається випадковою величиною

$$T'_H(i) = T_H(i) + D_H, \tag{1}$$

а величина

$$S'_H(n) = \sum_{i=1}^{n} T'_H(i) \tag{2}$$

визначає час, потрібний чесним майнерам на створення і розповсюдження n блоків підтвердження.

Лема 2. Функція розподілу випадкової величини (2) визначається так:

$$F_{S'_H(n)}(t) = P\left(S'_H(n) < t\right) = \begin{cases} 1 - e^{-\alpha_H \cdot (t - nD_H)} \cdot \sum_{i=1}^{n} \frac{\left(\alpha_H \cdot (t - nD_H)\right)^i}{i!}, & \text{if} \quad t \geq nD_H; \\ 0, \quad \text{else.} \end{cases}$$

3. Обчислення верхньої оцінки імовірності атаки подвійної витрати. Алгоритм обчислення кількості блоків підтвердження.

Тут і далі під словами «атака подвійної витрати» ми розуміємо атаку, при якій зловмисник таємно створює альтернативну гілку, в якій відсутній вибраний блок. Тобто це, швидше, атака на підміну блоку, яка не обов'язково призводить до подвійної витрати певної монети. Ми використовуємо цю термінологію, оскільки вона є загальноприйнятою для атаки, що відбувається за описаним сценарієм.

Тепер перейдемо безпосередньо до формулювання основного результату.

Теорема 1. Нехай в наших позначеннях виконується нерівність $p'_M < p'_H$, де $p'_M = 1 - e^{-\alpha_M D_H} \cdot p_H$, $p'_H = e^{-\alpha_M D_H} \cdot p_H$. Припустимо, що після блоку B_{Ch} вийшло z блоків підтвердження у сайдчейні. Тоді для довільного $l \in N$, такого, що $\tau \cdot z > l \cdot D_H$, справедлива наступна верхня оцінка для імовірності Q_z успіху атаки подвійної витрати на блок B_{Ch}:

$$Q_z \le e^{-\alpha_H \cdot (\tau \cdot z - l \cdot D_H)} \cdot \sum_{i=1}^{l-1} \frac{\left(\alpha_H \cdot (\tau \cdot z - l \cdot D_H)\right)^i}{i!} + 1 - \sum_{k=0}^{l} P_l(k) \left(1 - \left(\frac{p'_M}{p'_H}\right)^{l-k}\right), \quad (5)$$

де $P_l(k) = \frac{p_H^l}{(n-1)!} \cdot \frac{e^{-\alpha_M \cdot l \cdot D_H} \cdot (\alpha_M \cdot l \cdot D_H)^k}{k!} \cdot \sum_{i=0}^{k} \frac{(l-i+1)! \cdot C_k^i}{(\alpha \cdot l \cdot D_H)^i}$.

Наслідок 1. В умовах Теореми 1, виконується наступна нерівність:

$$Q_z \le \min_{l \in \mathrm{N}} \left\{ e^{-\alpha_H \cdot (\tau \cdot z - l \cdot D_H)} \cdot \sum_{i=1}^{l} \frac{\left(\alpha_H \cdot (\tau \cdot z - l \cdot D_H)\right)^i}{i!} + 1 - \sum_{k=0}^{l} P_l(k) \left(1 - \left(\frac{p'_M}{p'_H}\right)^{l-k}\right) \right\}. \quad (6)$$

Алгоритм 1.
Визначення кількості блоків підтвердження у дворівневому PoW/PoS блокчейні за заданими параметрами мережі та верхньою оцінкою імовірності атаки.

Вхід:

- бажана верхня границя імовірності атаки, $\varepsilon \in (0, 1)$;
- загальний гешрейт чесних майнерів у основному блокчейні, α_H;
- загальний гешрейт зловмисника у основному блокчейні, α_M;
- час затримки блоку для чесних майнерів у основному блокчейні, D_H;
- тривалість одного таймслоту у сайдчейні, τ.

Крок 1. Вибрати довільно $\varepsilon_1, \varepsilon_2 \in (0, 1)$, такі що $\varepsilon_1 + \varepsilon_2 = \varepsilon$.

Крок 2. Обчислити величини:

$$\alpha = \alpha_H + \alpha_M; \qquad p_H = \frac{\alpha_H}{\alpha}; \qquad p_M = \frac{\alpha_M}{\alpha};$$

$$p'_M = 1 - e^{-\alpha_M D_H} \cdot p_H; \qquad p'_H = e^{-\alpha_M D_H} \cdot p_H.$$

Крок 3. Перебором від $l = 1$ з кроком 1 визначити таке найменше $l \in \mathrm{N}$, що

$$1 - \sum_{k=0}^{l} P_l(k) \left(1 - \left(\frac{p'_M}{p'_H} \right)^{l-k} \right) < \varepsilon_1,$$

де $P_l(k) = \frac{p_H^l}{(n-1)!} \cdot \frac{e^{-\alpha_M \cdot l \cdot D_H} \cdot (\alpha_M \cdot l \cdot D_H)^k}{k!} \cdot \sum_{i=0}^{k} \frac{(l-i+1)! \cdot C_k^i}{(\alpha \cdot l \cdot D_H)^i}$

Запам’ятати значення l.

Крок 4. Перебором від $z = \left\lceil \frac{l \cdot D_H}{\tau} \right\rceil$ з кроком 1 визначити таке найменше $z \in \mathrm{N}$, що

$$e^{-\alpha_H \cdot (\tau \cdot z - l \cdot D_H)} \cdot \sum_{i=1}^{l} \frac{(\alpha_H \cdot (\tau \cdot z - l \cdot D_H))^i}{i!} < \varepsilon_2.$$

Вивід: z.

Дослідження здійснено в рамках проекту «Розвиток розподіленої енергетики в умовах ринку електричної енергії України з використанням технологій та систем цифровізації», що виконується за напрямом використання бюджетних коштів «підтримка пріоритетних для держави наукових досліджень і науково-технічних (експериментальних) розробок» бюджетної програми КПКВК 6541230 в НАН України.

1. Ковальчук Л., Кучинська Н., Кондратенко М. Визначення кількості блоків підтвердження у дворівневому блокчейні з протоколом консенсусу Proof-of-Proof при різних типах консенсусу у мейнчейні/сайдчейні для запобігання атаки подвійної витрати. Кібернетика та системний аналіз. 2024. Т. 60, № 4. С. 156–184.

2. Kovalchuk, L.; Kostanda, V.; Marukhnenko, O.; Pozhylenkov, O. Achieving Security in Proof-of-Proof Protocol with Non-Zero Synchronization Time. Mathematics 2022, 10, 2422. https://doi.org/10.3390/math10142422

3. Kondratenko M. Determining the number of confirmation blocks in the blockchain that hosts the second-level registry in the case that both blockchains use the POS-consensus protocol. Collection of materials of the XLI Scientific and technical conference of young scientists and specialists of G.E. Pukhov Institute for Modelling in Energy Engineering of National Academy of Sciences of Ukraine/PIMEE of NAS of Ukraine. 2023. P. 188-190 https://ipme.kiev.ua/wp-content/uploads/2023/05/Матеріали-конференції-2023.pdf

В.М. Горбачук, Т.О. Бардадим, М.С. Дунаєвський, В.В. Годлюк, Д.О. Рибачок

ОСНОВИ ДЕЦЕНТРАЛІЗОВАНИХ РИНКІВ ЕЛЕКТРОЕНЕРГІЇ

Динамічне впровадження відновлюваних джерел енергії (ВДЕ) та поява розподіленої генерації значно трансформували традиційний енергетичний ландшафт і привернули увагу до місцевих енергоринків, пристосованих для децентралізованої торгівлі енергією між різними учасниками ринку на рівні громади, сприяючи більшій енергетичній автономії та самопідтримуваності. З розвитком місцевих енергоринків виникають питання оптимізації стратегій енерготрейдингу, які враховують взаємодію з навколишнім середовищем і застосовують методи штучного інтелекту, зокрема навчання з підкріпленням (reinforcement learning), для максимізації виграшів (учасників енергоринків) через формування складних рішень шляхом машинного навчання. Уваги заслуговують різні проекти енерготрейдингу, започатковані на глобальному рівні, а також підходи машинного навчання і стратегії рішень для місцевих енергоринків, комплексний огляд моделей, стратегій рішень, підходів машинного навчання для торгівлі енергією на місцевих енергоринках [1]. За класифікацією сучасних алгоритмів навчання з підкріпленням, кожний відповідний метод може бути як основаним на моделі (model-based), так і вільним від моделей (model-free). Є різні алгоритми для енергетичних трансакцій, враховуючи тип агента, методи навчання, простір станів, вибір дій в залежності від стану, множину дій, значення функцій виграшу. Проекти енерготрейдингу на місцевих енергоринках потрібні дослідникам, зацікавленим сторонам (stakeholders), розробникам стратегій (policymakers), щоб формувати ефективне, самопідтримуване, резильєнтне і мирне майбутнє енергетики.

Глобальний світ переживає постійне збільшення попиту на енергію через комерціалізацію, індустріалізацію, урбанізацію. З іншого боку, у новому тисячолітті на Землі не розвідано значних великомасштабних запасів енергії. За прогнозами, відновлення після пандемії та зростаюче глобальне потепління вестимуть до приросту глобального споживання енергії від близько 1% на рік до майже на 2% на рік, тобто споживання енергії збільшуватиметься експоненціально. Крім того, економічне зростання Азії передбачає відповідне збільшення попиту на енергію, незважаючи на підвищену волатильність цін енергоносіїв внаслідок найбільшої від 1945 р. війни в Європі, починаючи з 2022 р., а також конфліктів у суміжних регіонах, які водночас пов’язуються з енергоносіями. Тому загрози майбутніх енергетичних криз стають дедалі помітнішими через нелінійність залежності між запасами енергії та її споживанням. За оцінками, до 2030 р. споживання відновлюваної електроенергії сягне 36% (порівняно з 40% сьогодні) загального глобального використання ВДЕ (включаючи традиційне використання біомаси): 14% – гідроенергетика;11% – вітрова енергетика; 6% – електрика з біомаси; 3% – сонячні фотоелектричні станції; 1% – електрика

від біогазу; менше 1% – геотермальна енергія; менше 1% – концентрована сонячна енергія (concentrated solar power, CSP).

Решта 64% (порівняно з 60% сьогодні) загального глобального використання ВДЕ припадатиме на сектори кінцевого споживання: 17% – теплоенергетика на біомасі (biomass heat industry) (включаючи ТЕЦ і централізоване теплопостачання (combined heat and power (CHP) and district heat)); 13% – транспорт на біопаливі; 11% – сучасна біомаса, що замінює традиційну; 11% – будівлі на теплі з біомаси і централізованому теплопостачанні; 9% – геліотермальна енергетика (solar thermal heat); 2% – будівлі на теплі з біогазу (включаючи ТЕЦ і централізоване теплопостачання); 1% – геотермальне тепло.

Традиційна електромережа характеризується централізованою структурою, де енергія виробляється на великих електростанціях (ЕС), а потім розподіляється споживачам після проходження великої відстані через складні сітки транспортування енергії. Ця складна структура, вразлива до окремих точок відмови, часто не в змозі забезпечувати універсальний доступ до енергії, особливо у віддалених або малозабезпечених регіонах. Крім того, ця структура не дає споживачам можливості брати активну участь в енергоринках або висуває споживачам непрозоре ціноутворення при купівлі чи продажу енергії [2]. Оскільки ця структура також чутлива до впливу забруднень довкілля, то стикається з підвищеними ризиками перебоїв постачання чи несподіваних відключень внаслідок вразливості до змін клімату. У новому тисячолітті глобальна енергосистема зазнала суттєвих трансформацій, спричинених зростанням попиту на розподілені енергоресурси (distributed energy resources (DERs)), прогресом енергетичних технологій, скороченням викидів парникових газів. Пов’язані з DERs ризики вели до зсуву від ринку, керованого лише споживачами, до ринку електрики, керованим усіма його учасниками, через конкурентний енергоринок (competitive energy market (CEM)). Традиційно ринок електроенергії включає оптовий ринок електроенергії (wholesale electricity market (WEM)) та роздрібний ринок електроенергії (retail electricity market (REM)).

Великі виробничі засоби (звичайні генеруючі установки, відновлювані ресурси, агреговані розподілені генератори (distributed generators (DGs)), прилади накопичення) на WEM подають електроенергію до оператора системи передачі (transmission system operator (TSO)), звідки вона надходить до провайдерів енергетичних послуг, роздрібних торгівців, великих споживачів і на REM, де електроенергія через оператора системи розподілу (distribution system operator (DSO)) надходить до груп споживачів; до груп споживачів електроенергія надходить також від великих споживачів. Маломасштабні засоби виробництва (малі споживачі, а також вищезгадані відновлювані ресурси, агреговані DGs, прилади накопичення) та нові учасники енергоринку (агрегатори електромобілів (electric vehicles (EVs)), провайдери послуг реагування на попит (demand response service)) мають як вхідні, так і вихідні потоки електроенергії на DSO.

У типовій структурі енергосистеми великі виробники та споживачі електроенергії беруть участь у WEM, щоб продавати і купувати енергію, сприяючи ефективному обміну електроенергією у ширшому масштабі, зокрема обміну з конкретними географічними областями чи регіонами для задоволення їх попиту. Хоча менеджмент попиту і пропозиції на WEM загалом є ефективним, існують певні обмеження, особливо для малих споживачів, які мають обмежені можливості вибору своїх постачальників електроенергії та можуть діставати її лише від афілійованих компаній розподілу, уповноважених встановлювати ціни електроенергії. Оскільки подібна відсутність конкуренції на CEM звужує споживчі переваги та рішення, то WEM стає неефективним для ВДЕ, які мають незначні чи нульові граничні витрати: на WEM ціна електроенергії встановлюється на рівні граничних витрат системи. З іншого боку, на REM система розподілу відокремлена від системи постачання. Запровадження DSO породило REM, першочерговим завданням якого є закупівля енергії від WEM і передача її споживачам. DSO виконує функцію шлюзу ринкових послуг, що регулює та надає доступ до мережі розподілу роздрібному постачальнику, який постачає електроенергію кінцевим споживачам.

Хоча протягом тривалого часу енергоринки виконували багато завдань, на REM залишаються деякі проблеми. Найбільший виклик у тому, що тарифи роздрібних продавців є фіксованими усередненими цінами для споживачів, а тому виграші низької вартості електроенергії у періоди непікового навантаження не передаються належним чином споживачам. Отже, оператори системи не в змозі скорочувати піковий попит і змінювати структуру використання енергії споживачами, хоча споживачам пропонуються різні цінові конфігурації, залежні від реального часу, фіксованої ставки, тривалості користування тощо. Хоча на REM споживачі можуть змінювати постачальників, подібна зміна чи відміна не є безкоштовною, внаслідок чого відповідні додаткові витрати обмежують кількість покупців, які можуть скористатися можливостями переходу від одного продавця до іншого. Такі проблеми, з якими стикаються споживачі на WEM та REMs, можна вирішувати поєднанням роботи генерації, накопичення, реагування на попит через запровадження локальних енергоринків (local energy markets (LEMs)).

LEMs − це децентралізовані системи, що працюють на рівні мікромереж або громад, зосереджуючись на одноранговій (peer-to-peer (P2P)) торгівлі енергією, локальній оптимізації, реагуванні на попит з використанням таких DERs, як сонячні панелі та батареї. LEMs спираються на технології розумних мереж, Інтернету речей (Internet of Things (IoT)), блокчейну для моніторингу в реальному часі та трансакцій з коротшими періодами розрахунків і новопосталими регуляторними структурами. З іншого боку, великомасштабні енергетичні ринки (large scale energy markets (LSEMs)) працюють на регіональному чи національному рівнях, управляючи масовим виробництвом і передачею енергії за допомогою централізованих ЕС і встановлених ринкових структур (наприклад, торгівля на добу наперед (day-ahead) і

допоміжні (ancillary) послуги). LSEMs надають пріоритет стабільності мережі, оптимізації великої вимірності, відповідності суворим регулюванням. Ключова технічна відмінність між LEMs і LSEMs полягає в їхній інфраструктурі, масштабі, учасниках і цілях: LEMs зосереджується на локальній резильєнтності та самопідтримуваності, а LSEMs − на надійності, ефективності та узгодженні енергетичної стратегії на макрорівні.

Уваги заслуговує оцінка стану LEMs на CEM. У 2009 р. Лейденський університет (заснований у 1575 р.) у Нідерландах запропонував розроблений ним програмний засіб для побудови та візуалізації бібліометричних мереж Visualization of Similarities (VOS) Viewer. Ці мережі, які можуть включати журнали, дослідників або окремі публікації, можуть будуватися на основі цитування, бібліографічних зв'язків, спільного цитування чи відносин співавторства. VOS Viewer також пропонує функціонал добування тексту, який можна використовувати для конструювання та візуалізації мереж спільного входження важливих термінів, добутих з корпусу наукової літератури. За допомогою VOS Viewer можна генерувати відображення мережевої візуалізації дослідницьких трендів на енергоринку, щоб подавати взаємозв'язки між різними поняттями і термінами на основі їх спільного входження у дані чи певний огляд літератури. На відповідній карті візуалізації кожний вузол, виділений кольором, подає конкретний термін або поняття, пов'язане з енергетичними ринками і технологіями, такими як «реагування на попит», «P2P-торгівля» і «навчання з підкріпленням», а розмір вузла пропорційний частоті використання предмета дослідження. Лінії (ребра), що з'єднують вузли, вказують на відношення між термінами: товстіші лінії чи ближче розташування загалом означає сильніші взаємозв'язки чи вищий рівень спільного входження. Аналіз спільного входження ключових слів позначає наукові кроки і тренди, які прогресували з часом, окреслюючи понятійну структуру й узагальнюючи її в бібліографічній збірці, щоб відображати і групувати терміни, добуті серед ключових слів.

Оскільки вузли «реагування на попит» і «трансактивна енергія» (transactive energy) розташовані в центрі згаданої карти, то ці терміни є ключовими з багатьма зв'язками до інших термінів, що вказує на їхню важливість у мережі. Вузол «реагування на попит» є центральним, пов'язуючись з різними іншими концепціями і демонструючи свою ключову роль в системах енергоменеджменту та розумних мереж.

1. Khaskheli S., Anvari-Moghaddam A. Energy trading in local energy markets: a comprehensive review of models, solution strategies, and machine learning approaches. *Applied Sciences,* 2024, 14, 11510. https://doi.org/10.3390/app142411510

2. Горбачук В.М., Дроб'язко А.О. Енергетичний сектор в економічній моделі України. *Електроенергетика України: стратегія ефективності*. І.Р.Юхновський (гол.ред.) Київ: Міжвідомча аналітично-консультативна рада з питань розвитку продуктивних сил і виробничих відносин, 2001. С. 63–67.

З.Х. Борукаєв, В.А. Євдокімов, К.Б. Остапченко

КОНЦЕПТУАЛЬНА МОДЕЛЬ ОРГАНІЗАЦІЇ ДЕЦЕНТРАЛІЗОВАНОЇ ТОРГІВЛІ ЕЛЕКТРИЧНОЮ ЕНЕРГІЄЮ В УКРАЇНІ

Головною метою реалізації основних трендів Енергетичного переходу, сформульованого в рамках концепцій Smart Grid (Розумна мережа) та Demand Response (Управління попитом) та нормативно закріпленого у Директиві ЄС 2019/944 Європейського парламенту і Ради від 05 червня 2019 року про спільні правила для внутрішнього ринку електроенергії, є суттєве підвищення енергоефективності процесів виробництва, передачі та споживання електричної енергії у електроенергетичних системах та перетворення електроенергетики в інтелектуальну екологічно безпечну систему, із безпосередньою участю суб'єктів ринку, включаючи кінцевих споживачів. Досягнення цієї мети пов'язують із реалізацією наступних принципів розвитку сучасних електроенергетичних систем.

Декарбонізація виробництва – перехід до екологічно чистої економіки, за рахунок більш масштабного впровадження енергетичних установок розподіленої, розосередженої генерації, що використовують відновлювальні джерела енергії, впровадження систем накопичення енергії, які відкривають нові можливості для підвищення гнучкості та якості управління режимами функціонування локальної електроенергетичної системи (ЛЕС) та покращення економічних показників енергетики в цілому на всіх етапах виробництва, передачі та розподілу електроенергії.

Децентралізація управління – перехід до нової системи організації торгівлі електричною енергією на основі утворення кластерів виробництва та споживання електроенергії – ЛЕС регіонального значення шляхом збільшення використання у них частини розподілених, розосереджених джерел генерації електроенергії, систем накопичення енергії із застосуванням технології керування мережами MicroGrid, проведення відповідної реорганізації структур організаційного управління ринком електроенергії та створення сучасних систем розрахунків платежів на регіональному рівні.

Діджиталізація (цифровізація) енергетики – перехід до реалізації концепції розумних мереж Smart Grid на основі застосування цифрових технологій динамічного управління пропозицією і попитом, виробництвом, передачею та споживанням електроенергії [1].

Практична реалізація названих принципів призводить до необхідності змін у функціональній архітектурі організаційної, організаційно-технологічної системі виробництва, передачі, розподілу та споживання електроенергії в об'єднаній електроенергетичній системі (ОЕС) України, у інформаційно-комунікаційному середовищі взаємодії учасників виробничих та економічних процесів на ринку електроенергії. Як наслідок, ця обставина зумовлює необхідність вирішення складних завдань удосконалення

структури управління ринком електроенергії в напрямку його децентралізації та запровадження дієвих механізмів процесу ціноутворення на ньому із безумовним дотриманням принципів функціонування ринку електричної енергії відповідно до статті 3 Закону України "Про ринок електричної енергії".

Очевидно, що реалізація такого проекту з децентралізації ринку, в цілому, потребує залучення значних фінансових ресурсів. Тому досить складним видається завдання з вибору найбільш раціонального шляху пошуку фінансових ресурсів на проведення зазначених структурних змін у функціональній архітектурі ОЕС. Крім того, залучення приватних інвестицій вимагає створення певних умов для стимулювання участі інвесторів у реалізації конкретних проектів з децентралізації із зрозумілими умовами, перспективами і термінами їх окупності. Тому, побудову нової архітектури децентралізованого ринку електроенергії необхідно починати відбудовувати "знизу догори", із створенням Мікроринків ЛЕС на базі технологій Microgrid, які об'єднують об’єкти малої генерації із генеруючими установками малої потужності та активних побутових і непобутових кінцевих споживачів електроенергії (до 10 000 кВт*год на рік).

Отже, постає завдання із розроблення і подання ринкової концептуальної моделі організації децентралізованого ринку електроенергії для вирішення задач управління попитом, яку слід розглядати в контексті гармонізації роботи централізованого ринку електроенергії та Мікроринків на рівні ЛЕС в умовах реалізації принципів концепції Smart Grid та програм Demand Response з використанням розподілених, розосереджених ресурсів виробництва та накопичення електроенергії споживачів.

Міжнародний досвід розвитку децентралізованої торгівлі електричною енергією, які отримали в літературі назву "місцевих ринків", дозволяє стверджувати, що такі ринки можуть стати драйвером післявоєнного розвитку децентралізованої ринкової інфраструктури України у частині впровадження та набуття практичного досвіду застосування принципів Smart Grid та Demand Response на регіональному рівні і формування відповідних нормативних, організаційних та технічних рішень.

На сьогоднішній день у світі на ринках електроенергії у напрямку їхньої децентралізації на основі широкомасштабного використання джерел розподіленої та розосередженої генерації домашніх господарств (просьюмерів) знаходять застосування дві основні моделі. У першій їх просьюмери індивідуально керують своїми енергоресурсами і потім торгують надлишками енергії з централізованою ринковою інфраструктурою чи один з одним. В іншій моделі кілька споживачів, що об'єднуються в енергетичну спільноту (агрегатор), формують мікромережу і спільно використовують і контролюють наявні енергетичні ресурси, такі як вітряні, сонячні станції, накопичувачі енергії, що належать співтовариству шляхом їх консолідації в ЛЕС. В результаті організовується інфраструктура Мікроринку (локального місцевого ринку) для проведення торгових операцій між його агентами, експорту надлишків енергії в загальну зовнішню мережу та імпорту енергії.

Очевидно, що для функціонування Мікроринку з метою забезпечення енергозабезпечення (безперебійного постачання електроенергії відповідної якості), енергодоступності (енергоощадності та доступності ціни на електроенергію), енергоприйнятності (мінімального впливу на навколишнє середовище виробництва електроенергії) згідно [2] необхідно створювати нові інфраструктурні елементи організаційного управління та диспетчерського керування, систему центрів сервісного обслуговування, що аналогічні наявним на централізованому ринку електроенергії. Крім того, природно необхідним є задоволення вимог до функціональності, які пред'являються до "розумних мереж" відповідно до Концепції їх впровадження в Україні до 2035 року [3].

Основним теоретичним базисом вирішення завдань інтеграції Мікроринків до централізованої багаторівневої ринкової системи управління та організації торгової взаємодії з учасниками ринку, які необхідно вирішувати при безпосередній побудові системи управління Мікроринками, є їх формулювання та постановка як задач оптимального функціонування ринку [4].

На першому етапі за основу формування структури організації ринкової взаємодії внутрішніх суб'єктів Мікроринку може бути використана відома модель «Єдиного покупця та продавця», шляхом утворення агрегаторів (операторів), як нових суб'єктів ринку з певними повноваженнями здійснення таких функцій від імені користувачів та активних споживачів, що його утворили, на технічної базі малих систем розподілу (МСР) в ЛЕС. Можливість створення МСР передбачена п.9 Кодексу систем розподілу [5], в якому визначені вимоги, обов’язки, права та функції агрегаторів МСР та особливості їх стосунків із користувачами МСР та з мережами операторів системи розподілу (ОСР), які визначаються Правилами роздрібного ринку електричної енергії, затвердженими постановою НКРЕКП від 14 березня 2018 року № 312. Окремо визначено, що МСР виконує функції, має такі ж права та обов’язки як і ОСР щодо користувачів МСР з урахуванням особливостей, визначених Кодексом систем розподілу та Правилами роздрібного ринку, без відповідних ліцензій.

На централізованому ринку електроенергії агрегатор Мікроринку здійснює свою діяльність як одна юридична особа, функціональна особливість якої відрізняється тим, що агрегатор на місцевому ринку реалізує функції єдиного покупця-виробника і продавця-постачальника електроенергії власним пасивним та активним споживачам. А на централізованому ринку він функціонально представляється як виробник електроенергії, що продає її надлишки на оптовому, роздрібному сегментах ринку або на ринку допоміжних послуг, якщо бере участь у програмі управління попитом від ОСР або постачальник універсальних послуг шляхом збільшення чи зниження активного навантаження своїх споживачів.

На наступному етапі, за наявності нормативної бази та технічних можливостей інформаційно-телекомунікаційного обладнання, можна впроваджувати автоматизацію процесів ціноутворення та функціонування

Мікроринку на основі Smart систем керування та застосування технології блокчейн для вирішення наступних завдань: дотримання незалежності прийнятих рішень щодо проведення торгівлі електроенергією (Товар і Продукція) та системними послугами (Послуги) на внутрішньому Микроринку на основі розроблення узгоджених Правил; впровадження відповідності технічних характеристик розосереджених генеруючих установок в ЛЕС міжнародним стандартам, а також стандартам їхньої сумісності IEC 61400-25 та IEC 61850; створення інформаційно-комунікаційного середовища Smart системи розумних мереж задля дотримання належного рівня інформаційної і технологічної безпеки, дотримання порядку інформаційного обміну даними між структурними агентами ринку відповідно до стандарту IEC 62325 «Інфраструктура комунікацій на енергоринку». Для реалізації цих завдань потрібно ввести до структурно-функціональної схеми концептуальної моделі інтеграції Мікроринку нових агентів – агрегатора управління попитом у ролі оператора Мікроринку, оператора МСР, оператора-виробника, оператора-постачальника, оператора управління навантаженням, учасників програми управління попитом у ролі агентів-генерації, агентів-навантаження.

Відмінність запропонованого підходу полягає в тому, що він розглядається в контексті гармонізації роботи централізованого ринку електроенергії та Мікроринків на рівні ЛЕС в умовах реалізації принципів концепції Smart Grid та програм Demand Response з використанням ресурсів виробництва електроенергії та навантаження споживачів. Концептуальна модель може бути покладена в основу розробки пілотного проекту побудови Мікроринку в ЛЕС.

1. Кириленко, О.В (2022). Заходи та засоби перетворення енергетики України на інтелектуальну екологічно безпечну систему: Доповідь на науковій сесії Загальних зборів НАН України 17 лютого 2022 року. Вісник Національної академії наук України. (3). 18-23. https://doi.org/10.15407/visn2022.03.018

2. Стогній, Б.С., Кириленко, О.В., Праховник, А.В., & Денисюк, С.П. (2012). Еволюція інтелектуальних електричних мереж та їхні перспективи в Україні. Технічна електродинаміка. (5). 62-67. https://techned.org.ua/index.php/techned/article/view/1372

3. Розпорядження Кабінету Міністрів України від 14 жовтня 2022р. №908-р. “Концепція впровадження “розумних мереж” в Україні до 2035 року”. (2022). https://zakon.rada.gov.ua/laws/show/908-2022-%D1%80#Text

4. Борукаєв, З.Х., Євдокімов, В.А., & Остапченко, К.Б. (2023). Стан та перспективи організації децентралізованої торгівлі електроенергією на регіональному рівні. Електронне моделювання. 45(3). 11-27. https://doi.org/10.15407/emodel.45.03.011

5. Постанова НКРЕКП від 14.03.2018р. №310 “Кодекс систем розподілу”. (2018). https://zakon.rada.gov.ua/laws/show/v0310874-18#Text

А.В. Полухін, В.А. Євдокімов, Я.П. Лукашевич

СМАРТ-КОНТРАКТИ НА ОСНОВІ БЛОКЧЕЙНУ ЯК ШЛЯХ ДО РОЗВИТКУ ДЕЦЕНТРАЛІЗОВАНОГО РИНКУ ЕЛЕКТРИЧНОЇ ЕНЕРГІЇ В УКРАЇНІ

Українська енергетика перебуває під постійними обстрілами та загрозою відключень електричної енергії. Концентрація значних потужностей виробництва призводить до того, що виведення з ладу одного ключового вузла спричинює проблеми з постачання електричної енергії у низці регіонів.

У зв'язку з проблемами постачання електричної енергії, на сьогодні в Україні існує необхідність у пошуку альтернативних способів забезпечення електропостачання. Разом з тим, досить розвиненою є розподілена генерація. Існує багато сонячних та вітрових станцій, приєднаних до розподільчих мереж, які могли б забезпечувати електричною енергією локальних споживачів критичної інфраструктури.

Наразі більша частина виробників з альтернативних джерел працюють за механізмом «зеленого» тариф. Тобто, весь обсяг виробництва викуповується за пільговою ціною центральним підприємством. З точки зору управління електромережою це означає, що диспетчер не бачить законтрактованих обсягів за певним регіоном, а тому точно не знає, чи буде спожитий увесь вироблений обсяг, чи ні. Як результат – застосовуються обмеження споживання для цього регіону.

Однією з можливостей, яка могла б бути реалізована для поліпшення цієї ситуації – запровадження системи смарт-контрактів та контрактація безпосередньо між виробником та споживачем у межах розподіленої мережі на певній платформі, яка б адмініструвала всі дії – блокчейні [2].

У зазначених умовах, необхідно забезпечувати споживання електричною енергією різні категорії споживачів, у тому числі житлово-комунальні господарства, транспорт, сільські господарства [1]. Для досягнення цієї мети у регіонах є можливість використовувати місцеве виробництво. При цьому, зрозуміло, що у поточних реаліях майже неможливо забезпечити повну потребу певного регіону електричною енергією, яка виробляється у його межах. Так чи інакше, найбільші частину споживання забезпечується найбільшими потужностями виробництва. Однак, ніщо не заважає розподіленій генерації забезпечувати безперебійну роботу критичної інфраструктури.

У довоєнні роки по Україні приблизно 26% споживання припадає на вище комунально-побутові, сільгоспоживачів, транспорт та інші критичні для функціонування країни та економіки категорії споживачів. Таким чином, більшу частину потреби є можливість задовільнити за допомогою внутрішньої, розподіленої генерації. Умовно можна розділити ринок на два рівні:

1) локальний ринок контрактів, на якому задовільняється споживання певної категорії критичних споживачів;

2) централізований ринок – оптовий ринок, на якому функціонують постачальники, крупні виробники тощо (рисунок 1).

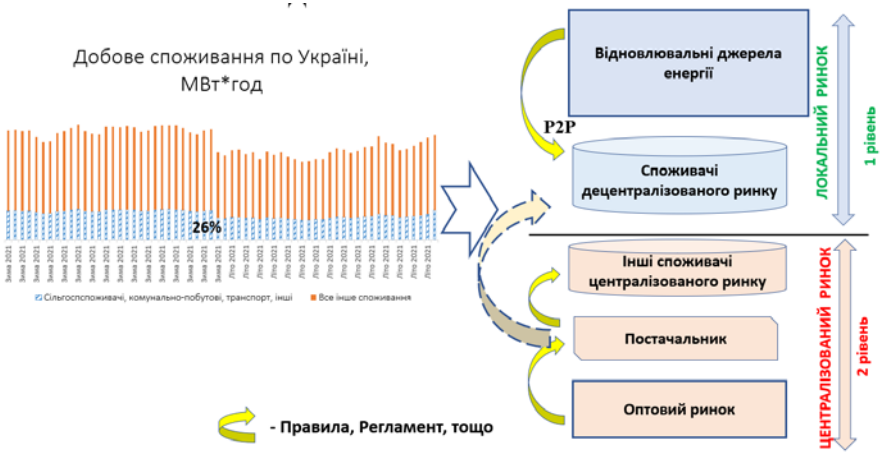

Рисунок 1 – Система децентралізованого ринку

Для практичної реалізації системи смарт-контрактів пропонується розглянути наступну блок-схему зазначеного механізму:

1. Учасники системи:

1.1. Виробники енергії: сонячні панелі, вітряки, малі електростанції, накопичувачі енергії.

1.2. Споживачі енергії: підприємства, інфраструктурні об'єкти.

1.3. Постачальник: забезпечує балансування для смарт-контрактів.

1.4. Оператор системи розподілу (ОСР): забезпечує фізичний баланс.

1.5. Блокчейн-платформа: використовується для адміністрування та реєстрації транзакцій.

2. Основні процеси:

2.1. Ініціалізація смарт-контракту: учасники реєструються на платформі.

2.2. Визначаються параметри контракту (ціна, обсяг енергії, час поставки).

2.3. Збір даних: виробники та споживачі надсилають дані про генерацію/споживання енергії до блокчейну. Дані фіксуються у смарт-контрактах та блокчейні.

2.4. Виконання смарт-контракту: споживач підтверджує отримання енергії. Смарт-контракт запускає автоматичний розрахунок і переказ коштів.

2.5. Завершення транзакції: усі дані записуються в блоки, формуючи прозору історію транзакцій.

3. Основні вузли процесу:

3.1. Реєстрація учасників: учасники підключаються до блокчейну.

3.2. Введення даних (генерація, споживання, баланс): учасники надсилають дані до ОСР.

3.3. Формування смарт-контрактів: умови контракту зберігаються в блокчейні.

3.4. Виконання контракту (транзакція): переказ енергії та коштів.

3.5. Зберігання інформації: усі дії записуються для аудиту.

Роботу виконано за держбюджетною темою «Розвиток розподіленої енергетики в умовах ринку електричної енергії України з використанням технологій та систем цифровізації» (шифр: ЦИФРОВІЗАЦІЯ), КПКВК 6541230.

1. Саух С. Концепція побудови структурно мінливої електроенергетичної системи України. Технічна електродинаміка. 2023. № 5. С.48-54. DOI: https://doi.org/10.15407/techned2023.05.048.

2. Gorbachuk, Vasyl & Dmytro, Nikolenko & Mykhajlo, Pustovoit & Victor, Godliuk & Rybachok, Dmytro. (2024). Smart contracts in energy. Usage of Blockchain Technologies in Energetics (June 5, 2024, Kyiv, Ukraine). Kyiv, Ukraine: G.E.Pukhov Institute for Modeling in Energy Engineering National Academy of Sciences of Ukraine, 2024. P. 6–9.

В.А. Євдокімов, Д.Р. Цвілій

КОНЦЕПТ ПОБУДОВИ ПЛАТФОРМИ ДЛЯ УКЛАДАННЯ P2P КОНТРАКТІВ НА РИНКУ ЕЛЕКТРИЧНОЇ ЕНЕРГІЇ УКРАЇНИ

Децентралізація ринку електричної енергії є важливим кроком на шляху до ефективної та сталої енергетичної системи. У сучасних умовах глобальних змін клімату, потреба у переході до відновлюваних джерел енергії стає дедалі актуальнішою. Децентралізовані моделі ринку надають можливість виробникам, зокрема тим, хто генерує електричну енергію з відновлюваних джерел, зменшувати залежність від великих енергетичних компаній, що контролюють централізовані системи. Це дозволяє не лише стимулювати розвиток зеленої енергетики, але й забезпечує більшу прозорість, справедливість та ефективність на ринку.

Одним із ключових аспектів децентралізації є можливість укладання прямих контрактів між учасниками ринку, що дозволяє знижувати витрати і надавати виробникам зеленої енергії більший контроль над ціноутворенням. У цьому контексті, розробка та впровадження інформаційних систем для укладання P2P (peer-to-peer) контрактів є необхідною для створення ефективного, гнучкого та прозорого ринку електричної енергії, де кожен учасник може реалізувати свій потенціал і отримувати вигоду від прямої взаємодії з іншими учасниками ринку.

Процес визначення акцептованих обсягів та цін при укладанні P2P контрактів, та, як наслідок формування відповідних транзакцій щодо купівлі або продажу електричної енергії, можна розділити на наступні основні складові (Рис. 1).

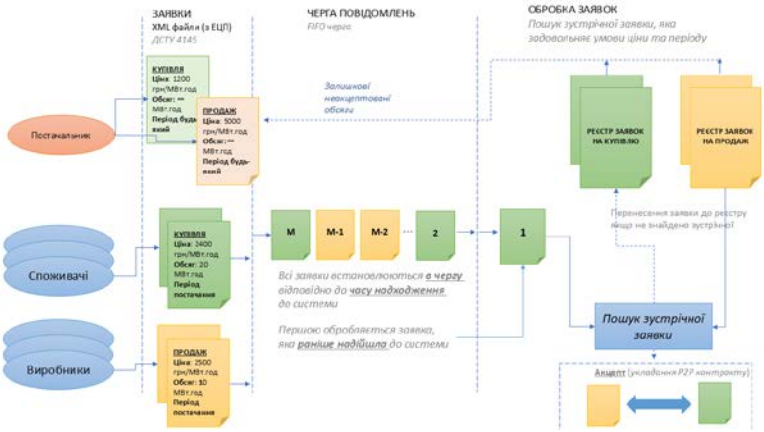

Рисунок 1. – Процес співставлення заявок

1) *Підсистема прийому заявок від учасників торгів*. Дана підсистема має забезпечувати безперервний прийом від споживачів, виробників та постачальників даних щодо цін, обсягів та періодів постачання електричної енергії. Також слід зазначити, що вказана підсистема має підтримувати механізм накладання та перевірки кваліфікованого електронного підпису (КЕП).

2) *Черга повідомлень*. Зазначена черга функціонує за принципом класичного FIFO (First Input First Output) буферу, де незалежно від інтенсивності (одночасності) надходження заявок до системи, всі заявки будуть оброблятися послідовно одна за одною, в залежності від часу надходження до системи [1]. В якості технічної реалізації та з метою забезпечення активного оновлення інтерфейсу користувача в процесі проведення торгів, можуть бути використані технології, які функціонують за протоколом AMQP.

3) *Підсистема торгів***.** Дана підсистема забезпечує пошук зустрічних заявок для їх подальшого акцепту та формування відповідних транзакцій. Співставлення заявок відбувається за наступним алгоритмом [2, 3].

Нехай

R_B, R_S - множини заявок $r_B \in R_B$ та $r_S \in R_S$ на купівлю та продаж відповідно, що наявні в системі в момент часу t_0;

p_B , p_B – ціни заявок r_B та r_S відповідно;

r^* - заявка із ціною p^*, що надійшла до системи в момент часу $t_1 > t_0$.

Процес пошуку зустрічної заявки r^A полягає у виборі такої заявки з множини R_B або R_S, яка відповідає умовам заявки r^* та, при цьому, має найнижчу ціну для заявок на продаж, та найвищу - для заявок на купівлю, незалежно від часу надходження до системи (1):

$$r^A = \begin{cases} r_B^A \in R_B : p_B^A \geq p^*, \forall r_B \neq r_B^A \; p_B \leq p_B^A \\ r_S^A \in R_S : p_S^A \leq p^*, \forall r_S \neq r_S^A \; p_S \geq p_S^A \end{cases} \quad (1)$$

4) *Підсистема ведення реєстру заявок*. Вказана підсистема призначена для збереження заявок, які надійшли до системи, та які не були акцептованими в процесі їх обробки. Дані заявки зберігаються до моменту закінчення часу, протягом якого вони можуть бути акцептованими.

5) *Підсистема транзакцій*. Зазначена підсистема відповідає за збереження акцептованих обсягів та цін співставлених заявок (транзакцій). Також, слід зауважити, що дані щодо транзакцій можуть зберігатися в децентралізованій базі даних за рахунок використання Blockchain технологій.

З метою організації основних функціональних можливостей системи та забезпечення зручного, інтуїтивно зрозумілого інтерфейсу є доцільним використання інтерфейсу подібного до Панелі торгів ВДР

(внутрішньодобового ринку), який протягом більш ніж 5 років використовується на ринку електричної енергії України (Рис. 2).

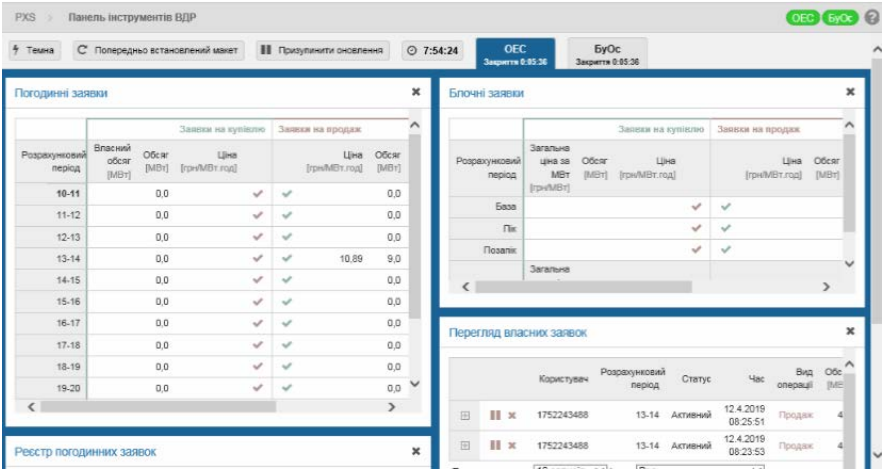

Рисунок 2 – Приклад інтерфейсу для проведення торгів

Вищезазначений інтерфейс складається із наступних компонентів:

1) Блок переліку заявок доступних для акцепту, де відображається поточний стан торгів, зокрема максимальна та мінімальна ціна купівлі/продажу електричної енергії, глибина торгів та доступні періоди торгів. В тому числі, даний блок забезпечує можливість детального перегляду списку заявок по вибраному періоду для розрахунку стратегії торгів.

2) Блок власних заявок призначений для керування заявками, що були подані учасником до системи, який має підтримувати функції скасування та призупинення вибраної заявки та надавати основну інформацію по заявці: час подачі, ціна, обсяг, акцептовані значення тощо.

3) Блок створення/подачі заявки на торги призначено для введення інформації щодо заявленої ціни, обсягів та бажаного періоду торгів. Також, зазначений блок забезпечує можливість підписання заявки КЕП.

Також слід звернути увагу на основні вимоги до інформаційної системи для укладання P2P контрактів на ринку електричної енергії:

- клієнтська частина повинна бути доступна для користувачів у вигляді веб додатків, що забезпечують зручний інтерфейс для укладання контрактів, перевірки транзакцій та моніторингу стану контрактів;

- серверна частина повинна мати високу продуктивність і масштабованість для обробки великої кількості запитів від користувачів, зберігання даних про контракти, а також забезпечення безпеки транзакцій;

- використання технології Blockchain для зберігання та верифікації всіх транзакцій є ключовим. Це дозволяє забезпечити прозорість, захист від підробок і створити децентралізовану мережу, де всі учасники можуть перевіряти справжність даних без участі посередників;
- використання смарт-контрактів;
- підтримка легкої інтеграції з іншими блокчейн-мережами.

Враховуючи зазначене, розробка інформаційної системи для укладання P2P контрактів на ринку електричної енергії є важливим кроком у напрямку децентралізації енергетичних ринків. Використання технології blockchain дозволяє забезпечити прозорість, безпеку та ефективність укладання контрактів між виробниками та споживачами, знижуючи залежність від посередників. Клієнт-серверна архітектура та інтуїтивно зрозумілий інтерфейс системи забезпечують зручність користування для різних категорій учасників ринку. Інтеграція з існуючими рішеннями та забезпечення високого рівня безпеки даних дозволяє створити надійну платформу для здійснення прозорих і автоматизованих торгів.

Роботу виконано за держбюджетною темою «Розвиток розподіленої енергетики в умовах ринку електричної енергії України з використанням технологій та систем цифровізації. Розділ 1. Організаційні та математичні моделі взаємодії учасників децентралізованого ринку електроенергії» (ЦИФРОВІЗАЦІЯ), КПКВК 6541230.

1. Грудзинський Ю. Алгоритми та структури даних : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2022. 215 с. URL:https://ela.kpi.ua/server/api/core/bitstreams/0db974f9-16fa-459c-9f19-fab0021222ed/content (дата звернення: 20.03.2025)
2. Блінов І., Парус Є. Оптовий та роздрібний ринок електричної енергії : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2023. 291 с.
3. Про затвердження Правил ринку : Постанова Нац. коміс., що здійснює держ. регулювання у сферах енергетики та комун. послуг від 14.03.2018 № 307 : станом на 1 берез. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/v0307874-18#Text (дата звернення: 20.03.2025).

В.З. Чіхладзе, А.М. Кудін

ВИРІШЕННЯ ЗАДАЧІ БАЛАНСУВАННЯ КРИПТОВАЛЮТНОГО ПОРТФЕЛЮ В СЕРЕДОВИЩІ СМАРТ-КОНТРАКТІВ ТА DeFi

У статті розглянуто задачу балансування криптовалютного портфеля, що складається з двох активів — базового (BaseToken, наприклад, ETH) та котируємого (QuoteToken, наприклад, USDT). Умова балансування полягає в мінімізації різниці між ринковою ціною активу та усередненою вартістю його закупівлі. Це дозволяє використовувати волатильність ринку для отримання прибутку шляхом покупки активу при зниженні ціни та продажу при її зростанні.

Для формалізації задачі запропоновано **алгебру позицій**, що оперує парами виду (q, p) — кількість активу та його середня ціна. Визначено операції агрегації (об'єднання позицій) та дезагрегації (розділення), що забезпечують точний облік та автоматизацію управління портфелем у смарт-контрактах.

Запропоновано **алгоритм балансування**, що базується на чотирьох правилах:

Купівля BaseToken – здійснюється, коли ринкова ціна зменшується нижче певного порогу.

Продаж BaseToken – при зростанні ціни вище заданої межі, з урахуванням комісій та бажаного прибутку.

Недопродаж (hedge sell) – реалізується при вичерпанні ліквідності QuoteToken; дозволяє поступово виводити BaseToken частинами.

Перекупка (hedge rebuy) – зворотна агрегація активу при подальшому зниженні ціни, що зменшує усереднену вартість позиції.

Запропонований підхід дозволяє реалізувати автономне управління криптовалютним портфелем за допомогою **смарт-контрактів у DeFi**, які можуть взаємодіяти з децентралізованими біржами (Uniswap, SushiSwap) та кредитними протоколами (AAVE, Compound). Це дає змогу створювати автоматизовані фінансові стратегії без участі посередників.

1. Adams, H., Zinsmeister, N., Salem, M., Keefer, R., & Robinson, D. (2021). "Uniswap v3 Core Whitepaper." [Електронний ресурс] (https://uniswap.org/whitepaper-v3.pdf)
2. Vitalik Buterin, Zoë Hitzig, E. Glen Weyl “Liberal Radicalism: A Flexible Design For Philanthropic Matching Funds.”
3. Markowitz, H. (1952). Portfolio Selection. *The Journal of Finance*, 7(1), 77–91
4. Ethereum Foundation. ERC-20 Token Standard

І.А. Кудін

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН, ДЛЯ ОБ'ЄДНАННЯ МАЛИХ ГОСПОДАРСТВ З МЕТОЮ P2P ТОРГІВЛІ ЕЛЕКТРОЕНЕРГІЄЮ ТА СПІЛЬНОГО ПРОДАЖУ ЕЛЕКТРОЕНЕРГІЇ ТРЕТІМ СТОРОНАМ

Господарства, насамперед фізичні особи часто стикаються із проблемами при продажі малих об'ємів електроенергії за справедливими цінами. Об'єднання малих виробників дозволить торгівлю електроенергією серед учасників мережі, та навіть може зробити можливим продаж великих об'ємів електроенергії промисловим споживачам або енергетичним компаніям.[1,2]

Запропоновано спосіб для об'єднання малих господарств та фізичних осіб, у мережу блокчейн, де кожен виробник електроенергії являє собою окрему ноду. Запропоновано алгоритм консенсусу для такої мережі, що відповідає наступним умовам:

1. Відсутність тенденції до централізації
2. Визначення доброчесності(репутації) конкретного вузла
3. Прозорість та відсутність анонімізації(для довіри третіх сторін, що не є учасниками мережі)

Запропонований підхід дозволяє малим виробникам електроенергії отримати збільшити економічну вигоду від продажу надлишків електроенергії з відновлювальних джерел. Також такий підхід веде до децентралізації енергетичної мережі, що підвищує автономність та стійкість, наприклад в умовах війни.

1. Ar Aravind, Dr. G.B.Santhi, Dr. ST Patil, Mr. Selvakumar P, Gunjan Sharma, Jeetendra Dhamone, Dr. S. Ragu Nathan ,"Blockchain Technology in Energy Markets: Enabling Peer-to-Peer Energy Trading", 2024

2. Kah Yung Yap , Hon Huin Chin, Jiří Jaromír Klemeš "Blockchain technology for distributed generation: A review of current development, challenges and future prospect", 2023

3. Sergio Cantillo-Luna, Ricardo Moreno-Chuquen, Harold R. Chamorro, Vijay K. Sood, Shahriar Badsha, Charalambos Konstantinou "Blockchain for Distributed Energy Resources Management and Integration", 2022

О.С. Кушнір

МОДЕЛЬ БАЛАНСУЮЧИХ ТОРГІВ АКУМУЛЬОВАНОЇ ЕЛЕКТРИЧНОЇ ЕНЕРГІЇ ДЛЯ РОЗПОДІЛЕНИХ ЕНЕРГЕТИЧНИХ МЕРЕЖ

Стабільне функціонування енергомереж передбачає рішення задачі балансування, що мінімізує ризики аварійних ситуацій. Однією з існуючих практик рішення проблем балансування, що спирається зокрема, але не обмежуючись на досвід Сполученого Королівства, можна назвати використання систем акумуляції [1].

Чинний Закон України «Про ринок електричної енергії» декларує, що в Україні функціонує єдиний балансуючий ринок. Згідно Закону на балансуючому ринку оператор системи передачі здійснює купівлю та продаж електроенергії для балансування та з метою врегулювання небалансів електричної енергії [2]. Існуючий механізм орієнтований на централізований підхід, який ускладнює залучення до процесів балансування власників малих систем акумуляції. Варто зауважити, що велика кількість малих систем акумуляції переважає над невеликою кількістю великих систем акумуляції з точки зору безпеки. Таким чином малі системи акумуляції можуть стати однією з базових компонент розподіленої енергомережі.

Створення ринкових механізмів для максимізації прибутку власників систем акумуляції незалежно від їх розміру може збільшити обсяг стабільних джерел електроенергії для балансування споживання та балансування перевиробництва від нестабільних джерел генерації (вітрових та сонячних електростанцій). Таким механізмом могла б стати балансуюча біржа, де торги відбуваються за принципом аукціону. Сучасний український досвід створення й моделювання аукціонів для торгівлі електроенергією передбачає використання традиційного одностороннього або ж двостороннього аукціонів [3]. Враховуючи наявний на ринку попит, вигідним для власників акумуляції може бути використання більш сучасних варіацій одностороннього аукціону, а саме аукціону закритих ставок першої ціни або ж аукціону закритих ставок другої ціни (Вікрі-Кларка-Гровса), що використовуються в інтернет-маркетингу [4]. В аукціонах закритих ставок запропоновані учасниками ціни не розголошуються. Такий підхід може знизити ризики появи монополій, гнучкий з точки зору автоматизації (що може зменшити навантаження на регулятора) й уникає можливих цінових маніпуляцій.

Пропонується розглянути модель для взаємодій споживачів з власниками систем акумуляції за участі організатора біржі, що виконує обов'язки організатора аукціону. Нехай $DE = \{de_1, de_2, \dots, de_m\}$ – множина споживачів, а $SU = \{su_1, su_2, \dots su_n\}$ – множина власників систем акумуляції. $E^{su_i} = \left(v^{su_i}, b^{su_i}_{min}\right), i = \overline{1, \dots, n}$ - пропозиція продажу електроенергії, розміщена власником su_i, де v^{su_i} – обсяг електроенергії в квт., що

пропонуються для продажу, а $b_{min}^{su_i}$ – ціна однієї квт./год. $C^{de_j} = (v^{de_j}, b^{de_j})$ – заявка на купівлю від споживача de_j, де v^{de_j} – бажаний обсяг споживання de_j в квт., а b^{de_j} – ціна однієї квт./год, яку готовий сплатити споживач. Припускається, що організатор біржі може точно визначити множину $SU_{de_j} \subset SU$ власників акумуляції, які знаходяться поблизу від споживача de_j. Тоді біржові торги може відбуватись наступним чином:

0) Визначається C – як множина всіх розміщених заявок C^{de_j}, E – як множина всіх розміщених на біржі пропозицій E^{su_i}, а $E^{SU_{de_j}}$ – як множина всіх розміщених на біржі пропозицій від власників систем акумуляції з множини SU_{de_j};

1) $\forall\, SU_{de_j}, j = \overline{1, \dots, |\mathrm{DE}|}$ знаходиться $su_i \in SU_{de_j}$: $b_{min}^{su_i} = \min\left(B_{min}^{SU_{de_j}}\right)$, де $B_{min}^{SU_{de_j}}$ - множина цін $b_{min}^{su_i}$ зі всіх пропозицій множини $E^{SU_{de_j}}$;

2) $\forall\, C^{de_j}, j = \overline{1, \dots, |\mathrm{DE}|}$, порівнюється $b_{min}^{su_i} + o_{fee}$ з b^{de_j}, де o_{fee} – це будь-які комісії, що визначається організатором біржі, наприклад комісія за транспортування й обслуговування мережі;

2.1) Якщо $b_{min}^{su_i} + o_{fee} > b^{de_j}$, то заявка на купівлю не буде оброблена доки будь яким власником акумуляції з SU_{de_j} не буде розміщена нова пропозиція, тобто в множину $E^{SU_{de_j}}$ не буде додано новий елемент, такий що $b_{min}^{su_i} + o_{fee} \leq b^{de_j}$, або ж споживач $\mathrm{d}e_j$ не змінить ціну b^{de_j} в своїй заявці C^{de_j} так, щоб виконувалась аналогічна умова;

2.2) Якщо $b_{min}^{su_i} + o_{fee} \leq b^{de_j}$, то споживач $\mathrm{d}e_j$ – бере участь в аукціоні, де в якості лоту виступає можливість придбати електроенергію у власника su_i по пропозиції E^{su_i};

3) Механізм роботи аукціону:

$\forall de_i$, що бере участь в аукціоні за електроенергію розміщену на продаж пропозицією E^{su_i}, b^{de_j} вважається ставкою учасника, а B – множиною цих ставок, в аукціоні обирається переможець $de_k : b^{de_k} = max\,(B)$. Переможець аукціону – купує електроенергію, сплачуючи $max(B)$ у випадку аукціону першої ціни або ж $max(B \backslash max(B))$ у випадку аукціону другої ціни (тобто ціну другої ставки після максимальної). Заявки інших учасників аукціону залишаються в множинах E та $E^{SU_{de_j}}$;

4) Визначається гіпотетичний залишок від обсягу електроенергії, який зазначено в пропозиції $v_{new}^{su_i} = v^{su_i} - v^{de_j}$;

4.1) Якщо $v_{new}^{su_i} < 0$, то пропозиція E^{su_i} вважається виконаною, $E = E \backslash \{E^{su_i}\}$, а $C^{de_j} = (v^{de_j} - v^{su_i}, b^{de_j})$;

4.2) Якщо $v_{new}^{su_i} > 0$, то $E^{su_i} = (v_{new}^{su_i}, b_{min}^{su_i})$, $C = C \backslash C^{de_j}$, а заявка C^{de_j} вважається задовільненою;

4.3) Якщо $v_{new}^{su_i} = 0$, то пропозиція E^{su_i} вважається виконаною, $E = E \backslash \{E^{su_i}\}$, а заявка C^{de_j} вважається задовільненою, $C = C \backslash C^{de_j}$;

5) Алгоритм виконується з кроку (1);

Наявність в актуальній моделі o_{fee}, яке визначається організатором біржі може бути зручним для випадків неможливості укладання прямої угоди. o_{fee} дозволяє укладання непрямої угоди де одночасно укладається угода споживача з організатором біржі й організатора біржі з власником акумуляції, де організатор біржі отримує дохід за механізмом частки доходу (revenue share). Таким чином, як перевагу цієї моделі можна зазначити можливість для автоматизованого укладання, як прямих, так і непрямих угод. Також варто зазначити, що розглянута модель може бути реалізована на блокчейні, з записом в блокчейн інформації про кожний окремий аукціон (власник, пропозиція, учасники, їх ставки, переможець), а подібні угоди можуть бути реалізовані у вигляді смарт-контрактів.

1. Newbery D., Strengths and weaknesses of the British market model, *Handbook on Electricity Markets*, 2021, 27 p., DOI: 10.4337/9781788979955.00012

2. Верховна Рада України, Стаття 68 Закону України «Про ринок електричної енергії», *Урядовий кур'єр*, URL: https://zakon.rada.gov.ua/laws/show/2019-19#Text

3. Іванов Г.А. Побудова імітаційної моделі лібералізованого ринку електричної енергії з урахуванням особливостей функціонування ОЕС України. *Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.14.01 284 «Енергетичні системи та комплекси» (141 – Електроенергетика, електротехніка та електромеханіка)*, 2021 191 с., URL: https://uacademic.info/ua/document/0421U101102

4. Гавриленко С., Кушнір О., Пустовойт М., Модель аукціону реклами в пошукових системах та результати її впровадження, *1 міжнародна науково-практична конференція "Інформаційні системи та технології: результати і перспективи"*, 2024, С. 164-166, URL: https://ist.fit.knu.ua/_files/ugd/016074_8fc56ecbbfa94cde874eedd872f3780e.pdf

С.В. Матвєєв, І.В. Івченко

БЛОКЧЕЙН-ТЕХНОЛОГІЇ ДЛЯ ОПТИМІЗАЦІЇ ЕНЕРГОСПОЖИВАННЯ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ

Анотація Зростання використання систем штучного інтелекту (ШІ) призводить до збільшення енергоспоживання, що вимагає пошуку нових підходів до оптимізації енерговитрат. Блокчейн-технології, відомі своєю децентралізованістю та безпекою, можуть сприяти підвищенню ефективності енергоспоживання в системах ШІ. Ця стаття досліджує потенціал інтеграції блокчейну та ШІ для оптимізації енергоспоживання, аналізує існуючі рішення та перспективи розвитку в цій сфері.

Ключові слова: штучний інтелект, блокчейн, енергоспоживання, оптимізація, децентралізація.

Зростаюча популярність та впровадження систем штучного інтелекту (ШІ) у різних галузях призводить до значного збільшення енергоспоживання. Це створює виклики щодо ефективного використання енергоресурсів та зниження вуглецевого сліду. Одним із перспективних підходів до вирішення цієї проблеми є використання блокчейн-технологій, які можуть забезпечити децентралізоване управління даними та процесами, сприяючи оптимізації енергоспоживання.

Сучасні моделі ШІ, особливо глибокі нейронні мережі, вимагають значних обчислювальних ресурсів для навчання та функціонування. Це призводить до високого енергоспоживання, що стає критичним фактором при масштабуванні таких систем. Навчання складних нейронних мереж, таких як GPT-3 або AlphaGo, потребує використання великих обчислювальних кластерів. Навчання однієї такої моделі може призвести до споживання тисяч мегават-годин енергії. Наприклад, дослідження показують, що тренування моделей із сотнями мільйонів або мільярдамі параметрів вимагає використання десятків тисяч графічних процесорів (GPU) на великих дата-центрах, що значно збільшує витрати електроенергії. [1]. Наприклад, компанія DeepMind, підрозділ Google, змогла зменшити використання електроенергії у своїх центрах обробки даних на 15%. Це стало можливим завдяки обробці системою операційних даних компанії за останні кілька років, на основі яких програмою була створена модель скорочення споживання для окремих підрозділів [2].

Блокчейн-технології можуть сприяти оптимізації енергоспоживання в системах ШІ через:

- Децентралізацію обчислень: Розподіл обчислювальних задач між різними вузлами мережі зменшує навантаження на окремі центри обробки даних, що може призвести до зниження загального енергоспоживання.
- Підвищення безпеки та прозорості даних: Блокчейн забезпечує незмінність та прозорість даних, що покращує цілісність інформації, використовуваної в системах [3].

- Створення децентралізованих енергетичних ринків: Блокчейн може сприяти створенню платформ для обміну енергією між споживачами та виробниками, що дозволяє більш ефективно балансувати попит та пропозицію на енергетичних ринках.

Використання блокчейн технологій в енергетичному секторі зростає Одна з найвідоміших блокчейн-компаній LO3 Energy має багатий досвід створення рішень для енергомереж, що охоплюють лічильники електроенергії, з'єднані з комп'ютерними пристроями, що вимірюють обсяг і якість електроенергії, та взаємодіють з іншими пристроями у мережі для активації енергетичних транзакцій. Споживачі реалізовують свої потреби за допомогою мобільного додатку, де вони мають можливість обрати бажаний вид генерації та ціну, яку готові платити. У свою чергу, іспанська енергокомпанія ACCIONA Energía використовує блокчейн для підтвердження походження електроенергії з ВДЕ [4]. У Чилі Національна енергетична комісія запустила блокчейн-проєкт, використовуючи технологію Ethereum для безпечного запису, зберігання та моніторингу даних, пов'язаних з енергоспоживанням [5]. Це сприяє підвищенню прозорості та ефективності в енергетичному секторі. Крім того, компанія Velas (VLX) використовує ШІ для оптимізації блокчейнів, скорочуючи витрати на енергоспоживання. Це демонструє потенціал інтеграції ШІ та блокчейну для підвищення енергоефективності.

Інтеграція блокчейн-технологій та систем штучного інтелекту має значний потенціал для оптимізації енергоспоживання. Децентралізація обчислень, підвищення безпеки та прозорості даних, а також створення децентралізованих енергетичних ринків можуть сприяти ефективнішому використанню енергоресурсів. Подальші дослідження та впровадження таких інтеграцій можуть призвести до значних покращень у сфері енергоефективності та сталого розвитку.

1. Alexandra Sasha Luccioni, Sylvain Viguier, Anne-Laure Ligozat (3 November, 2022) Carbon Footprint of BLOOM *arXiv:* https://arxiv.org/pdf/2211.02001v1

2. IT технології: застосування в електроенергетиці. *Kosatka. Media.* (20 бер. 2020) https://kosatka.media/uk/category/blog/news/it-tehnologii-primenenie-v-elektroenergetike

3. Штучний інтелект і блокчейн: тонкощі інтеграції та перспективи. (29 січня 2024). *Cryptomus Blog*. https://cryptomus.com/uk/blog/at-the-intersection-of-ai-and-blockchain-promising-applications-emerge?srsltid=AfmBOoo35zowDVjp1__wzHW1qoeidKpof-_ru1DOQzXAQyZw8Yx9HiaE

4. The software and IoT revolution for an energy-efficient HVAC-R / *Beebryte*. https://www.beebryte.com/

Б.М. Плескач, В.Д. Самойлов, Є.В.Новак

ВИКОРИСТАННЯ БЛОК-ЧЕЙН ТЕХНОЛОГІЇ В ЛОКАЛЬНІЙ ЕЛЕКТРИЧНІЙ МЕРЕЖІ З МОДУЛЬНОЮ СОНЯЧНО-ВІТРЯНОЮ ЕЛЕКТРОСТАНЦІЄЮ

Давно відомі блочні електростанції та котельні, змонтовані на базі побутових вагончиків або контейнерів. Їх перевагами, у порівнянні зі звичайними електростанціями та ТЕЦ є простота розгортання та значно менша вартість виготовлення в порівнянні з будівництвом при аналогічних потужностях.

Такі електростанції використовуються як основні або резервні джерела електроенергії у важкодоступних місцях для повного або часткового покриття електричних навантажень промислових, житлових і соціальних об'єктів. Силовими установками в блочних електростанціях є двигуни внутрішнього згоряння або газові турбіни.

Подальшим кроком у підвищенні енергоефективності виробництва електроенергії стало об’єднання в одному блоці електростанції та котельні в єдину когенераційну установку, в якій електростанція доповнена котлом-утилізатором. ККД такої установки, за рахунок котла-утилізатора, досягає 90%, але недоліком є необхідність спалювання органічного палива - мазуту, газу, або інших викопних палив.

Подальший розвиток мобільних модульних електростанцій пішов у напрямку використання альтернативних джерел енергії. Прикладом такої установки є мобільна сонячно-вітряна електростанція MASWES ™, яка призначена для забезпечення електроенергією невеликих господарств, або громад, і може використовуватися як в режимі підключення до центральної електромережі, так і повністю автономно від неї.

Рисунок 1 – Мобільна автономна сонячно-вітряна електростанція MASWES™ (20,5 кВт)

До складу MASWES™ входять два вітрогенератори, набір сонячних панелей, відповідні інвертори, акумуляторні батареї з контролерами заряду та станції заряду електромобілів. Потужність таких модульних сонячно-вітряних зарядно-генеруючих станцій складає 59, 32, і 20,5 кВт. Перший етап практичних випробувань зразка-прототипу такої електростанції потужністю 20,5 кВт вже завершено в умовах гірського району Закарпаття. Ця електростанція впродовж місяця забезпечувала живлення об'єкту готельного типу.

Впровадження подібних модульних електростанцій різної потужності дозволяє створювати локальні електричні мережі різної конфігурації із підключенням мобільних електростанцій як безпосередньо до окремого споживача, так і на шини низької напруги трансформаторної підстанції, знижуючи таким чином залежність від централізованих мереж [1] .

Такі мікромережі для забезпечення надійності, оптимального використання ресурсів, економічної вигоди та стійкості до відключень потребують ефективного управління. Таке управління може здійснюватись або за допомогою інтелектуальних систем моніторингу, або технологій блокчейн.

Розглянемо можливі варіанти управління локальними мережами до складу яких входять джерела відновлюваної енергії, віртуальні електростанції, та інші модульні джерела енергії. Умовно їх можна розділити на три групи. Це блокчейн платформи для торгівлі енергією, централізовані платформи без блокчейну, і платформи для peer-to-peer (P2P) торгівлі енергією.

До першої групи відносяться платформи:

- **WePower (WPR)** – це блокчейн-платформа, що токенізує енергію, дозволяючи її купувати, продавати та інвестувати в проєкти відновлюваної енергетики через смарт-контракти.
- **Electron** – це британська компанія, яка використовує блокчейн для управління децентралізованими енергетичними ринками. Вона зосереджується на ефективному балансуванні енергосистеми, торгівлі гнучкістю (demand-side flexibility) і інтерактивних мікромережах.
- **Power Ledger**—це блокчейн-платформа для децентралізованої торгівлі енергією,

До другої групи централізованих платформ без блокчейну можна віднести:

- **AutoGrid** – аналізує споживання та виробництво енергії для оптимізації мікромереж.
- **Schneider Electric (EcoStruxure Microgrid Advisor)** – інтелектуальна система управління мікромережею, що дозволяє вибирати джерела енергії для мінімізації витрат.

Платформи для P2P, головна мета якої тільки торгівля електроенергією:

- **Grid Singularity** – децентралізована біржа для торгівлі енергією на блокчейні.

- **SunContract** – P2P-платформа для продажу енергії без посередників.

Попередній аналіз показав, що кожна з цих платформ має свої переваги і недоліки. Але у нашому випадку перевагу можна віддати блок-чейн платформі **Power Ledger,** яка формує однорангові транзакції енергії, записуючи як генерацію, так і споживання всіма учасниками платформи в режимі реального часу.

Power Ledger має гібридну блокчейн-архітектуру, яка включає:

- **Ethereum (публічний блокчейн)** – використовується для токенізації активів та фінансових розрахунків.
- **EcoChain (приватний блокчейн)** – швидший та дешевший для обліку мікротранзакцій енергії.

Виробництво та використання енергії здійснюється за попередньо встановленими ставками. Платформа Power Ledger працює на двох рівнях блокчейну та використовує дві монети: токен Power Ledger (POWR) і Sparkz. POWR і Sparkz використовуються в системі та мають різні функції в обох блокчейнах. Платформа використовує публічний блокчейн Ethereum, а також блокчейн приватного консорціуму EcoChain.

Платформа передбачає два основних токени:

- **POWR** – основний токен, що використовується для доступу до мережі Power Ledger.
- **Sparkz** – внутрішній токен для обліку електроенергії, прив'язаний до місцевої валюти.

Токени дозволяють купувати/продавати електроенергію між користувачами (peer-to-peer) та автоматизувати платежі через смарт-контракти. Коли споживач хоче купити енергію, система автоматично виконує угоду через смарт-контракт. При цьому генерується транзакція з обраною ціною та обсягом, перевіряється баланс та доступність енергії, якщо умови виконані, записується обмін:

- Покупець отримує енергію (у фізичній мережі).
- Продавець отримує токени Sparkz.

Sparkz можна обміняти на фіатні гроші або POWR-токени.

Платформа передбачає інтегрування зі смарт-лічильниками або IoT-сенсорами, які реєструють в реальному часі.

- Генерацію електроенергії (сонячні панелі, вітряні турбіни),
- Залишок заряду акумуляторів,
- Споживання електроенергії кожним учасником мережі
- Вартість електроенергії у централізованій системі.

Дані з лічильників записуються в блокчейн, забезпечуючи прозорість транзакцій. Система підтримує динамічне ціноутворення, що дозволяє користувачам торгувати енергією залежно від попиту та пропозиції.

Використання **Smart Contracts Power Ledger** дозволяє визначати найбільш економічно вигідне для споживача джерела електроенергії. Наприклад, можна встановити правило:

- Якщо генерація сонячної енергії достатня → Використовуємо її

- Якщо вітряна генерація достатня - Використовуємо її,
- Якщо недостатня, але заряд акумуляторів високий → Використовуємо акумулятори
- Якщо альтернативні джерела не можуть покрити потреби → Підключаємо централізовану мережу

Інтеграція в **Smart Contracts** прецедентного метода машинного [2] навчання може зробити вибір джерела енергії більш ефективним для прогнозування:

- Споживання електроенергії на основі історичних даних
- Генерації енергії з урахуванням погоди
- Відслідковування тарифів на електроенергію

Висновки: Блок-чейн платформи, зокрема Power Ledger, поєднує блокчейн, смарт-контракти та токенізовану економіку для створення **децентралізованого ринку електроенергії**. Це дозволяє споживачам взаємодіяти напряму, оптимізуючи витрати та зменшуючи залежність від централізованих енергокомпаній.

1. Н. П. Савченко, А. В. Трет’як, О. М. Довгалюк Перспективи застосування мобільних електростанцій як джерел розосередженої генерації у локальних електричних мережах. Системи управління, навігації та зв'язку. 2023. № 4

2. Плескач Б.М. Застосування методу моделювання прецедентів для моніторингу енергетичного стану технологічного обладнання. Електронне моделювання, 2018, т.40, №4, с. 95-104.

Д.І. Симонов, Б.Ю. Заіка, Є.Д. Симонов

ВИКОРИСТАННЯ МАШИННОГО НАВЧАННЯ ДЛЯ ПІДВИЩЕННЯ БЕЗПЕКИ БЛОКЧЕЙН-ПРОЄКТІВ У СФЕРІ ЕНЕРГЕТИКИ

У сучасному світі технології блокчейну знаходять широке застосування в різних галузях, зокрема в енергетиці. Їхня децентралізована та прозора природа сприяє підвищенню ефективності, надійності та безпеки енергетичних систем. Однак зростаюча складність смарт-контрактів і фінансових механізмів, зокрема P2P-торгівлі енергією та DeFi-рішень для фінансування відновлюваних джерел енергії, підвищує їхню вразливість до кібератак. Водночас упродовж останніх років науковці активно досліджують можливості поєднання технологій блокчейну та штучного інтелекту для вдосконалення різних аспектів систем [1]. У цьому контексті особливо актуальним є дослідження застосування машинного навчання для підвищення безпеки блокчейн-проєктів, зокрема в критично важливій сфері енергетики, де будь-які збої можуть мати серйозні наслідки.

Аналіз транзакцій для виявлення аномалій є одним із прикладів використання машинного навчання для посилення безпеки енергетичних блокчейн-проєктів. Розробка моделей для аналізу послідовностей транзакцій у мережі дає змогу виявляти підозрілі закономірності, що можуть свідчити про потенційні атаки або спроби маніпуляцій у системі P2P-торгівлі електроенергією. Для визначення аномалій можуть застосовуватися різні алгоритми та моделі машинного навчання, зокрема Isolation Forest, K-Means, Random Forest [2, 3].

Використання NLP-моделей для аналізу вихідного коду смартконтрактів, що застосовуються в енергетичних платформах, дає змогу автоматично виявляти типові вразливості (повторне входження, переповнення чисел тощо) ще до їх розгортання. Поєднання NLP-моделі CodeBERT для текстового аналізу з додатковою структурною інформацією, отриманою із графів керування потоком на основі абстрактного синтаксичного дерева та операційного коду смартконтрактів, дало змогу визначати критичні шляхи коду та забезпечило високу точність виявлення вразливостей [4]. Комбінування технології фільтрації ключових слів, попередньо навченої моделі BERT та архітектури BiLSTM-CRF (Bidirectional Long Short-Term Memory – Conditional Random Field) також підвищило ефективність і точність виявлення вразливостей у смартконтрактах [5].

Машинне навчання також можна застосовувати для прогнозування кіберзагроз у блокчейн-проєктах енергетики. Інтеграція алгоритмів класифікації для аналізу логів і мережевих даних дає змогу прогнозувати ймовірність появи кібератак, що забезпечує своєчасне втручання та захист критичних елементів інфраструктури. Поєднання моделей глибокого навчання RNN (Recurrent Neural Networks) і CNN (Convolutional Neural

Networks) продемонструвало високу ефективність у розпізнаванні шаблонів і адаптації до динамічних методів атак [6]. У статті [7] автори запропонували ефективну кластерну архітектуру для виявлення аномалій у поєднанні з декількома моделями машинного навчання у федеративному середовищі.

До основних переваг застосування методів машинного навчання для забезпечення безпеки блокчейн-проєктів у сфері енергетики належать:

1. *Автоматичне виявлення аномалій та загроз*. Методи машинного навчання дають змогу розробляти алгоритми, здатні аналізувати великі обсяги даних і виявляти нетипову поведінку в мережі чи транзакціях [2, 3].

2. *Адаптивність*. Моделі, що використовують методи глибокого навчання, можуть адаптуватися до змін у поведінці зловмисників, що дає змогу підтримувати високий рівень безпеки навіть за появи нових типів атак [6].

3. *Підвищення ефективності реагування*. Автоматизація аналізу даних дає змогу зменшити час виявлення потенційних загроз і, відповідно, скоротити час реакції системи. Це особливо важливо для енергетичних проєктів, де збої можуть мати критичні наслідки [7].

4. *Інтеграція з іншими системами безпеки*. Аналітичні платформи на базі машинного навчання можуть взаємодіяти з системами моніторингу та управління інфраструктурою, забезпечуючи комплексний підхід до кібербезпеки [7].

Серед основних проблем використання методів машинного навчання для забезпечення безпеки блокчейн-проєктів у сфері енергетики можна виділити такі:

1. *Потреба у великих і якісних даних*. Для навчання ефективних моделей необхідний доступ до значних обсягів історичних даних. Незбалансованість або низька якість таких даних можуть спричинити неточні прогнози та помилкові спрацьовування. На практиці отримати великий обсяг розмічених даних складно, оскільки частка аномальних випадків у них зазвичай низька. Для розв’язання цієї проблеми застосовують методи зменшення вибірки (undersampling), збільшення вибірки (oversampling), SMOTE (Synthetic Minority Over-sampling Technique) та напівкероване навчання [8, 9].

2. *Інтерпретація результатів*. Деякі моделі, зокрема глибокі нейронні мережі, є занадто складними для інтерпретації їхньої логіки, що ускладнює аналіз прийнятих рішень і може впливати на рівень довіри до автоматизованих систем безпеки. Для підвищення прозорості таких моделей розробляють спеціальні алгоритми, серед яких Grad-CAM (Gradient-weighted Class Activation Mapping) та SHAP (SHapley Additive exPlanations) [10, 11].

3. *Децентралізованість та безпека даних*. Методи машинного навчання повинні враховувати такі особливості блокчейн-проєктів, як децентралізований характер системи та вимоги до захисту даних. Для цього застосовують спеціалізовані підходи, зокрема федеративне навчання (метод, у якому декілька незалежних учасників спільно навчають модель, передаючи

свої дані децентралізовано) та розподілене машинне навчання (Distributed Machine Learning, DML) [12, 13].

Підсумовуючи, машинне навчання є ефективним інструментом для підвищення безпеки блокчейн-рішень в енергетиці, оскільки воно дозволяє автоматизувати виявлення аномалій, прогнозувати кіберзагрози, аналізувати вихідний код смарт-контрактів і інтегруватися з іншими системами кібербезпеки. Його застосування забезпечує можливість аналізу великих обсягів даних у реальному часі, адаптацію до нових атак, підвищення швидкості реагування на інциденти та інтеграцію з комплексними системами моніторингу. Однак, попри значний потенціал, існують серйозні виклики, зокрема потреба у великих і якісних наборах даних, складність інтерпретації рішень глибоких нейронних мереж та необхідність адаптації методів машинного навчання до децентралізованого середовища блокчейну з урахуванням безпеки та приватності даних. Вирішення зазначених проблем потребує розробки нових підходів до обробки даних, інтерпретації складних моделей та спеціалізованих методів навчання для блокчейн-проєктів.

1. Al Shareef, A. M., Seçkiner, S., Eid, B., & Abumeteir, H. (2024). Integration of blockchain with artificial intelligence technologies in the energy sector: a systematic review. *Frontiers in Energy Research*, *12*, 1377950. https://doi.org/10.3389/fenrg.2024.1377950

2. Siddamsetti, S., Tejaswi, C., & Maddula, P. (2024). Anomaly Detection in Blockchain Using Machine Learning. *Journal of Electrical Systems*. https://doi.org/10.52783/jes.2988.

3. Solomka, I., Liubinskyi, B., & Torshyn, V. (2024). Application of machine learning algorithms to enhance blockchain network security. *Mathematical Modeling and Computing*. https://doi.org/10.23939/mmc2024.03.893.

4. Choi, R., Song, Y., Jang, M., Kim, T., Ahn, J., & Im, D. (2025). Smart Contract Vulnerability Detection Using Large Language Models and Graph Structural Analysis. *Computers, Materials & Continua*. https://doi.org/10.32604/cmc.2025.061185

5. Lin, C., Wang, X., & Lin, H. (2024). Elevating Smart Contract Defenses: A Coordinated NLP-Based Strategy for Vulnerability Detection. *2024 IEEE International Conferences on Internet of Things (iThings) and IEEE Green Computing & Communications (GreenCom) and IEEE Cyber, Physical & Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics*, 90-97. https://ieeexplore.ieee.org/document/10731796

6. Nagarjun, A., & Rajkumar, S. (2024). Design of an Anomaly Detection Framework for Delay and Privacy-Aware Blockchain-Based Cloud Deployments. *IEEE Access*, 12, 84843-84862. https://doi.org/10.1109/ACCESS.2024.3414998.

7. Yazdinejad, A., Dehghantanha, A., Parizi, R., Hammoudeh, M., Karimipour, H., & Srivastava, G. (2022). Block Hunter: Federated Learning for Cyber Threat Hunting in Blockchain-Based IIoT Networks. *IEEE Transactions on Industrial Informatics*, 18, 8356-8366. https://doi.org/10.1109/TII.2022.3168011.

8. Wongvorachan, T., He, S., & Bulut, O. (2023). A comparison of undersampling, oversampling, and SMOTE methods for dealing with imbalanced classification in educational data mining. *Information*, *14*(1), 54. https://doi.org/10.3390/info14010054

9. Yershov, S. and Zaika, B. (2025) Leveraging unlabeled data to enhance uplift meta-learners: A general approach for S-learner and T-Learner, *Наука і техніка*

сьогодні, 1(42), pp. 1000–1019. https://doi.org/10.52058/2786-6025-2025-1(42)-1000-1019.

10. Quach, L. D., Quoc, K. N., Quynh, A. N., Ngoc, H. T., & Thai-Nghe, N. (2024). Tomato health monitoring system: Tomato classification, detection, and counting system based on YOLOv8 model with explainable MobileNet models using Grad-CAM++. *IEEE Access, 12*, 9719-9737. https://ieeexplore.ieee.org/document/10385083

11. Симонов, Д. І., Заіка Б. Ю., & Симонов, Є. Д. (2024). МУЛЬТИВИХІДНІ РЕГРЕСІЙНІ МОДЕЛІ ДЛЯ УПРАВЛІННЯ БАГАТОКОМПОНЕНТНИМИ ДИНАМІЧНИМИ СИСТЕМАМИ. Таврійський науковий вісник. Серія: Технічні науки, (6), 106-119. https://doi.org/10.32782/tnv-tech.2024.6.12

12. Sun, Y., Li, Z., Li, Y., & Ding, B. (2024). Improving LoRA in Privacy-preserving Federated Learning. *ArXiv, abs/2403.12313*.

13. Liu, R., & Pan, J. (2024). CRS: A Privacy-Preserving Two-Layered Distributed Machine Learning Framework for IoV. *IEEE Internet of Things Journal, 11*, 1080-1095. https://ieeexplore.ieee.org/document/10158345

П.С. Чернишов, М.М. Ковальов

ЄCITY: БЛОКЧЕЙН-АРХІТЕКТУРА ЯК ОСНОВА ДЕЦЕНТРАЛІЗОВАНОГО УПРАВЛІННЯ ЕНЕРГОСПОЖИВАННЯМ ТА МОБІЛЬНІСТЮ У СМАРТ-МІСТАХ

Актуальність теми. У XXI столітті міста стикаються з критичними викликами: неефективне енергоспоживання, хаотичний транспортний потік. Паралельно з цим стрімко зростає потреба в цифровій трансформації урбаністичного простору, яка базується на принципах децентралізації, прозорості, енергоефективності та сталої мобільності.

Блокчейн-технології, зокрема у формі дистрибутивних реєстрів (DLT), здатні забезпечити прозоре управління транспортними потоками, енергетичними витратами, винагородами для користувачів, а також гарантувати достовірність та безпеку обміну даними між інфраструктурними об’єктами.

Мета та завдання дослідження. Проєкт «ЄCity» покликаний:

1. Впровадити інтелектуальну платформу міської мобільності, що базується на IoT + блокчейн + штучному інтелекті.
2. Забезпечити цифровий контроль зокрема в транспортній екосистемі.
3. Стимулювати сталу поведінку користувачів через токенізацію та винагороди у блокчейн-гаманці.
4. Розробити смарт-контрактні протоколи для автоматизованої взаємодії між громадським транспортом, пішоходами, паркувальними системами та муніципалітетом.

Наукові положення та інновації.

1. Блокчейн як енергетичний балансувальник міста:

- створення енергетичного профілю для транспортного вузла (на основі сенсорних даних про навантаження, споживання, час простою);
- застосування орієнтованих графів для моделювання потоків енергії та мобільності;
- використання динамічних NFT для ідентифікації об’єктів інфраструктури .

2. Цифровий токен для стимулювання сталого пересування:

- введення внутрішнього токена $CityCoin, що нараховується користувачам за: використання громадського транспорту, зменшення викидів CO_2;
- токен витрачається на оплату проїзду, знижки, доступ до паркінгу та інші послуги;

3. Децентралізоване управління паркуванням і енергією:

- смарт-контракти для динамічного тарифу на паркування залежно від завантаження;

- оптимізація енергоспоживання зарядних станцій (EV) на основі даних блокчейн-аналітики.

4. Інтеграція з енергомережами:

- потенційна синергія з Peer-to-Peer енерготрейдингом, де токени $CityCoin можуть бути використані в мікрогрідах;

- смарт-контракти забезпечують миттєвий розрахунок і баланс попиту-пропозиції.

Пілотна реалізація.

Україна — Львів:

- Франківський, Шевченківський, Галицький райони
- 19 розумних паркомісць, 1000+ Beacon-зон, інтеграція з транспортом

Швейцарія — Цюрих:

- Центр та район Альтштадт
- Транспортна децентралізація та кешбек для пішоходів і туристів

Висновки. Проєкт «ЄCity» демонструє мультидисциплінарну синергію між блокчейн-технологіями, енергетичним менеджментом, міською логістикою, урбаністикою та поведінковою економікою. Він є практичним прикладом інтеграції цифрового активу у міське середовище та відкриває нові горизонти для децентралізованого управління енергією в умовах Smart City.

К.В. Васильєв

МЕТОДИ КІБЕРЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЗА ДОПОМОГОЮ ШІ

Критична інформаційна інфраструктура (КІІ) відіграє ключову роль у забезпеченні сталого функціонування систем та стабільності держав. Однак цифровизація фінансової галузі, що зростає, і впровадження інноваційних технологій відкривають нові вектори атак для зловмисників. Сучасні кібератаки стають дедалі витонченішими, а традиційні засоби захисту виявляються неефективними проти нових, раніше невідомих загроз. Виникає гостра потреба у більш гнучких та інтелектуальних системах забезпечення кібербезпеки. Таким чином, предметом дослідження є сучасні інтелектуальні методи та технології захисту критичної інформаційної інфраструктури (КІІ) від кібератак.

Використання штучного інтелекту (ШІ) у математичних моделях кіберзахисту може значно покращити ефективність захисту від нових та невідомих загроз.

Штучний інтелект (ШІ) може бути використаний для захисту інформаційних систем від кібератак. Методи кіберзахисту можна класифікувати за різними критеріями: за рівнем захисту, за способом реалізації, за об’єктами захисту.

За рівнем захисту, а саме превентивні методи (запобігання атакам) що включають в себе:

– автоматичне управління ідентичностями та доступом (AI-driven IAM);

– адаптивна багатофакторна аутентифікація (MFA);

– AI-аналіз мережевого трафіку для раннього виявлення загроз;

– виявлення та виправлення вразливостей за допомогою AI;

– методи виявлення та реагування;

– методи відновлення після атак, а саме автоматизоване реагування на інциденти (SOAR – Security Orchestration,Automation, and Response);

– AI-оптимізовані системи резервного копіювання та відновлення;

– самовідновлювані мережеві структури на основі AI.

За способом реалізації:

– алгоритмічні методи, що включають в себе глибоке навчання (Deep Learning) для аналізу шкідливих програм, нейронні мережі для прогнозування атак та байєсівські моделі для аналізу ймовірності загроз;

– автоматизовані методи для патчування вразливостей;

– роботизовані системи для аналізу логів безпеки;

– генеративні AI-моделі для розробки захисних сценаріїв.

За об’єктами захисту користувачів та їхніх даних, мережевої інфраструктури та хмарних технологій та IoT.

А також існують такі методики.

Методика захисту на основі машинного навчання. Машинне навчання – це метод використання ШІ для навчання системи розпізнавати особливості кібератак та визначати реакцію на них. У цій методиці ШІ вчиться розпізнавати потенційно небезпечні дії, пов'язаніз кібератаками, і приймати рішення щодо захисту системи. Цей підхід дозволяєвиявлятинові типи кібератак,ранішеневідомі,іадаптувати систему захисту до нових загроз.

Методика захисту на основі аналізу поведінки. Цей підхідгрунтуєтьсяна тому, що кіберзлочинці мають власний стиль атаки, отже, ШІ може вивчити цей стиль та розпізнавати атаки на основі їх поведінки.У цій методиці ШІ аналізує поведінку користувачів і системи для виявлення незвичайних дій,які можуть бути пов'язаніз кібератаками. Цей підхід також дозволяє виявляти нові типи кібератак і захищати систему від них.

Управління ідентичностями та доступом де ШІ аналізує поведінкові шаблони користувачів, щоб виявити аномальні дії, які можуть вказувати на компрометацію облікових записів. Наприклад, системи машинного навчання можуть ідентифікувати нетипові спроби входу, такі як підключення з незвичних місць або пристроїв. Використовується багатофакторна автентифікація (MFA) з адаптивним AI-контролем.

Захист кінцевих точок де ШІ допомагає у виявленні шкідливого програмного забезпечення та інших загроз на пристроях користувачів (комп’ютерах, смартфонах тощо). Антивірусні та EDR-системи (Endpoint Detection and Response) використовують AI для поведінкового аналізу програм та автоматичного блокування підозрілої активності.

Хмарні середовища стають основною ціллю кібератак, тому AI-моделі аналізують вхідний і вихідний трафік для виявлення потенційних загроз. Використовується AI-контроль доступу, шифрування та автоматичний аналіз логів для швидкого реагування на інциденти.

ШІ допомагає аналізувати великі обсяги даних у режимі реального часу та розпізнавати аномалії, що можуть свідчити про кібератаку. Наприклад, SIEM-системи (Security Information and Event Management) інтегрують AI для виявлення підозрілих патернів у мережевому трафіку та поведінці користувачів.

ШІ дозволяє ідентифікувати, класифікувати та захищати конфіденційну інформацію. Наприклад, AI-системи можуть автоматично визначати документи, що містять персональні дані, і застосовувати до них необхідний рівень безпеки (наприклад, шифрування або обмеження доступу).

Ці методи допомагають значно підвищити рівень безпеки критичної інфраструктури, забезпечуючи автоматизований моніторинг та реагування на загрози.

1. Microsoft. (n.d.). *What is AI for cybersecurity? Microsoft Security.* Retrieved March 23, 2025, from https://www.microsoft.com/uk-ua/security/business/security-101/what-is-ai-for-cybersecurity

2. Nachasi. (2019, January 31). *Як працює machine learning та його застосування на практиці.* Retrieved from https://nachasi.com/tech/2019/01/31/yak-pratsyuye-machine-learning/

3. Science LPNU. (2023). *Забезпечення кібербезпеки систем штучного інтелекту: Аналіз вразливостей, атак і контрзаходів.* Retrieved March 23, 2025, from https://science.lpnu.ua/sites/default/files/journal-paper/2023/jan/29738/221029maket-9-24.pdf

4. Vinnytsia National Technical University (VNTU). (2024). *Застосування штучного інтелекту для виявлення та реагування на кіберзагрози.* Retrieved March 23, 2025, from https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/42057/20610.pdf

5. 10Guards. (n.d.). *Як ШІ бореться з ключовими кіберзагрозами.* Retrieved from https://10guards.com/ua/articles/how-ai-handles-top-cybersecurity-threats/

A. Davydiuk, S. Kulyk

CLOUD DATA MIGRATION SECURITY

Migration to cloud technologies has become an integral part of the modern business environment, providing organizations with flexibility, scalability and cost-effectiveness. However, the process of transferring data to the cloud is accompanied by several challenges, among which ensuring the integrity and confidentiality of information are a priority. In war conditions, backup processes and data migration to the cloud become especially important. Thanks to these processes, it is possible to protect data from destruction as a result of massive kinetic attacks and cyberattacks. More and more organizations are choosing cloud solutions instead of local environments. According to 2022 data, 93% of technology leaders reported that their organizations rely primarily on cloud solutions in various forms, compared to 83% two years ago, and 48% say that their infrastructure is primarily hybrid, compared to 40% two years ago. At the same time, the number of respondents who indicated that their organizations mainly use on-premises environments has halved to 7% [1].

In times when data volumes are only growing, cloud migration processes will become more frequent. At the same time, the war in Ukraine is an example of stress testing for such a process. In particular, in conditions of physical destruction of data carriers, many organizations have begun cloud migration of various data centers, both Ukrainian and foreign, almost simultaneously with a full-scale invasion.

In Ukraine, the main document regulating the issue of cloud services is the Law of Ukraine “On Cloud Services”. This law regulates legal relations arising from the provision of cloud services and establishes the features of their use by state authorities. It defines requirements for security and data protection when using cloud services [2].

The State Service of Special Communications and Information Protection of Ukraine (SSSCIP) also developed relevant recommendations and approved them by Order of the State Service for Special Communications Administration dated September 14, 2024 No. 505 “On approval of Methodological recommendations for ensuring cyber security when using cloud computing technology and Methodological recommendations for assessing the compliance of cloud services with security (assurance) levels” [3]. These recommendations contain measures and practices for ensuring cybersecurity when using cloud technologies.

Regarding international standards, it is worth mentioning ISO/IEC 27001, which sets requirements for the implementation, maintenance and improvement of an information security management system [4]. ISO/IEC 27017 - provides additional recommendations for information security controls for cloud service providers and consumers [5]. ISO/IEC 27018 focuses on the protection of personal data in cloud environments, providing guidelines for the processing of personal information [6].

In addition to Ukrainian documents and international standards, for this study, it is advisable to consider the following regional industry documents. Among them, one can identify NIST SP 800-53, which provides detailed recommendations on security and privacy measures for information systems and organizations, including those using cloud technologies. It covers a wide range of controls aimed at protecting information and ensuring its integrity during migration to and from the cloud [7]. NIST SP 800-144 contains recommendations on security and privacy when using public cloud computing. It focuses on the risks associated with the transfer and storage of data in the cloud environment and offers strategies for minimizing them [8]. The Uptime Institute Data Center Risk Assessment (DCRA) is designed to provide IT leaders and staff with an in-depth assessment of all risks associated with delivering IT services in any given data center, looking at technology, processes, and the people and skills involved. The DCRA is the industry's most strategic review of any data center to determine its ability to meet business needs [9]. Based on the principles outlined in the Uptime Institute's Tier Standard [10], the DCRA carefully examines the existing topology of a critical facility and all associated operational plans, then formulates a written, unbiased assessment of the expected performance of the Tier Standard structure under all specified operating conditions. The assessment also includes recommendations for mitigating and closing any gaps to align the data center infrastructure and operations with business requirements.

The Uptime Institute's Tier Standard: Operational Sustainability defines behaviors and risks beyond the Tier Classification System (I, II, III, IV) that impact the long-term performance of a data center. This standard integrates data center management behaviors with the functionality of the data center infrastructure layer to achieve an organization's business goals or mission imperatives [10].

The Law of Ukraine "On Cloud Services" is a national legislative document that regulates legal relations in the provision of cloud services [2]. It defines the requirements for security and data protection, ensuring data security when using cloud services. It also sets specific requirements for government agencies. However, while it covers legal aspects, it does not specify detailed technical measures for migration.

The Order of the Administration of the SSSCIP No. 505, issued on September 14, 2024, is an order from a government body that provides methodological recommendations on cybersecurity in cloud computing. It also outlines the assessment of cloud services' compliance with security levels. This document identifies measures and practices to ensure cybersecurity during data migration to the cloud, with a particular focus on security considerations when transitioning to cloud technologies.

The ISO/IEC 27001 is an international standard that establishes requirements for implementing, maintaining, and improving an information security management system. It serves as a framework for assessing and managing data security risks during cloud migration. This standard is applicable to all types of information systems, making it widely adopted across various industries.

The ISO/IEC 27017 is another international standard that provides recommendations for information security controls, specifically for cloud service providers and consumers. It supports data security and risk management in cloud environments by offering additional guidance on securing cloud infrastructure.

The ISO/IEC 27018 is an international standard that focuses on the protection of personal data in cloud environments. It provides guidelines for processing personal information and ensures confidentiality and data protection during migration. This standard is particularly aimed at safeguarding personal data and ensuring compliance with privacy regulations.

The NIST SP 800-53 is a regional industry standard that offers detailed recommendations for security and privacy measures for information systems. It plays a crucial role in protecting information during cloud migration and facilitates secure interactions between different cloud services. The high level of detail in this standard makes it essential for ensuring the security of information systems.

The NIST SP 800-144 is another regional industry standard that addresses security and privacy concerns related to public cloud computing. It provides a framework for risk assessment and outlines security strategies specifically designed for public cloud environments. This document is particularly useful for assessing and mitigating risks associated with public clouds.

The Uptime Institute Data Center Risk Assessment (DCRA) is an industry standard that focuses on evaluating risks in data centers providing IT services. It helps identify potential risks associated with cloud data centers and data migration, ensuring that organizations can take preventive measures to mitigate these risks effectively.

Finally, the Uptime Institute's Tier Standard: Operational Sustainability is an industry standard that assesses the sustainability of data center operating standards. It evaluates the ability of data centers to meet data migration and storage requirements while ensuring operational sustainability and compliance with business needs.

Ukraine's example of migrating to AWS is unique given the time and volume of data. In particular, Amazon Web Services helped Ukrainian ministries and enterprises transfer over 10 petabytes of data to secure servers, from land registry and banking information to university curricula. The information was transported in special AWS Snowball "suitcases" that arrived in Ukraine on Sunday, the third day of a full-scale war. Since then, AWS has provided migration to the "cloud" of sensitive information for 27 Ukrainian ministries, as well as dozens of educational institutions and private companies. Currently, 61 government data migrations from Ukraine are underway, and more are expected [11].

Despite detailed guidelines provided by existing standards, data centers remain vulnerable, particularly during data migration to the cloud. Key threats include Man-in-the-Middle (MITM) attacks, leading to data leaks and unauthorized modifications. Protective measures against MITM include TLS 1.3, VPN, IPSec, and HSTS certificates.

Another major issue is unsecured APIs, potentially resulting in unauthorized access and data theft. Countermeasures involve OAuth 2.0, Web Application

Firewalls (WAF), and rate limiting for API requests. Data leaks due to insufficient access controls or misconfigured cloud storage remain common. Effective mitigation strategies include AES-256 encryption, robust Identity and Access Management (IAM), and Zero Trust Architecture.

Cloud migrations are also susceptible to Distributed Denial of Service (DDoS) attacks, causing disruptions or incomplete transfers. Employing DDoS protection solutions such as Cloudflare or AWS Shield is crucial. Malware threats necessitate pre-migration audits to identify vulnerabilities and prevent infections.

Challenges arise from incompatible security policies across cloud platforms and a lack of unified security standards. Implementing centralized management systems like Cloud Security Posture Management (CSPM) and adhering strictly to international standards (ISO/IEC 27001, NIST 800-53) can address these issues. Comprehensive protection during migration thus requires robust security audits, continuous monitoring, multi-factor authentication, and advanced security methodologies such as UEBA and deception technologies.Compromise of account credentials is the most dangerous threat. One of the options for such compromise can be phishing attacks on system administrators and DevOps. It is also possible to use merged passwords, for example from the “Have I been Pwned” databases [12]. It is also possible to compromise an account through attacks on authentication protocols (for example, password selection through brute-force or attacks on OAuth tokens). Another reason may be the use of outdated AWS IAM tokens or Google Cloud API Keys that remained active after migration.

The problem may be the use of unsecured APIs. Namely, REST API requests without authentication are possible, there are no restrictions on the number of requests (DDoS via API), injection attacks (SQL Injection, Command Injection) via API requests.

Data temporarily stored in cloud storage during migration may be exposed or may have configuration issues.

DDoS attacks can also affect migrations. In particular, massive requests to the server performing migration via botnets are possible. UDP Amplification or SYN Flood attacks on cloud load balancers.

It is worth noting the existing risks of using artificial intelligence for cyberattacks. AI is already widely used for phishing, in particular for personalizing phishing emails. Traditional means of protection make it difficult to detect AI-based malicious code due to its dynamic and polymorphic nature. AI technologies also allow for exceptional efficiency in disguising DDoS attacks as regular traffic, which makes countering them an extremely difficult task [13].

Considering the analysis of the famous threats, one of the main problems is the lack of single and universal standards for multi-cloud environments. Each cloud provider develops its protocols, interfaces and management tools, which complicates integration between different platforms. This leads to increased costs for infrastructure support, and can also cause difficulties in ensuring the compatibility of various services and applications. The lack of standards also complicates process automation and reduces the efficiency of managing multi-cloud environments. It can also result in underestimating the complexity of the

migration process, which leads to budget and deadline overruns. The lack of a clear plan can cause data loss or reduced system performance [14].

Data migration between cloud environments is a complex and risky process that requires detailed and comprehensive planning. A successful migration process requires ensuring reliability, security, and continuity of operations, which in turn requires clear coordination between all stakeholders and the use of effective tools and methodologies to minimize risks.

The availability of national and international standards and regulations for multi-cloud environments is insufficient. The lack of uniform regulatory rules complicates the integration of different cloud platforms and increases compliance risks, especially in the context of data storage and processing in different jurisdictions.

Cybersecurity is critical at all stages of the data migration process. Proper access control, data encryption, and protection against potential threats are important aspects to ensure the confidentiality and integrity of information during its movement. Since the migration process may involve different technologies and providers, it is important to ensure continuous monitoring and rapid response to potential cyber threats.

1. *The Digital Crunch Time: 2022 State Of APIs and Applications | Google Cloud*. (n. d.). Google Cloud.https://cloud.google.com/resources/state-of-apis-and-applications-report

2. On Cloud Services, Law of Ukraine No. 2075-IX (2024) (Ukraine).https://zakon.rada.gov.ua/laws/show/2075-20#Text

3. On approval of Methodological recommendations for ensuring cyber security when using cloud computing technology and Methodological recommendations for assessing the compliance of cloud services with security (assurance) levels, Order of the Administration of the State Special Communications Service No. 505 (2024) (Ukraine).https://www.cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-14-09-2024-505-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-zabezpechennya-kiberzakhistu-pri-vikoristanni-tekhnologiyi-khmarnikh-obchislen-ta-metodichnikh-rekomendacii-shodo-ocinki-vidpovidnosti-khmarnikh-poslug-rivnyam-bezpeki-vpevnenosti

4. *ISO/IEC 27001:2022*. (n. d.). ISO.https://www.iso.org/standard/27001

5. *ISO/IEC 27017:2015*. (n. d.). ISO.https://www.iso.org/standard/43757.html

6. *ISO/IEC 27018:2019*. (n. d.). ISO.https://www.iso.org/standard/76559.html

7. *SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations | CSRC*. (n. d.). NIST Computer Security Resource Center | CSRC.https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

8. *SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing | CSRC*. (b. d.). NIST Computer Security Resource Center | CSRC.https://csrc.nist.gov/pubs/sp/800/144/final

9. *Data Center Risk Assessment. (n. d.). Uptime Institute.https://uptimeinstitute.com/professional-services/data-center-risk-assessment#:~:text=Uptime%20Institute's%20Data%20Center%20Risk,people%20and%20skill-sets%20involved.*

10. *Uptime Institute Resource Page - Uptime Institute. (b. d.). Digital Infrastructure Authority | Tier Certification & Training - Uptime Institute.https://uptimeinstitute.com/resources/asset/tier-standard-operational-sustainability*

11. *Amazon helped Ukraine transfer 10 petabytes of data to its cloud servers. (n. d.).https://minfin.com.ua/ua/2022/06/11/86966942/*

12. *Have I Been Pwned: Check if your email has been compromised in a data breach. (n. d.). Have I Been Pwned: Check if your email has been compromised in a data breach.https://haveibeenpwned.com/*

13. *AI-based cyberattacks: strategies and countermeasures | Wezom. (n. d.). IT-company of the full cycle of development of software products WEZOM - Kyiv, Ukraine.https://wezom.com.ua/ua/blog/ataki-na-osnovi-shtuchnogo-intelektu-novi-vikliki-dlya-kiberbezpeki*

14. *Fly to the clouds: the main migration mistakes. (n. d.). Mind.ua.https://mind.ua/openmind/20215250-poletiti-v-hmari-osnovni-pomilki-migraciyi*

Я.Ю. Дорогий, В.В. Цуркан, В.Ю. Колісніченко

ПОКРАЩЕНИЙ МЕТОД ВИЯВЛЕННЯ ТА ІДЕНТИФІКАЦІЇ ВУЗЛІВ БЛОКЧЕЙН–МЕРЕЖІ ROOTSTOCK

Анотація. У роботі запропоновано метод покращення виявлення та ідентифікації вузлів блокчейн–мережі Rootstock. Запропоновано адаптивний алгоритм обходу графа мережі на основі пріоритетної функції, що враховує ступінь вузла та часові характеристики його активності. Використано поведінкову модель ідентифікації вузлів на основі машинного навчання, що дозволяє зменшити кількість хибних класифікацій. Запропоновано підхід до розподіленої обробки даних із кластеризацією вузлів, що покращує масштабованість і швидкість аналізу мережі. Отримані результати сприяють ефективнішому та точнішому виявленню вузлів у реальному часі..

Вступ. Розвиток блокчейн–технологій [1] сприяє зростанню популярності децентралізованих платформ, серед яких Rootstock є однією з найперспективніших для розгортання смарт–контрактів на основі Bitcoin. Ефективне функціонування таких мереж значною мірою залежить від можливості виявлення та ідентифікації їхніх вузлів, що є важливим для забезпечення безпеки, стійкості та оптимальної роботи мережі.

У статті [2] запропоновано метод обходу блокчейн–мережі Rootstock шляхом послідовного опитування вузлів із використанням алгоритму пошуку на графі. Проте такий підхід має певні обмеження, зокрема значні часові витрати та потенційне дублювання запитів. Крім того, відсутність механізму поведінкової ідентифікації вузлів може призводити до некоректної класифікації та збільшення навантаження на мережу.

У даній роботі запропоновано вдосконалений метод виявлення та ідентифікації вузлів Rootstock, який включає адаптивний алгоритм обходу графа мережі з динамічним пріоритетом опитування вузлів, модель поведінкової ідентифікації на основі машинного навчання та підхід до розподіленої обробки даних. Запропоновані модифікації дозволяють підвищити швидкість аналізу мережі, зменшити хибні класифікації та покращити масштабованість процесу виявлення вузлів..

Метод виявлення та ідентифікації вузлів блокчейн–мережі Rootstock. Удосконалення процесу виявлення та ідентифікації вузлів блокчейн–мережі Rootstock вимагає розробки формальної математичної моделі, що враховує структуру мережі, динаміку її зміни та поведінкові характеристики вузлів.

У статті [2] запропоновано алгоритм обходу графа блокчейн–мережі Rootstock для збору інформації про активні вузли. Однак такий підхід має певні обмеження, зокрема повільний процес опитування та неможливість адаптивного вибору вузлів для подальшої взаємодії. Крім того, у статті не розглядається питання поведінкової ідентифікації вузлів, що є важливим для зменшення кількості хибнопозитивних результатів.

У цій роботі пропонується вдосконалений алгоритм, що складається з трьох основних компонентів:

– адаптивного обходу графа на основі пріоритетної функції вибору вузлів;

– поведінкової моделі ідентифікації вузлів із використанням методів машинного навчання;

– розподіленої обробки підграфів мережі для підвищення швидкості аналізу.

Адаптивний обхід графа мережі. Нехай блокчейн–мережа представлена у вигляді орієнтованого графа $G = (V, E)$,

де:

V – множина вузлів (peer–ів),

E – множина ребер (зв'язків між вузлами).

Для покращення процесу пошуку нових вузлів вводимо пріоритетну функцію вибору вузлів для опитування (1):

$$P(v_i) = \alpha \cdot \frac{d(v_i)}{D_{max}} + \beta \cdot \frac{1}{t(v_i)} \text{ (1)},$$

де

$P(v_i)$ – пріоритет опитування вузла v_i,

$d(v_i)$ – ступінь вузла (кількість з'єднань),

D_{max} максимальний ступінь серед усіх вузлів,

$t(v_i)$ – час останньої відповіді від вузла (менше значення – більший пріоритет),

α, β – вагові коефіцієнти, що визначають вплив характеристик вузла на вибір.

Алгоритм обходу мережі наступний:

1. Вибрати вузол v_i із найбільшим значенням $P(v_i)$.
2. Відправити до нього запит про сусідні вузли.
3. Додати нові вузли до черги аналізу, оновлюючи їхні пріоритети P(v).
4. Повторювати кроки 1–3 до досягнення заданого критерію завершення.

Поведінкова модель ідентифікації вузлів. Для зменшення кількості хибних ідентифікацій запропоновано поведінкову модель оцінки вузлів. Кожен вузол характеризується множиною поведінкових ознак (2):

$$S(v) = \sum_{i=1}^{n} w_i \cdot f_i(v), \text{ (2)}$$

де:

$S(v)$ – підсумковий скоринговий бал для вузла v,

$f_i(v)$ – значення i–ї поведінкової характеристики (наприклад, середній час відповіді, частота запитів, стабільність зв'язку),

w_i – вагові коефіцієнти, що визначають важливість кожної характеристики.

Для класифікації вузлів використовуємо логістичну регресію (3):

$$P(\text{trusted}|v) = \frac{1}{1+e^{-S(v)}}, \text{ (3)}$$

де

$P(\text{trusted}|v) > T$ (поріг довіри) означає, що вузол вважається справжнім.

Розподілена обробка підграфів. Для підвищення швидкості аналізу мережі використовується розподілена обробка підграфів G_k (4):

$$G = \bigcup_{k=1}^{m} G_k, \quad V_i \cap V_j = \emptyset, \quad E_i \cap E_j = \emptyset, \quad i \neq j, \text{ (4)}$$

де

m – кількість потоків обробки.

Кожен підграф формується за допомогою кластеризації вузлів за критерієм відстані (5):

$$\mathrm{C}_k = \{v \in V | dist(v, v_0) \leq R_k\}, \text{ (5)}$$

де

v_0 – стартовий вузол,

R_k – радіус кластеризації.

Висновки. Запропонований метод покращення виявлення та ідентифікації вузлів блокчейн-мережі Rootstock забезпечує ефективніший обхід графа за рахунок адаптивного алгоритму вибору вузлів, підвищує точність ідентифікації шляхом аналізу поведінкових характеристик та скорочує час обробки мережі завдяки розподіленій обробці підграфів. Використання математичної моделі з логістичною регресією дозволяє зменшити кількість хибнопозитивних результатів, а застосування паралельного аналізу підвищує масштабованість рішення. Отримані результати сприятимуть підвищенню безпеки та надійності Rootstock, а подальші дослідження можуть бути спрямовані на впровадження методів машинного навчання та адаптацію підходу до інших блокчейн-мереж.

1. Dorohyi I., Kolisnichenko V. Y. Blockchain Transaction Analysis: A Comprehensive Review of Methods and Applications / I. Dorohyi, V. Y. Kolisnichenko // System research and information technologies. – 2023. – T. 4. – P. 37–53. DOI: 10.20535/SRIT.2308-8893.2023.4.03.

2. Dorohyi I., Kolisnichenko V. Y. Development of a method for nodes exploration and identification of Rootstock blockchain network / I. Dorohyi, V. Y. Kolisnichenko // Eastern-European Journal of Enterprise Technologies. – 2024. – No. 1/2 (127). – P. 6–15. DOI: 10.15587/1729-4061.2024.297903.

Я.Ю. Дорогий, В.В. Цуркан, В.С. Кравчук

ТЕНЗОРНА МОДЕЛЬ ОЦІНКИ РЕЗУЛЬТАТИВНОСТІ ПЕНТЕСТУ НА РІЗНИХ ЕТАПАХ РОЗГОРТАННЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація. У статті пропонується тензорна модель для оцінки результативності пентесту на різних етапах розгортання критичної інфраструктури. Модель дозволяє оцінити ефективність захисту системи в процесі тестування, налаштування та після розгортання в продуктивному середовищі, що допомагає виявити потенційні слабкі місця на кожному з етапів. Оцінка проводиться за допомогою трьох основних показників: результативності тестів, адаптивності засобів захисту та ефективності захисту. Використання такої моделі дозволяє точніше і комплексно аналізувати стан захисту на різних етапах розгортання інфраструктури.

Вступ. Актуальність використання тензорного аналізу для дослідження критичних інфраструктур обумовлена зростанням складності та взаємозалежності сучасних технологічних систем. Критична інфраструктура, яка охоплює енергетичні мережі, телекомунікації, фінансові та транспортні системи, стає все більш уразливою до кібератак і технічних збоїв. У зв'язку з цим виникає необхідність у нових підходах для комплексного аналізу безпеки таких систем, які дозволяють ефективно оцінити та забезпечити їх надійність і стійкість до загроз. Тензорний аналіз пропонує потужний інструмент для моделювання та аналізу складних взаємозв'язків між елементами критичної інфраструктури, що дозволяє більш точно передбачати можливі вразливості та загрози, що обговорюється в роботі [1].

Застосування тензорного аналізу в контексті пентестінгу критичних інфраструктур дозволяє детально вивчити та візуалізувати залежності між різними компонентами системи, такими як апаратне забезпечення, програмне забезпечення, мережеві ресурси та фізична безпека. Це відкриває нові можливості для виявлення потенційних слабких місць на ранніх етапах розгортання та експлуатації інфраструктури. Тензорні моделі дозволяють обчислювати результативність засобів захисту, їх адаптивність до змін середовища та ефективність у реальному часі, що є критично важливим для оцінки ризиків і мінімізації загроз у складних системах. Такий підхід розглядається у статті [2], де визначаються основні параметри та характеристики тензорного аналізу для пентестів.

Модель, запропонована в цій статті, спрямована на розширення можливостей тензорного аналізу для оцінки результативності пентесту на різних етапах розгортання критичної інфраструктури. Оцінка результативності пентесту проводиться з урахуванням ключових аспектів тестування на різних етапах, що дозволяє більш ефективно виявляти уразливості, оцінювати їх вплив на загальну безпеку та підвищувати стійкість інфраструктур до зовнішніх і внутрішніх загроз. Подібні сценарії

дослідження та оцінки результативності пентесту розглядаються в роботі [3], де детально аналізуються різні стратегії застосування тензорних моделей для оцінки ефективності захисту критичної інфраструктури.

Модель оцінки результативності пентесту на різних етапах розгортання критичної інфраструктури. Оцінка результативності пентесту на різних етапах розгортання критичної інфраструктури є важливою для визначення слабких місць в системі безпеки та забезпечення надійності інфраструктури. Математична модель оцінки результативності пентесту на різних етапах розгортання критичної інфраструктури може враховувати такі фактори, як кількість виявлених уразливостей, час на їх усунення, рівень їх критичності, а також вартість потенційного збитку від кожної вразливості.

Нехай визначено наступні тензори:

1. Тензор результативності тестів S: $S_{i,j,k,l}$ вказує на результативність тестів на кожному етапі розгортання інфраструктури, наприклад, на етапі тестування, налаштування або після розгортання в продуктивному середовищі. Даний тензор може відображати рівень виявлених уразливостей або кількість вдало проведених тестів. Нехай $S_{i,j,k,l}$ визначає результативність тестів на етапі i для компонента j з уразливістю k на етапі l.

2. Тензор адаптивності засобів захисту A: $A_{i,j,k,l}$ відображає адаптивність засобів захисту на різних етапах розгортання. Тензор визначає, наскільки ефективно система може реагувати на нові або змінювані уразливості на кожному з етапів. Нехай $A_{i,j,k,l}$ визначає адаптивність засобів захисту на етапі i для компонента j з уразливістю k на етапі l.

3. Тензор ефективності захисту R: $R_{i,j,k,l}$ оцінює ефективність захисту на кожному етапі та для кожної уразливості. Він також допомагає виявити найбільш вразливі етапи в процесі пентесту, тобто ті етапи, де захист є найбільш слабким. Нехай тоді $R_{i,j,k,l}$ відображає ефективність захисту на етапі i для компонента j з уразливістю k на етапі l.

Індекси тензорів визначають наступне:

- i – етапи розгортання інфраструктури, наприклад:
  - $i = 1$ – тестування,
  - $i = 2$ – налаштування,
  - $i = 3$ – продуктивне середовище.
- j – компоненти критичної інфраструктури, такі як сервери, мережі, бази даних, операційні системи тощо.
- k – типи уразливостей для кожного компонента.
- l – етапи пентесту, наприклад:
  - $l = 1$ – попереднє тестування,
  - $l = 2$ – тестування в умовах атаки,
  - $l = 3$ – тестування після атаки.

Опишемо математичну модель на базі введених позначень.

Для кожного етапу i, результативність тестів для компонентів критичної інфраструктури можна виразити наступним чином (1):

$$S_i = \frac{\sum_{j=1}^{M}\sum_{k=1}^{L}\sum_{l=1}^{L} S_{i,j,k,l}}{M \cdot L}, \quad (1)$$

де:

$S_{i,j,k,l}$ – результативність тестів для компонента j на етапі i для уразливості k на етапі l,

M – кількість компонент критичної інфраструктури,

L – кількість видів уразливостей.

Адаптивність засобів захисту на етапі i для кожного компонента j з уразливістю k можна оцінити так (2):

$$A_i = \frac{\sum_{j=1}^{M}\sum_{k=1}^{L}\sum_{l=1}^{L} A_{i,j,k,l}}{M \cdot L}, \quad (2)$$

де $A_{i,j,k,l}$ – адаптивність засобів захисту для компонента j на етапі i.

Ефективність захисту на кожному етапі i можна оцінити наступним чином (3):

$$R_i = \sum_{j=1}^{M}\sum_{k=1}^{L}\sum_{l=1}^{L} R_{i,j,k,l}, \quad (3)$$

де $R_{i,j,k,l}$ – ефективність захисту для компонента j на етапі i.

Загальна результативність пентесту по всіх етапах розгортання критичної інфраструктури можна отримати як середнє значення результативності для кожного етапу (4):

$$E_{\text{total}} = \frac{1}{N}\sum_{i=1}^{N} S_i\,, \quad (4)$$

де N – кількість етапів розгортання.

Потенційний збиток від усіх уразливостей розгорнутої критичної інфраструктури можна оцінити через (5):

$$C_{\text{damage}} = \sum_{i=1}^{N}\sum_{j=1}^{M}\sum_{k=1}^{L}\sum_{l=1}^{L} R_{i,j,k,l} \cdot D_{i,j,k,l}, \quad (5)$$

де

$D_{i,j,k,l}$ – потенційний збиток від експлуатації уразливості для компонента j на етапі i.

Представлена тензорна модель дозволяє зберігати та обробляти складні взаємозв'язки між різними етапами розгортання критичними інфраструктури, уразливостями та засобами захисту. Врахування таких факторів, як адаптивність засобів захисту та результативність тестів на різних етапах, дозволяє більш точно оцінювати вразливості на кожному етапі розвитку критичної інфраструктури та запобігати потенційним загрозам. Такий підхід дозволяє вчасно виявити слабкі місця і підвищити рівень захисту на кожному з етапів розгортання інфраструктури.

Висновки. У результаті проведеного дослідження тензорного аналізу для оцінки результативності пентесту на різних етапах розгортання критичної інфраструктури отримані важливі результати, які можуть значно підвищити ефективність забезпечення безпеки таких систем. Використання тензорних моделей дозволяє враховувати складні взаємозв'язки між різними компонентами інфраструктури, що дає змогу точніше оцінити ефективність засобів захисту на кожному етапі розгортання, починаючи від тестування і налаштування до експлуатації в продуктивному середовищі.

Розроблена модель, яка оцінює результативність пентесту на основі тензорних структур, дозволяє виявляти потенційні уразливості та загрози на різних етапах розвитку системи. Це дає можливість не лише своєчасно коригувати стратегії захисту, а й значно зменшити ймовірність виникнення критичних помилок, які можуть призвести до серйозних збоїв у роботі інфраструктури. Завдяки адаптивним тензорним моделям забезпечується висока ефективність аналізу і надійність системи захисту на всіх етапах її життєвого циклу.

Перспективи подальших досліджень в даному напрямку пов'язані з удосконаленням тензорних моделей для більш детальної оцінки впливу кожного етапу розгортання на загальну безпеку критичної інфраструктури. Крім того, важливим напрямком є інтеграція таких моделей з іншими методами та технологіями, зокрема з машинним навчанням і штучним інтелектом, для забезпечення більш точного прогнозування і своєчасної реакції на нові загрози та вразливості..

1. Дорогий Я.Ю., Цуркан В.В., Кравчук В.С. Тензорна модель представлення критичної інфраструктури / Я.Ю. Дорогий, В.В. Цуркан, В.С. Кравчук // Інформаційні технології та безпека. Матеріали XXIV Міжнародної науково-практичної конференції ІТБ-2024. – Київ: Інжиніринг. – с. 97-100. – doi: 10.5281/zenodo.14592839.

2. Дорогий Я.Ю., Кравчук В.С. Використання тензорного аналізу для задач пентестінгу / Я.Ю. Дорогий, В.С. Кравчук // Сучасний стан та перспективи розвитку науки, освіти і технологій: збірник тез доповідей міжнародної науково-практичної конференції (Кременчук, 4 січня 2025 р.): у 2 ч. – Кременчук: ЦФЕНД, 2025. – Ч. 2. – с. 62-63. – doi: 10.5281/zenodo.14698727.

3. Дорогий Я.Ю., Кравчук В.С. Сценарії дослідження пентесту на базі тензорних моделей / Я.Ю. Дорогий, В.С. Кравчук // Традиційні та інноваційні підходи до наукових досліджень: збірник наукових праць з матеріалами VIII Міжнародної наукової конференції, м. Дрогобич, 31 січня, 2025 р. / Міжнародний центр наукових досліджень. – Вінниця: ТОВ «УКРЛОГОС Груп, 2025. – с. 304-307. – doi: 10.5281/zenodo.14777058.

М.С. Дунаєвський

ІНФОРМАЦІЙНІ МОДЕЛІ ТОРГІВЛІ НА ВНУТРІШНЬОДОБОВИХ РИНКАХ ЕЛЕКТРОЕНЕРГІЇ

Вступ. Тренд збільшення частки відновлювальних джерел енергії означає більш децентралізовану та більш гнучку систему в якій крім традиційних джерел енергії використовуються сотні тисяч сонячних панелей, вітрових турбін та загалом малих електростанцій (а також енергоакумулюючих потужностей). Енергетична система повинна бути досить інтелектуальною, динамічною та інтерактивною для підтримки таких змін. Виникає запит на розроблення та впровадження сучасних інформаційних моделей торгівлі на ринку електроенергії, які б природньо інтегрувалися та підсилювали енергетичний сектор на системному рівні інформаційно-цифрової інфраструктури та на системному рівні операційної методології та управління [1, 2].

Мета та завдання. Мета цієї роботи – дослідити особливості та практики організації внутрішньодобового ринку (ВДР) електроенергії. Розглянути інформаційні моделі торгівлі на ВДР, цифрову інфраструктуру ринку. Об'єктом цього дослідження є енергоринок зі значною часткою відновлювальних джерел електроенергії (ВДЕ) та внутрішньодобовий ринок (ВДР) зокрема. Предмет вивчення – механізм внутрішньодобової торгівлі електроенергією, ціноутворення, балансування обсягів попиту та пропозиції, аналіз різних торгових стратегій учасників.

Виклад основного матеріалу. Закон України (ЗУ) «Про ринок електричної енергії» визначає наступні сегменти енергоринку: роздрібний ринок (постачальники електроенергії та електростанції потужністю до 20 МВт), ринок двосторонніх договорів (РДД), ринок «на добу наперед» (РДН), внутрішньодобовий ринок (ВДР), балансуючий ринок (БР), ринок допоміжних послуг [3]. Основні засади функціонування РДН та ВДР визначені статтею 67 цього закону. Так, для участі на ВДР учасники укладають з оператором ринку (ОР) типовий договір за встановленою формою, що є невід'ємною частиною правил ВДР. Учасники укладають такий договір в електронній формі шляхом внесення своїх реквізитів в шаблон, використовуючи інтерфейс програмного забезпечення наданого ОР, та підписують електронним підписом. В таких договорах узгоджуються загальні умови розрахунку та торгів [4]. Такі істотні умови як ціна та обсяг електроенергії узгоджуються автоматично під час торгів на РДН/ВДР. Закон визначає оператора ринку (ОР) як юридичну особу, яка забезпечує функціонування ВДР та організацію купівлі-продажу електричної енергії на цьому ринку, а також має право організовувати та проводити електронні аукціони з купівлі-продажу електричної енергії за двосторонніми договорами на підставі відповідних ліцензій, що видаються Національною комісією з цінних паперів та фондового ринку (НКЦПФР). Для продажу та купівлі

електроенергії учасники ВДР подають ОР свої заявки (пропозиції). До торгів допускаються лише ті учасники, які надали гарантії виконання фінансових зобов'язань. Ціна купівлі-продажу електроенергії на ВДР визначається за принципом ціноутворення «по заявленій (пропонованій) ціні» згідно з правил ВДР. Ціни ВДР (як і ціни на РДН) визначені законом як вільні (ринкові) ціни [2]. Варто зауважити, що порівняно з роздрібним ринком електроенергії, оплата електроенергії на ВДР здійснюється, виходячи з договірних обсягів, а не з фактичних обсягів відпуску та споживання. ОР за формою та у порядку визначеними правилами ВДР, для кожного розрахункового періоду, інформує про договірні обсяги купівлі-продажу електроенергії учасниками ринку.

Відповідно до «Правил ринку «на добу наперед» та внутрішньодобового ринку» подання заявок і торги на ВДР розпочинаються з 15:00 доби, що передує добі постачання та закінчуються за 60 хвилин до початку кожної години постачання [5]. Торгівля електроенергією на РДН/ВДР відбувається на електронних торгах з використанням централізованої комп'ютерної мережі [4]. Заявки подаються в електронній формі і підписуються електронним підписом. Подані заявки перевіряються на предмет достатності коштів для придбання електроенергії, заявленої для купівлі. Також вони перевіряються на відповідність обсягу електроенергії, заявленого для продажу, максимальному обсягу, розрахованому для учасника оператором системи передачі (ОСП). На основі допущених заявок комп'ютерні програми забезпечують автономне узгодження істотних умов договорів купівлі-продажу електроенергії на РДН/ВДР (ціни, обсягу електроенергії). На ВДР запрограмований алгоритм зіставляє заявки, що подаються на ВДР. Якщо серед раніше поданих заявок існують зустрічні заявки з ціною, що відповідає ціні поданої заявки та достатнім обсягом електроенергії, то вони акцептуються за найбільш вигідними цінами. Якщо обсягу електроенергії за раніше поданими заявками недостатньо, то, залежно від умов виконання поданої заявки, вона або відхиляється; або акцептується частково, а в іншій частині відразу відхиляється; або акцептується частково, а в іншій частині залишається на ринку [4]. Учасники ВДР відкривають ескроу рахунки в уповноваженому банку, який щоденно виконує розрахунки за придбану електроенергію згідно з укладеними договорами. Платіжні документи, на основі яких банк здійснює переказ коштів, надає ОР за результатами торгів [4].

Основні характеристики найбільш відомих проєктів платформ локальних енергетичних ринків (ЛЕР) з внутрішньодобовою торгівлею представлено в таблиці 1 [6]. Зауважимо, що основним сервісом, на який орієнтовані більшість платформ є сервіс управління перевантаженнями. Наприклад, німецька платформа Enera, спрямованою на досягнення гнучкості між постачанням та попитом для вирішення проблем перевантаження, з якими стикаються оператори системи розподілу (ОСР). Іншим прикладом є нідерландська GOPACS (Grid Operators Platform for Congestion Solutions), яка пропонує управління перевантаженнями та забезпечує гнучку координацію

між оператором системи передачі (ОСП) та ОСР. Також зазначимо мету забезпечення децентралізованої гнучкості (маневреності) платформи InteGrid, мету забезпечення гнучкості автоматичної торгівлі платформи GOFLEX.

Розрізняють односторонній та двосторонній ринкові механізми. Наприклад, GOPACS є двосторонньою платформою, де ОСР та ОСП виступають покупцями гнучкості (маневреності), а домогосподарства, промислові підприємства та енергетичні компанії — її продавцями.

Використовується ціновий механізм «за ціною заявки» (Pay-as-bid) та «за ринковою ціною» (Pay-as-clear).

Таблиця 1 – Проєкти платформ ЛЕР з внутрішньодобовою торгівлею

Платформа	**Країна**	**Роки функціонування**	**Сервіси**	**Ринковий механізм**	**Ціновий механізм**
Enera	Німеччина	2018 – 2020	Управління перевантаженнями	Двосторонній ринок	За ціною заявки
GOPACS	Нідерланди	З 2019 – до сьогодні	Управління перевантаженнями	Двосторонній ринок	За ціною заявки
Nodes	Норвегія, Німеччина	2018 – до сьогодні	Управління перевантаженнями	Двосторонній ринок	За ціною заявки
CoordiNet	Греція, Іспанія, Швеція	2019 – 2023	Управління перевантаженнями	Односторонній ринок	За ціною заявки та за єдиною ринковою ціною
InteGrid	Португалія, Словенія, Швеція	2017 – 2020	Децентралізована гнучкість	Децентралізовані ринки одного покупця	За ціною заявки
GOFLEX	Швейцарія, Німеччина, Кіпр	2017 – 2020	Гнучкість автоматичної торгівлі	Ринок одного покупця	За ринковою ціною
IREMEL	Іспанія	2019 – до сьогодні	Управління перевантаженнями	Двосторонній ринок	За ціною заявки чи за єдиною ринковою ціною

Серед сучасних інформаційних моделей торгівлі на ВДР електроенергії особливої уваги заслуговує модель на основі агентів (agent-based model) представлена A. Alberizzi, P. Barba та F. Ziel [7]. Ця агентоорієнтована модель здатна відтворювати безперервну еволюцію ринку, розрізняти диспетчеризовані та недиспетчеризовані типи електростанцій, аналізувати поведінку учасників ВДР та взаємодію між ними. Результати показують що модель здатна відтворювати основні характеристики безперервного внутрішньодобового ринку електроенергії, такі як цінова динаміка, що

сильно залежить від внутрішньої та зовнішньої інформації, зростання кількості заявок ближче до завершення торгової сесії та слабко-ефективний ринок (weak market efficiency). Кожному агенту можна призначити стратегію на основі результатів статистичного аналізу його історичних заявок. Враховується факт різних рівнів граничних витрат різних електростанцій. Гнучкість моделі дозволяє досліджувати широке коло сценаріїв.

Перспективними технологіями проведення взаєморозрахунків на ВДР електроенергії може бути децентралізована технологія блокчейн (blockchain) та смарт (smart) контракти, однак їх впровадження буде можливим тільки після відповідних змін в законодавстві, оскільки на разі купівля-продаж електроенергії на ВДР здійснюється централізовано через ОР [4]. Перевагами цих технологій є вищий рівень довіри між учасниками та вища прозорість транзакцій ринку, вирішення проблеми подвійного використання активів, відсутність потреби в посередниках та третіх особах, високий рівень захищеності, автоматичне виконання контрактів за виконання умов.

Висновки. Варто продовжувати дослідження та використати найкращі практики організації ВДР на вітчизняному ринку. Сучасною інформаційною моделлю ВДР електроенергії є модель на основі агентів. Перспективною технологією проведення взаєморозрахунків може стати, за відповідних законодавчих змін, децентралізована технологія блокчейн (blockchain).

1. Дунаєвський М.С., Сулейманов С.-Б. (2024). Архітектура цифрової трансформації енергетичного сектору України. Збірник тез VI науково-практичної конференції «*Безпека енергетики в епоху цифрової трансформації*». (с. 75–78). Інститут проблем моделювання в енергетиці імені Г.Є. Пухова НАН України. https://ipme.kiev.ua/konferencii/naukovo-praktichna-konferenciya-bevect-2024/

2. Горбачук В.М., Дунаєвський М.С., Сирку А.А. (2020) Сучасні питання генерування та накопичення енергії в енергосистемі України. *Східна Європа: економіка, бізнес та управління*. В. 1 (24). С. 260–268. http://www.easterneurope-ebm.in.ua/journal/24_2020/40.pdf

3. Закон України «Про ринок електричної енергії» № 2019-VIII (2017, 13 квітня). https://zakon.rada.gov.ua/laws/show/2019-19#Text (дата звернення 21.03.2025)

4. Кулинич В., Циба С. (2020) Біла книга 2020: Смарт-контракти для нового ринку електроенергії. Asters.

5. Постанова НКРЕКП № 308 «Про затвердження правил ринку «на добу наперед» та внутрішньодобового ринку» (2018, 14 березня). https://zakon.rada.gov.ua/laws/show/v0308874-18#Text (дата звернення: 21.03.2025).

6. Khaskheli S., Anvari-Moghaddam A. (2024) Energy trading in Local Energy Markets: A Comprehensive Review of Models, Solution Strategies, and Machine Learning Approaches. *Applied sciences*. 14(11510). https://doi.org/10.3390/

7. Alberizzi A, Di Barba P., Ziel F. (2025) Agent based modeling for intraday electricity markets. OPSEARCH. V. 62. pp. 178–197. https://doi.org/10.1007/s12597-024-00805-w

Н.В. Заїка, О.С. Верховець, М.Ю. Комаров, О.М. Дроботун

МЕТОДИ ОБФУСКАЦІЙНОГО ЗАХИСТУ ПЗ ДЛЯ КІБЕРБЕЗПЕКИ ОКІ

Розробка та процес створення обфускатора для захисту програмного забезпечення критичної інфраструктури, включає аналіз загроз, розробку методів заплутування коду, тестування та інтеграцію в цикл розробки для підвищення безпеки. Алгоритми обфускації включають зміну структури коду (вставка псевдологіки, застосування таблиць викликів), модифікацію змінних (перейменування, ускладнення їхньої структури), шифрування текстових даних, переміщення блоків коду та впровадження механізмів захисту від налагодження. Такі методи допомагають зберегти працездатність програмного забезпечення, ускладнюючи його зворотний аналіз і декомпіляцію [1]. На початку роботи розробникам програмного забезпечення необхідно створити псевдокод та описати основні процедури, що використовуються. Під поняття псевдокод розуміється компактний (найчастіше неформальний) опис методу, з використанням ключових слів імперативної мови програмування, але в якому опускаються несуттєві подробиці і специфічний синтаксис.

Тестування та перевірка працездатності обфускованого коду та оптимізація продуктивності потребує включення обфускації в процес розробки ПЗ для ОКІ в тестовому середовищі, для відстеження ефективності налаштувань механізмів перевірки на віртуальні середовища та дебагери, та для проведення контролю цілісності через хешування та цифрові підписи для виявлення змін у коді, при рандомізації виконання коду або динамічному завантаженні частин програми [2].

Методи заплутування коду в кібербезпеці для захисту працівників і критично важливих об’єктів:

1. Захист від зловмисного аналізу програмного забезпечення для унеможливлення або ускладнення пошуку вразливостей зловмисниками потребує застосування умовних операторів і циклів, які не змінюють функціональність, але ускладнюють аналіз. Проведення періодичної перевірки прав доступу користувачів та налаштувань з обмеження доступу. Заміна назв змінних на випадкові нелогічні імена із додаванням коментарів до коду, що створюють видимість хаосу у вихідному коді. Застосування анти-реверсних інструментів для захисту від зворотного інженерування, такі як пакувальники та шифрування виконуваних файлів [3].

2. Методи захисту IoT-пристроїв на об'єктах критичної інфраструктури від зломів і зворотного інженерування включають обфускацію коду прошивки, шифрування критичних даних та конфігураційних файлів, а також маскування коментарів та зміна структури коду в прошивці для протидії автоматизованому аналізу ключових логічних компонентів для ускладнення аналізу зловмисниками. Наприклад, датчики у водопостачанні або

енергетичних мережах, часто є вразливими через недостатній захист. Для захисту від дій зловмисників, які можуть зламати їхню прошивку або вивчити її, рекомендовано виконати перетворення структури коду шляхом включення недокументованих функцій та шифрування ключових логічних компонентів, через шифрування ділянок коду, що обробляють критичні дані. Фільтрація мережевого трафіку для виявлення атак типу "відмова в обслуговуванні". Внесення додаткових змін у структуру, таких як вкладеність чи зайві пробіли ускладніють декомпіляцію програм захисту [4].

3. Захист мобільних додатків для співробітників ОКІ. Мобільні додатки, які використовують співробітники об'єктів критичної інфраструктури, можуть бути ціллю атак для отримання даних про логістику, паролі або доступ до внутрішніх систем. Обфускація алгоритму обробки токенів доступу для приховування механізмів їх перевірки дій користувачів посилює механізми багатофакторної автентифікації (MFA) додатків через додаткові логічні умови [5]. Виявлення емуляторів та рутованих пристроїв для запобігання атакам через скомпрометовані пристрої.

4. Захист SCADA-систем, що забезпечують управління критичними процесами (енергетика, водопостачання, транспорт), часто є пріоритетними цілями для кіберзлочинців. Заплутування команд управління шляхом заміни стандартних команд їх ускладненими аналогами. Ускладнення коду для протидії зворотному інженеруванню. Зміна структури системних скриптів для ускладнення їх аналізу [6].

5. Метод захисту з використанням графів. Для роботи із програмою користувачеві пропонується ввести ключ, а потім, після перевірки розробленим методом, у стандартному вікні виводиться повідомлення про те, чи вірний уведений користувачем ключ. При цьому проводиться обхід по фрагментах, що відповідають вершинам, якщо ключ невірний, то обхід «рушиться» і відбувається перехід на фрагмент із видачею повідомлення про помилку відразу (або не напряму через проміжні елементи, які можуть виглядати як «шум» або неструктуровані повідомлення про помилки, які важко інтерпретувати). Після кожної роботи підпрограми проводитися перевірка на правильність роботи програми. У випадку, якщо файли з псевдокодом працюють некоректно буде виводитися повідомлення про помилку. Після завершення роботи усіх підпрограм відбувається запис логів та даних у новий файл, для генерації ключа.

6. Методи захисту програмного забезпечення через використання динамічного коду (наприклад, асемблера x86) та графів, зокрема, для забезпечення захисту від зворотного інженерування (дизасемблювання) й анти-налаштування (анти-дебаг). Генерація динамічного коду відбувається на основі графів, зокрема за допомогою задачі про Гамільтоновий цикл (пошук шляху через всі вершини графа без повторів). Згенерований код включає перевірку ключа (наприклад, певну кількість біт, що перевіряються в кожній вершині). Захист базується на вирішенні складної задачі для отримання ключа (в даному випадку — розв'язок задачі Гамільтонового циклу), тобто

кількість переходів у захисті залежить від довжини ключа (k) та розміру фрагмента ключа (m). Формула для розрахунку кількості переходів (N) виглядає так:

$$N = f(k, m) \quad (1)$$

де:

k — довжина ключа (в бітах),

m — кількість біт, перевірених у кожній вершині графа.

Якщо збільшити розмір фрагмента ключа (m), зменшується кількість вершин у графі, але кількість переходів на кожній вершині збільшується, що дозволяє зберігати загальну складність захисту.

Другий рівень захисту включає в себе захист від дизасемблювання, що ускладнює процес аналізу і модифікації коду.

7. Методи протидії засобам сканування, що функціонують в режимі користувача включають в себе:

1) пасивні емулятори коду, що функціонують у користувацькому режимі, імітуючи виконання програм;

2) програми відлагоджувачі для відстеження коду, з якими можна боротися, виявляючи їх у процесі виконання;

3) засоби статичного сканування аналізує код без виконання, захистом є обфускація та шифрування;

4) програми одержання дампу пам'яті. Слід зазначити, що зніманню дампу пам'яті ефективно протидіє використання шифрування й псевдокоду, але способів протидії самому процесу знімання дампу на теперішній момент не існує.

Ці заходи в комплексі з використанням обфускаційних методів створюють надійний захист і підвищують стійкість ОКІ до кібератак. Підвищення обізнаності персоналу, компетенцій адміністраторів і зниження ризику атак на об'єкти критичної інфраструктури.

1. Dowd, M., McDonald, J., Schuh, J. The Art of Software Security Assessment. 2006. С. 46–48.

2. Журиленко, Б., Ніколаєва, Н. Визначення коефіцієнта ефективності технічного захисту інформації за її параметрами. Безпека інформації. 2015. Т. 21, № 3. С. 245–250.

3. Dang, B., Gazet, A., Bachaalany, E. Practical Reverse Engineering. 2014. 384 с.

4. Singer, P. W., Friedman, A. Cybersecurity and Cyberwar: What Everyone Needs to Know. 2014. 306 с.

5. Mitnick, K. The Art of Deception: Controlling the Human Element of Security. 2011. 368 с.

6. Іванченко, С. О., Гавриленко, О. В., Липський, О. А. [та ін.]. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації: навчальний посібник. Київ: НТУУ «КПІ». 2016. 104 с.

Є.О. Застьола, О.Б. Білоцерківський

РЕАЛІЗАЦІЯ БЛОКЧЕЙН-ПРОЕКТІВ У ЕНЕРГЕТИЧНОМУ СЕКТОРІ ТА СПЕКУЛЯЦІЇ НА КРИПТОВАЛЮТНИХ РИНКАХ ЯК ШЛЯХ ДО ФІНАНСОВОЇ НЕЗАЛЕЖНОСТІ ПІДПРИЄМЦЯ

Сучасні економічні та технологічні трансформації відкривають нові можливості для розвитку бізнесу та досягнення фінансової незалежності.

Однією з найбільш перспективних технологій, що стимулюють цей процес, є блокчейн. Зокрема, блокчейн має значний потенціал для зміни енергетичних ринків, створюючи нові можливості для підприємців. У той же час, криптовалютні ринки дають можливість отримати значний прибуток завдяки спекуляціям. Ця теза розглядає два аспекти: технічні особливості реалізації блокчейн-проектів у енергетиці та фінансові можливості для підприємців через криптовалютні ринки.

Блокчейн-технології мають великий потенціал для трансформації енергетичних ринків завдяки своїй здатності забезпечувати прозорість, безпеку та ефективність операцій. У енергетиці блокчейн може бути використаний для автоматизації процесів обліку, розподілу енергії та здійснення угод, що дозволяє зменшити витрати, підвищити ефективність і скоротити адміністративні витрати. Наприклад, за допомогою смарт-контрактів можна автоматизувати виконання угод між виробниками та споживачами енергії, зменшуючи ризики шахрайства та забезпечуючи своєчасність розрахунків.[1]

Одним із яскравих прикладів є використання блокчейн у системах «peer-to-peer» енергетичних ринків, де користувачі можуть безпосередньо обмінюватися енергією між собою. Це дозволяє оптимізувати розподіл енергетичних ресурсів, знижувати залежність від централізованих постачальників і створювати більш гнучкі механізми управління енергетичними потоками.

Зокрема, блокчейн може бути використаний для моніторингу відновлювальних джерел енергії, таких як сонячні або вітрові електростанції, де точність обліку та прозорість даних є важливими для ефективного управління. Ці технології також відкривають нові можливості для інтеграції різних джерел енергії в єдину мережу, що робить енергетичні системи більш стійкими та адаптивними до змін.

Незважаючи на те, що блокчейн в основному асоціюється з технологіями для забезпечення безпеки та прозорості, він також створює умови для розвитку криптовалют, які на сьогодні є одним з найбільш вигідних інструментів для підприємців у пошуках фінансової незалежності. Криптовалюти, такі як біткойн, ефіріум та інші, дозволяють здійснювати фінансові операції без необхідності використовувати традиційні банківські системи, що знижує витрати на транзакції і підвищує швидкість операцій.

Спекуляції на криптовалютних ринках стали популярним інструментом досягнення фінансової незалежності для багатьох підприємців. Вони можуть отримувати прибуток завдяки змінам курсів криптовалют, інвестуючи в них на ранніх етапах розвитку або активно торгуючи на криптовалютних біржах. Криптовалютні ринки мають високу ліквідність і доступність, що дозволяє швидко здійснювати угоди та реалізовувати прибуток навіть при невеликих коливаннях ринку.[2,3]

Однак варто зазначити, що спекуляції на криптовалютних ринках супроводжуються високими ризиками, зокрема через волатильність курсів криптовалют і можливі маніпуляції на ринку. Для зменшення ризиків підприємцям необхідно мати глибокі знання про ринок криптовалют, а також використовувати різноманітні стратегії хеджування та управління ризиками.

Блокчейн у енергетиці та криптовалютні ринки можуть взаємодіяти і створювати додаткові можливості для підприємців. Наприклад, підприємці, які займаються енергетичними проектами, можуть використовувати криптовалюти для фінансування своїх проектів або як інструмент для розрахунків з партнерами та постачальниками. Одним із прикладів є токенізація енергетичних активів або проектів, коли підприємства випускають криптовалютні токени, що представляють частину енергетичних ресурсів або прав на їх використання. Це дозволяє залучати інвестиції в енергетичні проекти через криптовалютні ринки.

Також блокчейн може забезпечити прозорість фінансових операцій у рамках енергетичних проектів, що підвищує довіру інвесторів і дозволяє створювати нові можливості для підприємців, що працюють в галузі. [4]

Як висновок, можно сказати, що інтеграція блокчейн-технологій в енергетичний сектор і використання криптовалютних ринків відкриває нові горизонти для підприємців, що прагнуть до фінансової незалежності. Блокчейн дозволяє створювати більш ефективні, прозорі та безпечні енергетичні ринки, що сприяє зниженню витрат і підвищенню ефективності. Водночас криптовалютні ринки дають можливість отримати значний прибуток через спекуляції, однак вони потребують ретельного управління ризиками. У цілому, комбінація цих двох технологій може стати потужним інструментом для досягнення фінансової автономії та розвитку інноваційних бізнес-проектів у різних сферах.

1. https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/41193/18800.pdf?sequence=3&isAllowed=y
2. https://academy.binance.com/uk-UA/articles/peer-to-peer-networks-explained
3. Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance. CRC Press.
4. Реалізація використання блокчейн-технологій у енергетичному секторі.URL: https://www.econ.vernadskyjournals.in.ua/journals/2019/30_69_4/30_69_4_2/28.pdf

Г.В. Неласа, О.В. Неласий, С.С. Самойлик

ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ СМАРТ-КОНТРАКТІВ В ДЕЦЕНТРАЛІЗОВАНИХ ЗАСТОСУНКАХ

Блокчейн в широкому сенсі – це технологія зберігання, погодження та синхронізації даних між учасниками, які не довіряють один одному. Часто помилково ототожнюють поняття блокчейну та криптовалюти. Насправді ж технологія блокчейн має більш узагальнене застосування. Насамперед це спосіб зберігання даних, який забезпечує їх цілісність шляхом застосування криптографічних геш-функцій.

«Похідні» технології блокчейн, зокрема крипто валюти та смарт контракти, є основою розподіленої децентралізованої захищеної технології обробки інформації, призначеної для розв'язання широкого кола прикладних задач: децентралізованого випуску та обігу електронної готівки (криптовалюти); аутентифікації та електронного нотаріату; розподіленого підписання контрактів; проведення електронних виборів; проведення електронних аукціонів; функціонування інтернет-магазинів; автоматичної оплати послуг в рамках контрактів, переведених в форму комп'ютерних програм і таке інше [1].

На технічному рівні криптографічно пов'язані блоки формуються із транзакцій. Транзакція - це цифрова заява про передачу прав власності, засвідчена електронним підписом. В мережі Ethereum акаунти користувачів асоційовані з публічним ключем — адресою, яку використовують для отримання або запиту монет у мережі. Приватний ключ надає доступ до гаманця. З точки зору інформатики Ethereum представляє собою детерміністичний, але по суті необмеженыы скінченний автомат Ethereum Virtual Machine (EVM), який має глобальний стан сінглтон та віртуальну машину, що вносить зміни в цей стан. З практичної точки зору Ethereum є відкритою глобально децентралізованою обчислювальною інфраструктурою, яка виконує специфічні програми - смарт-контракти. Технологія блокчейн тут використовується для синхронізації та зберігання змін станів системи, а внутрішня криптовалюта мережі ефір (Ether) для виміру та обмеження вартості обчислювальних ресурсів. Таким чином, платформа дозволяє розробникам створювати потужні децентралізовані застосування з вбудованими економічними функціями [2].

Здатність платформи Ethereum виконувати програми з пам'яті в скінченному автоматі EVM а також читати й писати дані у сховище робить її Тьюринг-повною (UTM-Universal Turing machine). Ethereum може виконати любий алгоритм, що підтримується машиною Тьюринга, якщо має достатньо пам'яті. В Ethereum існують два типи акаунтів користувачі (External owned account - EOA) і смарт-контракти. Зовнішні облікові записи (EOA) - це користувачі поза мережею. Вони мають пару ключів відкритий і закритий та можуть ініціювати виконання контрактів та підписувати транзакції. Смарт-

контракти це довільні on-chain програми, які мають тільки відкритий ключ, хеш якого дає адресу контракту і можуть викликати інші контракти та передавати їм дані, але не можуть запускатися самі. По суті, смарт-контракти це і є EVM – програмами, що пишуться на мовах програмування високого рівня (наприклад Solidity або Vyper (Scala)) і компілюються в байт-код для подальшого виконання в EVM [3].

Наступним етапом розвитку інтернет технологій має стати концепція «фінансового інтернету» на основі технології Web3, як концепції децентралізованого вебу, який буде повністю децентралізованим та повністю побудований на блокчейн-технології. У Web3 кожна одиниця контенту є цифровим активом, що повністю контролюється його власником.

Версія Web 3.0 працює на основі економіки токенів. Під токеном на блокчейні розуміють основану на блокчейні абстрактну одиницю, яка може належати користувачеві та представляти фізичні активи, валюту (засіб обміну) або права доступу. Головна перевага при реалізації DApp (decentralized application) за допомогою точену (наприклад ERC20) на відміну від прямих розрахунків в валюті Ether є варіант виконувати двокроковий переказ токенів функціями approve()+transferFrom() за дві транзакції з можливістю власнику токенів делегувати їх переказ з іншої адреси (передача повноважень контракту, який розподіляє токени) (рис.1.).

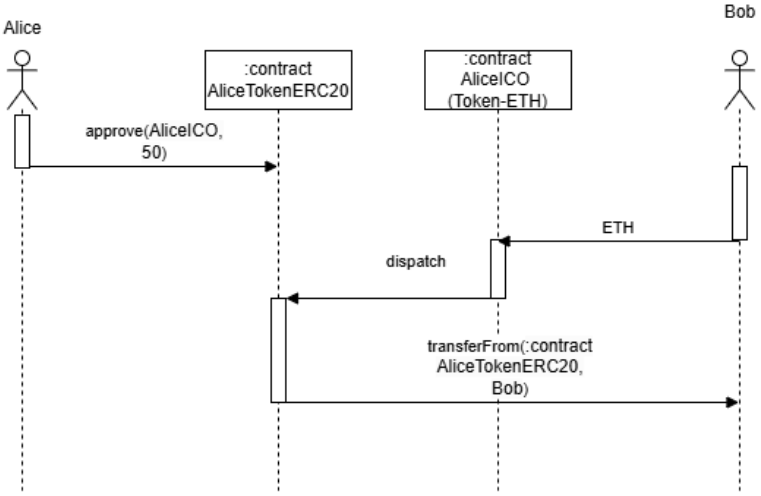

Рисунок 1 – Двокроковий переказ токенів ERC20

В блокчейні більшість токенів мають декілька призначень в глобальному масштабі та підлягають обміну між собою та на інші валюти на світових ринках ліквідності. Токени можуть бути взаємозамінними [4] та невзаємозамінними [5]. Також існують так звані мультитокени, які є частково взаємозаміннми [6]. Деякі токени є внутрішніми активами (intrinsic asserts) по

відношенню до конкретного блокчейну. Такі активи регулюються правилами консенсусу. На відміну від них токени, які використовуються для представлення зовнішніх сутностей (об'єктів нерухомості, корпоративних акцій, золотих злитків і т.і.) регулюються законами та нормами, відокремленими від правил консенсуса та можуть бути схильний до ризику контрагента, який полягає в тому що друга сторона транзакції може не виконати свої обов'язки.

Приклади використання токенів: цифрова валюта; ресурс; фізичний актив; право доступу до цифрової або фізичної власності; капітал (доля акціонера); право голосу в системі електронного голосування; предмет колекціонування; посвідчення особи; свідоцтво; платіж за послуги інформаційної системи [3].

Бібліотека OpenZeppelin включає набір написаних на мові програмування Solidity смарт контрактів, що забезпечують основні функції безпеки для створення, автоматизації та роботи децентралізованих програм [7].

В ході дослідження, авторами розроблені вріанти використання токену ERC20 в сфері зеленої енергетики та відповідні смарт-контракти на мові програмування Solidity [8] в якості макету для подальшого використання.

Дослідження здійснено в рамках проекту «Розвиток розподіленої енергетики в умовах ринку електричної енергії України з використанням технологій та систем цифровізації», що виконується за напрямом використання бюджетних коштів «підтримка пріоритетних для держави наукових досліджень і науково-технічних (експериментальних) розробок» бюджетної програми КПКВК 6541230 в НАН України.

1. P. Kravchenko, B. Skriabin, O. Kurbatov, Engineer's guide to financial internet. – Kharkiv: PROMART, 2019. – 224 p.

2. Kravchenko, Pavel Blockchain and Decentralized Systems : in Three Vol. : Authors' Edition / P. Kravchenko, B. Skriabin, O. Dubinina. - Kharkiv : PromArt, 2020, Vol. 2. - 395 p.

3. Andreas M. Antonopoulos, Dr. Gavin Wood, Mastering Ethereum: Building Smart Contracts and Dapps, 1st Edition, O'Reilly, 2018, 422 p.

4. Fabian Vogelsteller, Vitalik Buterin, ERC-20: Token Standard. 2015, https://eips.ethereum.org/EIPS/eip-20

5. William Entriken, Dieter Shirley, Jacob Evans, Nastassia Sachs, ERC-721: Non-Fungible Token Standard, 2018, https://eips.ethereum.org/EIPS/eip-721

6. Witek Radomski, Andrew, Philippe Castonguay, James Therien, Eric Binet, Ronan Sandford, ERC-1155: Multi Token Standard, 2018, https://eips.ethereum.org/EIPS/eip-1155

7. The standard for secure onchain applications at any scale, © 2025 Zeppelin Group Ltd, https://www.openzeppelin.com/

8. Solidity documetation, © Copyright 2016-2025, The Solidity Authors. https://docs.soliditylang.org/en/latest/

В.О. Побережник, В.С. Балацька

КОНЦЕПЦІЯ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН ДЛЯ ПІДТВЕРДЖЕННЯ ЦІЛІСНОСТІ ТА АВТЕНТИЧНОСТІ ДАНИХ

Блокчейн сьогодні знайшов своє застосування у багатьох сферах [1]. Основними характеристиками технології, які забезпечують її успіх є:

- Незмінність: жодна інформація, збережена у блокчейні, не може бути змінена.
- Децентралізованість: на відміну від традиційних систем, роботу мережі підтримується кожним вузлом мережі.
- Криптографія: публічні адреси користувачів генеруються за допомогою криптографічних методів, які не дозволяють визначити приватний ключ, а кожен блок даних в блокчейні криптографічно пов'язаний із наступним – геш попереднього блоку зберігається у наступному, що дозволяє зберігати блоки пов'язані між собою і виявляти будь-які зміни.

Ці характеристики дозволяють розглядати блокчейн як своєрідну базу даних, яка може забезпечувати цілісність та автентичність даних, пов'язуючи дані та їхнього творця публічним ключем, за замовчуванням. Тому, застосування технології блокчейн можна розглядати як основу для створення системи, яка можна виконувати завдання підтвердження цілісності даних, що є важливим для роботи різних ресурсів, зокрема для державних реєстрів, оскільки вони потребують інформацію, яка є достовірною, цілісною та автентичною, щоб унеможливити будь-які махінації із нею.

Однак, попри очевидні переваги технології, вона має свої недоліки [2]. Однак, одним із основних недоліків є проблема масштабованості мережі, оскільки розмір блокчейну негативно впливає на швидкодію мережі, збільшуючи час на обробку транзакцій в мережі. Окрім цього збільшуватиметься і сама вартість обслуговування мережі з ростом розміру даних, які циркулюють в мережі, яскравим прикладом цього процесу є блокчейн Bitcoin як для підтримки своєї роботи щорічно споживає 87 ТВт.год [3], що зумовлене використанням алгоритму PoW [4].

Якщо нівелювання недоліку споживання великої кількості енергії можна обійти вибором іншого алгоритму консенсусу, наприклад, PoS [5], то сама обробка інформації потребує вибору іншого підходу до обробки самої інформації. Вирішенням цієї проблеми є застосування підходу, який виносить обробку інформації за межі мережі блокчейн, але зберігає в мережі лише необхідні дані для підтвердження даних. Такий підхід відомий як Layer 2[6].

Спираючись на ідеї Layer 2 можна розробити концепцію застосування технології блокчейн для забезпечення цілісності та автентичності інформації.

Основний принцип роботи такої системи заснований на ідеї збереження відбитку даних у мережі блокчейн. Такий підхід дозволить зберігати дані

поза мережею блокчейн, що знизить навантаження на саму систему, а самі відбитки даних – у мережі блокчейн, що дозволить гарантувати достовірність відбитків, що дозволить користувачам системи підтвердити цілісність та достовірність даних. Відбиток даних можна отримати шляхом генерування геш значення даних, наприклад через застосування алгоритмів сімейства SHA-2, які одночасно визнанні безпечними і дозволяють гешувати об'єми інформації розміром до 2^{64} байтів. Також для забезпечення автентичності інформації, можна застосувати алгоритм HMAC, який одночасно дозволяє підтверджувати цілісність та автентичність інформації. Такий підхід дозволить зберігати саму інформацію у потенційно небезпечному середовищі, перевагою якого є те, що воно може значно ефективніше зберігати саму інформацію, однак не має тих переваг, які надає блокчейн, а в блокчейні зберігати лише відбитки даних, оскільки він дозволяє забезпечувати збереження незмінною, однак не може продемонструвати таку саму простоту у збереженні даних та масштабуванні, як традиційні системи. Тобто такий підхід дозволяє використати блокчейн одночасно із традиційними системами збереження даних, що дозволить одночасно задіяти їхні сильні сторони та нівелювати слабкі. Втім, варто зазначити, що при розробці такої системи слід зважати на ряд викликів, які можуть постати, зокрема те, що такий спосіб є ефективним, коли інформацію створює та підписує сторона із високим рівнем довіри, оскільки такий метод не дозволяє підтвердити правдивість інформації, оскільки він орієнтований на те, щоб підтвердити цілісність та автентичність, а не доброчесність користувачів системи.

1. 40 blockchain applications | real-world use cases in 2025 - webisoft blog. (б. д.). Webisoft. https://webisoft.com/articles/blockchain-applications/

2. GeeksforGeeks. (2022, 2 лютого). Advantages and disadvantages of blockchain - geeksforgeeks. https://www.geeksforgeeks.org/advantages-and-disadvantages-of-blockchain/

3. How much energy does bitcoin consume? | crypto.com. (б. д.). Crypto.com | Securely Buy, Sell & Trade Bitcoin, Ethereum and 400+ Altcoins. https://crypto.com/bitcoin/bitcoin-energy-consumption

4. Academy, B. (2018, 6 грудня). What is proof of work (pow)? | binance academy. Binance Academy. https://academy.binance.com/uk-UA/articles/proof-of-work-explained

5. Academy, B. (б. д.). Proof of stake (pos) | binance academy. Binance Academy. https://academy.binance.com/uk-UA/glossary/proof-of-stake

6. Gudgeon, L., Moreno-Sanchez, P., Roos, S., McCorry, P., & Gervais, A. (2020). SoK: Layer-two blockchain protocols. У Financial cryptography and data security (с. 201–226). Springer International Publishing. https://doi.org/10.1007/978-3-030-51280-4_12

А.О. Попова, О.М. Любименко, Н.О. Маслова, О.А. Штепа

БЕЗПЕКА СМАРТ-КОНТРАКТІВ: КОМПЛЕКСНИЙ ПІДХІД ДО ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ АТАКАМ

Блокчейн-технологія забезпечує безпечне, прозоре середовище для обміну інформацією та здійснення транзакцій без участі посередників. Створена спочатку для криптовалюти Bitcoin у 2008 році, блокчейн-технологія знайшла широке застосування в різних галузях [1].

Принцип децентралізації в блокчейні означає, що жодна сторона не має одноосібного контролю над даними, а система керується мережею вузлів, які підтверджують транзакції за допомогою алгоритмів консенсусу. Це робить блокчейн потужним інструментом для збереження цілісності даних та запобігання фальсифікації.

Смарт-контракти є ключовим компонентом сучасних блокчейн-систем, забезпечуючи можливість створення децентралізованих додатків та автоматизації складних бізнес-процесів. Це самовиконуючі цифрові протоколи, які автоматично виконують та контролюють юридично значущі дії відповідно до запрограмованих умов. Однак, попри всі переваги, смарт-контракти залишаються вразливими до різних типів атак, що може призвести до значних фінансових втрат та втрати довіри користувачів.

Серед найнебезпечніших атак на смарт-контракти варто виділити атаки повторного входу, які стали причиною відомого зламу DAO у 2016 році з втратою близько 60 мільйонів доларів. Атака відбувається, коли зовнішній контракт викликає функцію вразливого контракту, а потім, до завершення виконання цієї функції, знову викликає її. Це дозволяє зловмиснику багаторазово виконувати дії, які повинні бути обмежені одноразовим виконанням [2].

Аналіз показує, що для захисту від таких атак необхідно використовувати модифікатори "Check-Effects-Interactions", які забезпечують, що всі зміни стану контракту відбуваються до зовнішніх викликів, а також механізми блокування для запобігання повторним викликам функцій.

Не менш небезпечними є атаки переповнення цілих чисел, які використовують обмеження мов програмування щодо представлення чисел. Коли результат арифметичної операції перевищує максимально допустиме значення змінної, відбувається переповнення, що може призвести до непередбачуваної поведінки контракту. Наприклад, додавання одиниці до максимального значення uint може повернути нуль, що потенційно дозволяє зловмиснику отримати необмежену кількість токенів [2].

Для запобігання цим атакам рекомендується використовувати бібліотеки безпечної математики та строгий контроль введення даних.

Користуючись прозорістю блокчейну, зловмисники часто застосовують атаки фронт-раннінг. Атаки фронт-раннінгу створюють значну загрозу для децентралізованих бірж, p2p-аукціонів та систем голосування, оскільки

дозволяють зловмисникам використовувати інформацію про ще не підтверджені транзакції для отримання фінансової вигоди..

Згідно з моделлю, запропонованою в [4], ймовірність успіху атаки випередження залежить від розміру комісії, яку атакуючий готовий заплатити за пріоритетне виконання транзакції; навантаження на мережу та кількості конкурентних транзакцій у пулі очікування; затримки між створенням і підтвердженням транзакції.

Оракули, які забезпечують смарт-контракти даними з зовнішнього світу, також стають мішенню для атак. Підміна даних або компрометація джерел інформації призводить до виконання контрактів на основі неправильних даних, що особливо критично для фінансових контрактів, які залежать від точності цінової інформації. Для підвищення безпеки рекомендується використовувати децентралізовані оракули та криптографічні доведення достовірності даних.

Помилки в логіці управління доступом можуть дозволити неавторизованим користувачам викликати функції, призначені лише для власників або адміністраторів. Наприклад, недостатня перевірка дозволів може дозволити зловмиснику змінювати критичні параметри контракту або виводити кошти. Детальний аналіз та ретельне тестування систем контролю доступу є необхідними для запобігання таким атакам.

Для забезпечення безпеки смарт-контрактів фахівці рекомендують використовувати формальну верифікацію, яка застосовує математичні методи для доведення коректності контрактів відносно їх специфікації. Це дозволяє виявляти потенційні вразливості ще до розгортання контракту в мережі. Статичний аналіз коду за допомогою спеціалізованих інструментів також показує високу ефективність у виявленні типових вразливостей без фактичного виконання контракту.

Розглянемо застосування методів захисту на прикладі системи квадратичного голосування на блокчейні. У цій системі кожен голос має свою вартість, яка зростає квадратично зі збільшенням кількості голосів. Це дозволяє знизити вплив окремих виборців та забезпечити більш збалансоване прийняття рішень. У моделі квадратичного голосування застосовується математичний підхід, де кожен голос має свою вартість, яка зростає квадратично зі збільшенням кількості голосів [3].

У формулі сума внесків спонсорів для конкретного проекту визначається як сума квадратів кількості голосів, що виділяються кожним спонсором [3]:

$$s(p_m) = \sum_{i=1}^{n} c_i^2 , \quad (1)$$

де p_m – проект, висунутий на голосування;

m – загальна кількість проектів на голосуванні;

s – сума вкладу спонсорів за голоси;

n – загальна кількість спонсорів;

c_i – кількість голосів спонсора.

Загальний бюджет конкурсу (2) представлений як сума внесків усіх спонсорів для всіх проектів, що є на голосуванні.

$$b = \sum_{i=1}^{m} s(p_i)\,, \quad (2)$$

де b – бюджет конкурсу;

p_i – проект, висунутий на голосування;

s – сума вкладу спонсорів за голоси;

m – загальна кількість проектів на голосуванні.

Потенційні вразливості в такій системі включають атаки Сибіл (створення множини фіктивних акаунтів для обходу квадратичної вартості голосів), маніпуляції з часом (тактичне відкладання голосування для впливу на результати) та фронт-раннінг (перехоплення та модифікація транзакцій голосування). Для захисту від цих атак ефективними є впровадження системи ідентифікації для мінімізації ризику Сибіл-атак, впровадження механізмів моніторингу голосування та виявлення аномальних шаблонів у розподілі голосів, а також застосування приватних транзакцій для запобігання фронт-раннінгу через шифрування транзакцій до їх підтвердження.

Пропонуємо Методику аналізу вразливостей смарт-контрактів на основі комплексного підходу.

В основі аналізу лежить концепція багаторівневого захисту, що включає три етапи:

- Статичний аналіз коду (виявлення вразливостей до розгортання);
- Динамічний аналіз та моніторинг (виявлення атак у реальному часі);
- Формальна верифікація (математичний доказ коректності контракту);
- Моніторинг у реальному часі з використанням ШІ.

Особливості проведення етапів наведено в Таблиці 1.

Таблиця 1 - Етапи Методики

Етапи	Інструменти/вразливості	Принципи аналізу
Статичний аналіз коду	Slither, Mythril, Oyente Вразливості: атаки повторного входу; переповнення цілих чисел; помилки в логіці управління доступом	Аналіз патернів написання коду за принципом Checks-Effects-Interactions
Динамічний аналіз та моніторинг	Foundry, Echidna, Hardhat Вразливості: фронт-раннінг атаки	- емуляції роботи мережі; - аналіз поведінки оракулів при зміні зовнішніх даних
Формальна верифікація	логіка Хоара	Доведення, що: - переповнення чисел неможливе; - алгоритми управління доступом не мають логічних помилок; - зовнішні виклики не можуть спричинити повторний вхід
Моніторинг у реальному часі з ШІ	Аналіз історичних даних для розпізнавання патернів атак	використання машинного навчання для виявлення аномалій у транзакціях

Застосуванням пропонованої методики до квадратичного голосування є:

- впровадження механізму детекції Сибіл-атак через перевірку зв'язків між акаунтами;

- використання затримки між подачею голосу та його обробкою для мінімізації фронт-раннінгу;

- запровадження криптографічних доказів достовірності даних оракулів.

Звернемо увагу на останній пункт таблиці. Інтеграція методів штучного інтелекту в системи блокчейн надає нові можливості для моніторингу та аналізу транзакцій в режимі реального часу, значно підвищуючи безпеку смарт-контрактів. ШІ відіграє ключову роль у виявленні аномальних шаблонів у взаємодії з контрактами, що є особливо важливим для запобігання маніпуляціям та зловживанням у децентралізованих системах.

Тож Методика поєднує класичні підходи (статичний аналіз, верифікація) з сучасними (ШІ та динамічне моделювання атак). Це дозволяє забезпечити всебічний аналіз безпеки смарт-контрактів, включно із системами квадратичного голосування.

Забезпечення безпеки смарт-контрактів є комплексним завданням, що вимагає поєднання різних підходів та технологій. Формальна верифікація, статичний аналіз коду, дотримання перевірених патернів програмування та використання штучного інтелекту для виявлення аномалій формують багаторівневу систему захисту, здатну значно знизити ризики успішних атак. Враховуючи природу смарт-контрактів та їх застосування у таких сферах, як фінансові операції та голосування, ефективне управління ризиками через комбінування різних методів стає критичним для запобігання потенційним загрозам.

У роботі були розглянуті загальні механізми атак випередження та запропоновані заходи захисту, однак для перспективою є доповнення методики математичним моделюванням ймовірності таких атак. Поєднання комплексного підходу до виявлення та запобігання атакам, запропонованого у нашій роботі, з математичним аналізом ймовірності їх успіху дозволить підвищити рівень безпеки смарт-контрактів. Зокрема, моделювання ризиків атак випередження може стати ефективним доповненням до систем раннього виявлення аномальних транзакцій та адаптивного встановлення комісій.

1. Apix-Drive. Розповідаємо, що таке блокчейн простими словами - як працює мережа, як будуються блоки, що роблять майнери. https://apix-drive.com/ua/blog/useful/tehnologija-blokchejn-sho-ce-i-jak-pracjue

2. Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A Survey of Attacks on Ethereum Smart Contracts. В Principles of Security and Trust (с. 164-186).

3. Benhaim, A., Falk, B. H., & Tsoukalas, G. (2023). Balancing Power in Decentralized Governance: Quadratic Voting under Imperfect Information (с. 1-4).

4. Ковальчук Л. В., Вихло А. О. Оцінка ймовірності успіху фронтової атаки на смарт-контракти. *Cybern Syst Anal* **60** , 881–890 (2024). https://doi.org/10.1007/s10559-024-00725-z

М.Б.Фесенко

КЛІЄНТ-СЕРВЕРНА АРХІТЕКТУРА ДОСТУПУ ДО БАЗИ ЗНАНЬ З ВИКОРИСТАННЯМ БЛОКЧЕЙН ТЕХНОЛОГІЇ

У країні сформована величезна аудиторія користувачів смартфонів. Сучасна телефонія не тільки дозволяє виконувати комунікації, а також отримувати будь-яку інформацію. Для цього задіяна інфраструктура Інтернет та мобільних платформ. Ця інформація далеко не завжди систематизована та підготована щодо її вивчення та засвоєння, а також не завжди достовірна. Однієї зі складних форм представлення інформації є формування баз знань (БЗ). Зараз дуже актуальною темою є інформування населення країни про небезпеку її життя, зокрема від особо небезпечних засобів (ОНЗ). Населення обов'язково має бути попереджено про небезпеку. Тому що прийняття особистого рішення про те, залишити країну, або залишитися у неї, незважаючи на безпеку життя, має бути свідомим. Ця інформація має бути достовірною, непошкодженою та достатньо захищеною від хакерских атак.

Предметна область ОНЗ поділяється на рухомі та стаціонарні ОНЗ. До рухомих ОНЗ належать озброєні безпілотні літальні апарати військового призначення, артилерійське, мінометне, бомбове та ракетне озброєння, боєприпаси ударних апаратів, а також елементи касетних боєприпасів, зокрема міни. До нерухомих ОНЗ належать стаціонарно встановлені міни, гранати, саморобні вибухові пристрої, бензосховища, сховища піротехніки, сховища боєприпасів, бензо та газо заправки, газопроводи, нафтопроводи та об'єкти енергетики, зокрема греблі ГЕС. Ураження стаціонарних ОНЗ може призвести до техногенної події не тільки у акваторії та поблизу пошкодженого або знищуваного об'єкту ОНЗ, але й на значно більших територіях, де мешкає цивільне населення. Приклад такої події вже маємо - це підрив греблі Каховскої ГЕС. В умовах військового стану кількість ОНЗ поступово зростає. ОНЗ вже маємо уявляти як предметну область щодо онтологічного моделювання та побудови бази знань. Цивільне населення країни має у цілому вельми віддалене представлення щодо ОНЗ, що вже знаходяться, або можуть опинитися поруч з ними. Для побудови предметно-орієнтованої бази знань необхідно онтологічне представлення ОНЗ.

Метою нашої роботи є побудова онтологічної бази знань (ОБЗ) щодо ОНЗ забруднення територій, де тимчасово або постійно мешкає цивільне населення. Така предметно — орієнтована ОБЗ призначена до попередження та інформування цивільного населення про дійсну неприховану небезпеку ОНЗ. Надійних відкритих джерел щодо ОНЗ зараз не так багато. Однак й вони не дуже достовірно використовують декілька базових понять, таких як підривач, запал, детонатор та деякі інші. Тому виникає проблема, як користувачу не заплутатися у цих базових поняттях, яки, може навмисно, даються не завжди вірно. Предметна область ОНЗ є своєрідне дзеркало, що відображає досягнення сучасної науки та техніки. Військова наука також не

стоїть на місці. Постійно з'являються новітні розробки, проходять випробування на полігонах та у бойових умовах. Сучасні війни та конфлікти мають економічну та промислову складову. Усе має свою ціну.

Інженерія знань минулих років мала вузьку спрямованість та обмежене коло користувачів. Звичайно використовувались статичні мови програмування. Розробники основну увагу приділяли алгоритмам, логіці та забезпеченню зладженої функціональності системи. Розробки систем штучного інтелекту не були розраховані на поширену аудиторію мережевого користувача та великі об'єми інформації. Поширена мережевість має досить великий вплив на інженерію знань. Якщо БЗ будується під сучасного користувача, то має використовувати й мережеві архітектури, платформи та інструменти. Предметно — орієнтована ОБЗ ОНЗ - це рухома субстанція, яка має постійно поповнюватися, змінюватися, оновлюватися, має свої керуєми бази даних (БД) відповідної предметної області. БЗ мають свої особисті знання-орієнтовані архітектури. БД предметної області також мають свої архітектурні традиції. Але не треба забувати, що ці окремі архітектури слід обов'язково перетинати зі клієнт-серверними архітектурами. Архітектура предметно-орієнтованої ОБЗ має також службову БД, що містить інформацію о користувачі та о системі. Але клієнт-серверна архітектура також має свої бази даних, де не тільки користувачі, але й ще провайдери та відношення між ними та інтелектуальною системою, за допомогою якої функціонує БЗ. Щоб не було збоїв у праці цього тандему, як раз зручно підходить технологія блокчейн. Вплив фреймворку клієнт-серверної архітектури на додаток, що розроблюється, неможливо не врахувати. Тому що цей фреймворк задає правила побудови архітектури додатка, задає вже на початковому етапі розробки поведінку за умовчанням та готові рішення для багатьох рутинних задач, тобто деякий каркас або структурний шаблон, що маємо пристосовувати, розширити, доповнити чи модифікувати згідно вказаним вимогам. Тому виникає парадоксальна ситуація, що основна інтелектуальна архітектура предметно-орієнтованої онтологічної бази знань для цієї хмарної розробки стає другорядною та значно втрачає у якості функціонування. При цьому виникає залежність збереження інтелектуального інформаційного ресурсу від провайдера cloud computing. У зв'язку з цим розробники інтелектуальних систем все частіше обмежуються побудовою лише БД. З ними значно менше клопоту, ніж з інтелектуальними БЗ.

Мобільні клієнт - серверні архітектури звичайно містять дві окремих частини: частина користувача, тобто клієнта, та серверна частина, що закрита та схована від клієнта. Частина користувача, тобто інтерфейс користувача User Interface (UI), формується як фронтенд. Для розробки фронтенда є фреймворки Angular, React, jQuery, Ember, що задають каркас будуємого додатку. Серверна частина архітектури, її бекенд, базисна частина системи, її внутрішня реалізація. Для розробки бекенда призначені фреймворки Laravel, Ruby on Rails. Як правило, бекенд реалізує увесь спектр Application Platform Infrastructure (API), що використовує фронтенд.

Для організації якісного зв'язку між інтелектуальною системою предметно — орієнтованої ОБЗ та аудиторією користувачів мобільних додатків маємо обрати конкуренто спроможну платформу та мову програмування. Не зважаючи на те, що існують декілька варіантів, вибір у нас невеликий. Тому уточнимо деякі ринкові моменти. Зараз платформа Flutter, мова програмування Dart та мобільна операційна система Android належать компанії Google, що перекупувала ці програмні продукти разом з патентами та фірмами, що їх розробили. Далі ці розробки були поєднані однією ціллю та дороблені до потрібного рівню. Інші конкуренто здатні розробки, за виключенням мобільної операційної системи iOS, були поступово витиснути з ринку. Тому на ринку смартфонів зараз панують два хазяїна, й цей факт треба урахувати щодо нашої розробки. Що ми й робимо. У даному випадку маємо аж чотири у одному, оскільки Google має ще хмарний сервіс Google Диск, тобто Google Cloud.

Інструменти фреймворку Flutter дозволяють створювати частини додатків, з якими взаємодіє як мобільний користувач, так й веб-користувач, що дозволяє охопити значну кількість потенційних користувачів. Але для розробки додатків маємо реалізувати множину функцій, що користувач не бачить, наприклад: аутентифікацію, зберігання файлів та аналітику. Для цього призначені AWS Amplify та Amplify Flutter. Платформа AWS Amplify створена для розробки захищених і масштабуємих додатків як для мобільних засобів, так й для мережі Інтернет. Amplify Flutter – це набір інструментів і бібліотек, що дає можливість надавати, компонувати та розгортувати серверні частини додатків Flutter. Amplify Flutter можливо використовувати для підключення додатку Flutter до AWS та вирішувати загальні проблеми серверної частини. Amplify Flutter надає можливість працювати з AWS та додавати загальні функції серверної частини у додаток Flutter.

За аналогією, у БЗ пропонуємо увести інтенд, тобто інтелектуальну серверну частину, що також скрита від користувача. Для інтенд теж треба розробити відповідний фреймворк. Тоді у поєднанні отримаємо увесь цикл клієнт-серверної розробки як full stack, тобто повний стек інструментів для розробки, що може використовувати увесь спектр технологій мобільної телефонії або веб-розробки. Зараз існує декілька технологій як створення фронтенд та бекенд, так й створення одразу фулленд, наприклад: client – server фреймворк Django. Ця розробка не належить Google. Більш того, виникають деякі обмеження між Django та середовищем виконання платформи Google App Engine, що дозволяють розробнику контролювати лише частину параметрів операційної системи та вносять деякі негаразди щодо розробки додатків. На ринку блокчейн фреймворків зараз ще не має просунутих розробок Google. Тому слід очікувати, що у найближчий час з'явиться нова розробка подібного фреймворку компанії Google. Якщо це відбудеться, то будемо мати приклад успіху вірно обміркованої стратегії, що дозволила зробити цілком сумісний повний фреймворк. За аналогією, назвемо цей майбутній продукт Google full framework.

Набір програмного забезпечення (SDK) Flutter дозволяє використовувати єдину кодову базу, що не залежить від платформи, для кросплатформної розробки мобільних додатків. Набір інструментів Firebase може поєднати одразу і серверну частину програми, і її базу даних з використанням хмарного сховища. Хмарні функції Firebase дозволяють надсилати запити безпосередньо на сервери Google, щоб їх відповідь була автоматичною. Для зберігання та передачі даних клієнту в застосунку маємо підключити декілька пакетів, зокрема, *firebase_core* і *cloud_firestore.*

Сучасний користувач мобільної мережі використовує то мобільні додатки, то веб-сайти. Поєднати одне та друге не так просто. Якщо з веб додатками не виникає значних проблем зі зміною інформації у блоках, то з мобільними додатками вони обов'язково виникають. Фактично кожна зміна інформації потребує перепрограмування додатку. Подібна проблема виникає й у блокчейн фреймворків, оскільки кожен блок цепі заборонено змінювати, а тільки уводити новий з попередженням усіх та консенсусом що до цієї зміни. Тобто ми бачимо, що фреймворки мобільних додатків та фреймворки блокчейн мають багато спільного. Це лише підтверджує той факт, що блокчейн технологія побудови ланцюжків блоків може бути розповсюджена на будь-яки взаємопов'язані інформаційні блоки. Поява бокових відгалужень типу сайдчейн, типу дерева графу збігається також з деякими моментами побудови ієрархічних онтологічних структур БЗ.

Основна перевага технології блокчейн, що впливає на її розповсюдження, це надійне зберігання ресурсу розробника, як цінностей у надійному банку. Друга перевага цієї технології полягає у тому, що фінансові питання підтримки розробленого ресурсу проводяться надійно та прозоро, зі хронологічним збереженням та відображенням усього процесу проплати та фінансових документів. Зі цепі цих комерційних блоків не може безслідно зникнути ні один блок. Тому розробник додатку може працювати впевнено та спокійно, якщо він своєчасно вносить плату за зберігання та забезпечення надійного функціонування своєї розробки. Сторонній користувач не в змозі наробити шкоди цьому ресурсу, доки він знаходиться під захистом технології блокчейн.

Блокчейн технологія дозволяє зробити фінансові питання прозорими, а також увести у них зворотній зв'язок. Але у відношення між власником та проектувальником ресурсу, з одного боку, та власником хмарного середовища, з іншого боку, ця технологія у багатьох випадках поки що "за бортом." Складається враження, що доставати її зі води поки що ніхто не збирається. На борту все спокійно, а що коїться поза бортом на цьому кораблі майже нікого не цікавить. Тому питання залишається актуальним щодо його вирішення.

НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

«ВИКОРИСТАННЯ БЛОКЧЕЙН ТЕХНОЛОГІЙ В ЕНЕРГЕТИЦІ – 2025»

Збірник матеріалів конференції

26 березня 2025 р.

Usage of blockchain technologies in energetics – 2025 : collection of materials of the scientific and practical conference, Kyiv, March 26, 2025, PIMEE of NAS of Ukraine. - 2025. - 84 p.

Використання блокчейн технологій в енергетиці – 2025: збірник матеріалів науково-практичної конференції, м. Київ, 26 березня 2025 р., ІПМЕ ім. Г.Є. Пухова НАН України. – 2025. – 84 с.