НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

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

НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

«ВИКОРИСТАННЯ БЛОКЧЕЙН ТЕХНОЛОГІЙ В ЕНЕРГЕТИЦІ – 2026»

Збірник матеріалів конференції
25 березня 2026 р.

Київ – 2026

УДК 620.9 + 349 + 004 + 003.26

Рекомендовано до друку Вченою радою
Інституту проблем моделювання в енергетиці
ім. Г.Є. Пухова НАН України
(протокол №4 від 26 березня 2026 р.)

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 – 2026: collection of materials of the scientific and practical conference, Kyiv, March 25, 2026, PIMEE of NAS of Ukraine. - 2026. - 66 p.

Використання блокчейн технологій в енергетиці – 2026 : збірник матеріалів науково-практичної конференції, м. Київ, 25 березня 2026 р., ІПМЕ ім. Г.Є. Пухова НАН України. – 2026. – 66 с.

ЗМІСТ

В.В. Мохор, В.А. Євдокімов, А.М. Кудін, Л.В. Ковальчук

ПРОТОКОЛ ДЕЦЕНТРАЛІЗОВАНИХ КУПІВЛІ-ПРОДАЖУ ЕЛЕКТРОЕНЕРГІЇ З ВИКОРИСТАННЯМ СМАРТ-КОНТРАКТІВ НА БЛОКЧЕЙНІ

1. Вступ.

Розвиток децентралізованої генерації, зростання частки відновлюваних джерел енергії та поява активних споживачів-виробників (prosumer) формують передумови для переходу до нових моделей організації ринку електроенергії. За таких умов особливого значення набувають механізми прямої взаємодії між учасниками ринку, зокрема peer-to-peer купівля-продаж електроенергії, що дає змогу зменшити кількість посередників, підвищити прозорість розрахунків і створити додаткові стимули для локальної генерації [1–3].

Одним із найбільш перспективних інструментів для підтримки таких моделей є блокчейн у поєднанні зі смарт-контрактами. У науковій літературі показано, що смарт-контракти можуть бути використані для автоматизації укладання та виконання енергетичних угод, фіксації обсягів постачання, реалізації правил розрахунків і зниження транзакційних витрат у децентралізованому середовищі [1, 2]. Окремі дослідження також розглядають застосування блокчейн-рішень для P2P-торгівлі електроенергією в мікромережах, де особливо важливими є питання довіри між учасниками, незмінності даних та прозорого підтвердження факту постачання енергії [3].

У цій доповіді пропонується протокол децентралізованої купівлі-продажу електроенергії з використанням смарт-контрактів на блокчейні, який враховує взаємодію між постачальником (виробником), споживачем та інвестором (кредитором). На відміну від найпростішої двосторонньої моделі, запропонований підхід передбачає також можливість дострокового фінансування постачальника шляхом створення фінансового смарт-контракту, забезпеченого майбутнім платежем споживача. Це дає змогу поєднати товарний контур постачання електроенергії з фінансовим контуром обігу відповідних цифрових активів та розширити практичні можливості впровадження P2P-ринку електроенергії.

2. Опис протоколу.

У цьому розділі ми опишемо основних учасників (сутності) протоколу та наведемо сам протокол.

Сутності:

- *Постачальник* та/або *Виробник* – продає ЕЕ
- *Споживач* – купує ЕЕ
- *Інвестор* – дає цільовий кредит Постачальнику та/або Виробнику під зобов’язання сплати Споживача за продану ЕЕ.
- Розрахунки по смарт-контрактам здійснюються через *уповноважені банки*, які є учасниками цього процесу.

Протокол:

Крок 1. Розміщення запитів та пропозицій.

Постачальник та/або Виробник - «мейкер» розміщує на відповідній блокчейн-платформі свою пропозицію щодо продажу ЕЕ (обсяги, терміни, способи/розклад надання, з якого джерела, тощо).

Зауваження: ціну можна не вказувати, оскільки вона в Ваткоїнах.

Споживач-«мейкер» розміщує відповідний запит.

Крок 2. Матчінг.

Постачальник та/або Виробник - «тейкер» знаходить відповідну пропозицію від споживача-«мейкера», і навпаки.

Крок 3. Укладання угоди між Постачальником та/або Виробником та Споживачем.

П/В та С укладають типову угоду, в якій вносяться параметри щодо обсягу, ціни та умови оплати, в якій визначається також можливість з боку П/В виставити на вторинний фінансовий ринок вартість укладеного контракту у вигляді Ваткоїна.

Формують відповідний товарний смарт-контракт.

П/В та С підписують товарний смарт-контракт, який фіксує обсяг поставленої електричної енергії та загальну вартість активу, який може бути реалізований на вторинному фінансовому ринку.

Крок 4. Вибір типу виконання контракту по оплаті.

Постачальник та/або Виробник вирішує, чи потрібно йому отримати кошти раніше ніж сплатить Споживач (варіант 2). У разі такого рішення Постачальник та/або Виробник створює фінансовій смарт-контракт (Ваткоїн), в якому визначена вартість його та дисконт до нього (як правило ця вартість буде дисконтована не більше одиниці). Зазначений контракт реалізовується на відповідних торгових площадках, на яких торгуються фінансові контракти і покупцем такого контракту буде Інвестор. При цьому, оплата Інвестору за цим контрактом буде здійснюватися з боку Споживача в сумі, яка визначена у товарному смарт-контракті.

Варіант 1 – без залучення Інвестора.

Варіант 2 – залучення Інвестора.

Наступні кроки залежать від вибору Варіанту.

<u>Варіант 1.</u>

Крок 5. Виконання угоди між Споживачем та Постачальником та/або Виробником.

С сплачує кошти П/В за отриману електричну енергію, яка була підтверджена оператором системи розподілу (як оператора комерційного обліку).

Укладений товарний смарт-контракт визначається - виконаним.

Варіант 2.

Крок 5. Виконання угоди між Споживачем та Інвестором.

С сплачує кошти І за отриману електричну енергію по укладеному товарному смарт-контракту, яка була підтверджена оператором системи розподілу (як оператора комерційного обліку). При цьому, оплата коштів С здійснюється після підтвердження від П/В щодо отримання коштів від Інвестора.

Укладені товарний смарт-контракт та фінансовий смарт-контракт визначається - виконаним.

3. Висновки.

Запропонований протокол децентралізованої купівлі-продажу електроенергії на блокчейні формалізує основні етапи взаємодії між постачальником (виробником), споживачем та, за потреби, інвестором. Його перевагою є поєднання прозорої фіксації параметрів постачання електроенергії у товарному смарт-контракті з можливістю окремого фінансового супроводу угоди через механізм токенізованого контракту. Це створює передумови для більш гнучких моделей розрахунків, зменшення ризиків невиконання зобов'язань та підвищення ліквідності на локальних ринках електроенергії.

Практична реалізація такого підходу потребує належної інтеграції блокчейн-платформи з системами комерційного обліку, а також нормативного врегулювання ролей учасників, порядку підтвердження поставки та механізмів банківського супроводу розрахунків. Разом з тим запропонований протокол може слугувати концептуальною основою для побудови цифрових платформ P2P-торгівлі електроенергією в децентралізованих енергетичних системах.

1. Aloqaily, M., Boukerche, A., Bouachir, O., Khalid, F., & Jangsher, S. (2020). An energy trade framework using smart contracts: Overview and challenges. IEEE Network, 34(4), 119–125. https://doi.org/10.1109/MNET.011.1900573

2. Lu, J., Wu, S., Cheng, H., Song, B., & Xiang, Z. (2021). Smart contract for electricity transactions and charge settlements using blockchain. Applied Stochastic Models in Business and Industry, 37(3), 442–453. https://doi.org/10.1002/asmb.2570

3. Kajaan, N. A. M., Amidi, N. H. N., Salam, Z., & Radzi, R. Z. R. M. (2022). Blockchain-Based Smart Contract for P2P Energy Trading in a Microgrid Environment. Journal of Physics: Conference Series, 2312, 012020. https://doi.org/10.1088/1742-6596/2312/1/012020

В.М. Горбачук, Д.І. Ніколенко, О.С. Павлюк, А.О. Камуз, С.П. Осипенко

СПЕЦІАЛІЗОВАНИЙ P2P-ТРЕЙДИНГ ЕЛЕКТРОЕНЕРГІЄЮ

Ринок розподіленого трейдингу електроенергією є суттєвим компонентом енергосистеми нового типу, де визначним механізмом служить одноранговий (peer-to-peer (P2P)) трейдинг (між користувачами однакового рангу). Оскільки просування P2P-трейдингу електроенергією стикається зі значними перешкодами, включаючи вразливості безпеки даних, інформаційну асиметрію та недостатньо розвинену систему оцінки кредитоспроможності протягом усього процесу трансакції, то варто звертати увагу на механізм консенсусу блокчейну та методологію для P2P-трейдингу електроенергією. Грунтуючись на цій методології, можна проектувати метод і механізм доступу до пулу ресурсів трейдингу електроенергією для побудови дерева рішень кредитного рейтингу, тим самим гарантуючи безпеку та достовірність (trustworthiness) вузлів P2P-трансакцій. Також можна проектувати оснований на смарт-контрактах механізм реагування на попит, дозволяючи просумерам (prosumers) подавати торгові вимоги та часові обмеження, виходячи зі своїх операційних умов, щоб гарантувати своєчасність трансакцій. Можна будувати багатокритеріальну цільову функцію з основаним на пріоритетах консенсусом та алгоритмом динамічної адаптації вагових коефіцієнтів. Включаючи поведінку користувачів як ключову метрику, можна знижувати рівні шкідливої діяльності (malicious activities), уможливлюючи автономність у блокчейні (on-chain autonomy). Динамічний консенсус блокчейну досягається шляхом мінімізації відхилення між цільовими показниками попиту та значеннями відповідності реакції (response matching), тим самим сприяючи балансу виробництва та споживання. Такий метод консенсусу можна емпірично перевіряти у лабораторних умовах шляхом проведення порівняльного аналізу (benchmarking) й аналізу продуктивності на блокчейні, досліджуючи його валідність і практичність. Уваги заслуговують новітні методології досліджень і рішень для P2P-трейдингу електроенергією.

У державних планах щодо розвитку відновлюваної енергетики пропонується поліпшувати основані на ринку механізми трейдингу для розподіленого виробництва електроенергії, стандартизувати процедури трейдингу та розширювати масштаби трансакцій. В цьому контексті P2P-трейдинг є новітнім підходом, який дозволяє просумерам енергії торгувати безпосередньо один з одним. Такий трейдинг є особливо зручним для розподілених енергосистем і широко вважається новою парадигмою, зумовленою декарбонізацією, децентралізацією та цифровізацією (decarbonization, decentralization, and digitalization (3D)) енергетичного сектору. На повністю децентралізованому P2P-ринку користувачі можуть автономно домовлятися про ціни та здійснювати трансакції без центрального органу. Однак така модель часто стикається з викликами безпеки,

включаючи витік інформації (information leakage), фальсифікацію даних (data tampering), недостатня прозорість трансакцій, недостатньо розвинену систему оцінки довіри. Спираючись на свою децентралізовану та непорушну природу, блокчейн сприяє встановленню заслуговуючого довіри (trustworthy) P2P-ринку трейдингу електроенергією, таким чином забезпечуючи життєспроможне вирішення вищезгаданих питань [1].

З перспективи інтегрованих технологій розробляється вдосконалена децентралізована система трейдингу електроенергією для підключених електромобілів (з мережевим підключенням) на паркувальних майданчиках, яка спирається на консорціумний блокчейн, машинне навчання та теоретико-ігрове моделювання для максимізації прибутковості трансакцій. Подібним чином запроваджується механізм CE-SDT (Secure blockchain based Distributed Community Energy Trading) з розподіленою системою трейдингу енергією спільноти, що користується економічною моделлю з подвійними токенами (dual-token) для заохочення залучення користувачів у виробництво та споживання зеленої енергії. В області прогнозування та ціноутворення застосовуються штучний інтелект і машинне навчання для передбачення виробництва фотоелектричної енергії в інтелектуальних (смарт-) мікромережах, тим самим підтримуючи функціонування самопідтримуваних ринків електроенергії [2].

Водночас проектується динамічна модель ціноутворення для послуг заряджання й розряджання електромобілів з метою зниження пікового навантаження. Для подальшого просування децентралізованого трейдингу створюється повністю децентралізована платформа P2P-трейдингу енергією, де всі ринкові функції та операційні правила втілюються через смарт-контракти, досягаючи повної операційної автономії. Також пропонується автономна модель P2P-трейдингу електроенергією для спільнот мікромереж, яка інтегрує гібридні системи накопичення енергії.

З перспективи зменшення ризиків кібербезпеки наголошується, що інтегрування блокчейну (часто в поєднанні з іншими технологіями) у складні смарт-мережі та системи трейдингу енергією вимагає всебічної ідентифікації загроз і втілення робастних контрзаходів для підвищення безпеки та надійності екосистеми. З цим тісно пов’язується та розробляється оснований на машинному навчанні протокол для виявлення атак введення хибних даних (False Data Injection) у середовищах P2P-трейдингу енергією, а потім запроваджується інтегрована платформа, що поєднує блокчейн, Інтернет речей та машинне навчання для зменшення критичних загроз кібербезпеці в смарт-мікромережах. В області проектування ринку створюється операційна модель P2P-трейдингу для мікромереж, спираючись на автоматизовані системи та смарт-контракти для поліпшення ефективності та безпеки трансакцій. З метою подальшого просування ринкової продуктивності доєднується теорія інформаційної ентропії, щоб будувати більш справедливу, ефективну та ризик-інформовану платформу трейдингу відновлюваною чи альтернативною енергією.

Дослідження оптимізації алгоритмів консенсусу досягають значного прогресу. Пропонується оснований на групуванні алгоритм, що включає механізм динамічного кількісного оцінювання вузлів (Dynamic node Scoring mechanism) для практичної візантійської відмовостійкості (practical byzantine fault tolerance (PBFT)) (DS-PBFT), який поліпшує ефективність консенсусу шляхом зменшення кількості вузлів-учасників. Подається метод, що спирається на історичні дані про трансакції, використовуючи алгоритм кластеризації для реорганізації консенсусної мережі в двошарову багатоконсенсусну кластерну архітектуру. Вдосконалюється алгоритм доведення репутації (Proof-of-Reputation-X) до першого загальнодоступного (бездозвольного; permissionless) механізму, основаного виключно на репутації, розвиваючи тему, яка досліджувалася в численних роботах, зосереджених на репутації та механізмах стимулювання вузлів. Пропонується алгоритм достовірного консенсусу (Trustworthy Consensus Algorithm) для з'ясування питань цілісності та наявності даних в архітектурах мікросервісів. Також подається механізм доведення більшості (Proof of Majority (PoM)), призначений для покращення децентралізації та зменшення споживання енергії. Розробляється алгоритм динамічної випадкової візантійської відмовостійкості (Dynamic Random Byzantine Fault Tolerance), який складається з трьох підалгоритмів для узгодженості рядків, верифікації даних та бінарної узгодженості.

Таким чином, хоча існують важливі дослідження щодо інтеграції блокчейну з іншими технологіями, з'ясування ризиків кібербезпеки й автоматизованих систем трейдингу, поєднання блокчейну з алгоритмами оптимізації цілей залишається недостатньо вивченим. Також бракує досліджень, що стосуються автентифікації користувачів, достовірності інформації та поведінкового нагляду в межах децентралізованих платформ трейдингу енергією. Що стосується алгоритмів консенсусу, існуючі результати часто залежать від основаного на ставках (stake-based) голосування вузлів, оптимізуючи продуктивність за допомогою механізмів репутації чи обмеження кількості учасників. Однак згадані загальні підходи не відповідають конкретним вимогам P2P-трейдингу електроенергією, наприклад, вимогам швидкого реагування та ефективного двостороннього зіставлення (bilateral matching). Тому пропонуються інноваційні механізми консенсусу блокчейну та методології, спеціально розроблені для P2P-трейдингу електроенергією. По-перше, дерево рішень щодо доступу до трейдингу електроенергією гарантує участь лише автентифікованих і заслуговуючих довіри вузлів. По-друге, метод консенсусу, оснований на багатокритеріальній цільовій функції, ідентифікує оптимальні збіги виробник-споживач за часових обмежень, підвищуючи рівні безпеки та своєчасності. По-третє, механізм кількісного оцінювання кредитоспроможності вбудовується у процес консенсусу блоків для підвищення автономності в блокчейні та запобігання зловмисній поведінці, яка заважає укладанню угод трейдингу. Ці інноваційні механізми з'ясовують такі критичні виклики, як виявлення підробки особистих даних (identity

forgery), придушення зловмисної діяльності, ефективне виконання трансакцій, точне зіставлення попиту та пропозиції. Разом ці механізми висувають нову методологію та практичне рішення для гарантування безпечної та стабільної роботи розподілених ринків електроенергії.

У відповідь на характеристики та ризики безпеки (наприклад, інформаційну асиметрію) P2P-трейдингу електроенергією будується основана на блокчейні платформу трейдингу. Щоб задовольняти численним вимогам (а) автентичність і достовірність вузлів трейдингу, б) точне зіставлення виробників і споживачів енергії, в) своєчасність трансакцій), проектується механізм консенсусу блокчейну для P2P-трейдингу електроенергією, оснований на багатокритеріальної цільової функції.

а) Автентичність і достовірність вузлів трейдингу визначають автентифікація особи, поведінкове кількісне оцінювання, масштаб трансакції.

б) Точне зіставлення виробництва та споживання визначають оснваний на пріоритетах консенсус і механізм динамічного консенсусу з адаптацією вагових коефіцієнтів.

в) Своєчасність трансакцій визначають часові обмеження і двораундовий процес верифікації широкомовлення (two-round broadcast verification process). Такий процес гарантує безпечну, автентифіковану комунікацію (наприклад, у візантійській відмовостійкості (Byzantine Fault Tolerance) чи багатосторонніх обчисленнях (Multi-Party Computation)), вимагаючи від вузлів обміну зобов'язаннями та даними протягом двох різних фаз. Зазвичай процес включає трансляцію значення чи хешу в першому раунді та розкриття фактичних даних/підпису в другому раунді, уможливлюючи перевіреним (чесним) вузлам виявляти шахрайство.

Спочатку створюється пул ресурсів для трейдингу електроенергією. Кредитні рейтинги в межах цього пулу оцінюються, виходячи з автентифікації ідентичності вузла, поведінкового кількісного оцінювання, обсягу трансакцій та інших відповідних факторів. Тільки користувачам, які відповідають заздалегідь визначеному кредитному порогу, дозволяється приєднуватися та брати участь у трейдингу, тим самим гарантуючи автентичність і достовірність усіх вузлів трансакцій. Згодом користувачі переключаються на смарт-контракти: сторони попиту встановлюють цілі трансакцій відповідно до своїх операційних потреб, а сторони, які відповідають, надають зворотний зв'язок сполучення (matching).

Користуючись основаним на пріоритетах алгоритмом консенсусу та механізмом динамічного консенсусу з адаптацією вагових коефіцієнтів, досягається точне узгодження (matching) між виробництвом та споживанням.

1. Gorbachuk, V., Bardadym, T., Dunaievskyi, M., Godliuk, V., Rybachok, D. (2025). Fundamentals of decentralized electricity markets. In: Usage of Blockchain Technologies in Energetics – 2025, 26 March 2025, Kyiv, Ukraine, pp. 15–18.

2. Romanuk, V. V. (2026). Smart contracts in decentralized energy markets:opportunities and regulatory challenges. *Системи та технології*, № 1 (71), pp. 107−117.

А.А. Вихло

ЗАЛЕЖНІСТЬ ЧАСУ ОБРОБКИ ТРАНЗАКЦІЇ ВІД РОЗМІРУ ЇЇ КОМІСІЇ ЯК ПАРАМЕТР АТАКИ ВИПЕРЕДЖЕННЯ В МЕРЕЖІ BITCOIN

Однією з основних складових частин блокчейн мережі є механізм включення транзакцій в блок. У більшості публічних блокчейн мереж майнери надають пріоритет транзакціям із вищою комісією з метою максимізації власної винагороди [1,2]. Така поведінка створює передумови для здійснення атак на порядок транзакцій всередині блоку.

Атака випередження – це різновид атак на смарт контракти в блокчейні в основі яких лежить маніпуляція порядком транзакцій в блоці [3]. Одним з методів виконання атаки є суттєве підвищення розміру комісії транзакції зловмисника для підвищення її пріоритету серед майнерів. Ефективність такого підходу зумовлена наявністю залежності між часом обробки транзакції та розміром її комісії. Дослідження з оптимізації розміру комісії та прогнозуванню часу очікування транзакції підтверджують існування такої залежності [4,5].

В роботі [6] наведено наступну математичну модель для розрахунку імовірності успіху атаки випередження типу заміщення. Нехай випадкова величина T_τ – це час обробки транзакції з комісією τ, Δ – час створення дублюючої транзакції, τ_1 – комісія оригінальної транзакції, τ_2 – комісія дублюючої транзакції. Припускається, що T_τ має експоненційний розподіл з параметром $\lambda = \lambda(\tau)$. Тоді імовірністю успіху атаки випередження типу заміщення обчислюється наступною формулою:

$$P_{dis}(\tau_1, \tau_2, \Delta) = e^{-\lambda(\tau_1)\cdot\Delta} \cdot \frac{\lambda(\tau_2)}{\lambda(\tau_1)+\lambda(\tau_2)} \quad (1)$$

Для подальшого дослідження важливо дослідити характер залежності між часом обробки транзакції та розміром її комісії в реальних умовах роботи блокчейн мережі. Хоч зазначені раніше роботи з оптимізації комісій [4,5] надають моделі для прогнозування, але не показують статистичний характер залежності, тому в цій роботі досліджується характер та сила статистичної залежності між розміром комісії транзакції та часом її обробки на прикладі мережі Bitcoin.

Введемо необхідні позначення. Нехай для дослідження цієї залежності було обрано набір розміром з n транзакцій, тоді позначимо час обробки транзакції як випадкову величину τ. Відповідно, введемо позначення $\tau_1, \tau_2, \ldots, \tau_n$, де τ_i – час обробки транзакції з індексом i в наборі розміру n.

Аналогічно введемо позначення η як випадкову величину, що відповідає розміру комісії транзакції, відповідно, введемо позначення $\eta_1, \eta_2, \ldots, \eta_n$, де η_i – розмір комісії транзакції з індексом i в наборі розміру n.

Таким чином потрібно дослідити залежність між τ_i та η_i для набору з n транзакцій.

Для аналізу характеру і сили залежності між часом обробки транзакції та розміром її комісії використовуються коефіцієнти Пірсона та Спірмана [7].

Коефіцієнт Пірсона показує силу та напрямок лінійної залежності між двома випадковими величинами. Відповідно, необхідно дослідити залежність між випадковими величинами τ та η, які приймають значення $\tau_1, \tau_2, \ldots, \tau_n$ та $\eta_1, \eta_2, \ldots, \eta_n$. В наших позначеннях коефіцієнт Пірсона буде відповідати наступній формулі:

$$r = \frac{\sum_{i=1}^{n}(\tau_i - \bar{\tau})(\eta_i - \bar{\eta})}{\sqrt{\sum_{i=1}^{n}(\tau_i - \bar{\tau})^2}\sqrt{\sum_{i=1}^{n}(\eta_i - \bar{\eta})^2}} \quad (2)$$

де η_i – розмір комісії транзакції з індексом i, τ_i – час обробки транзакції з індексом i, $\bar{\eta}$ – медіанне значення розміру комісії для вибірки транзакцій, $\bar{\tau}$ – медіанне значення часу обробки для вибірки транзакцій, n – розмір вибірки.

Коефіцієнт Спірмана показує монотонність залежності між двома випадковими величинами, не обов'язково лінійної. Вводячи позначення аналогічно до позначень коефіцієнта Пірсона ми отримуємо, що коефіцієнт Спірмана відповідає наступній формулі:

$$\rho = 1 - \frac{6\sum_{i=1}^{n}\left(R(\tau_i) - R(\eta_i)\right)^2}{n(n^2-1)} \quad (3)$$

де η_i – розмір комісії транзакції з індексом i, де τ_i – час обробки транзакції з індексом i, $R(\tau_i)$ – ранг i-го значення часу обробки транзакції, $R(\eta_i)$ – ранг i-го значення розміру комісії, n – розмір вибірки.

Для дослідження було зібрано дані послідовних блоків у різні періоди завантаженості мережі, що обирались на основі розміру мемпулу [5]. Для кожного блоку проводилась фільтрація від викидів даних та обчислювались коефіцієнти Спірмана та Пірсона. Для періодів високої, середньої та низької завантаженості мережі обирались набори послідовних блоків. Для більшості з них зберігалась закономірність значень коефіцієнтів Спірмана та Пірсона, яка наведена в наступних таблицях.

Таблиця 1 – Результати аналізу для періоду середньої завантаженості мережі. Початок спостереження – 27.12.2025 12:00.

Коефіцієнт Спірмана	Коефіцієнт Пірсона	Номер блоку
-0.3877	-0.0554	929702
-0.7670	-0.1527	929703
-0.9148	-0.2215	929704
-0.6870	-0.1545	929705
-0.8170	-0.3269	929706
-0.6180	-0.0204	929707
-0.8366	-0.1111	929708

-0.2410	-0.1713	929709
-0.0788	0.0293	929710
-0.7032	-0.0020	929711

Для блоків, обраних в період середньої завантаженості, коефіцієнт Спірмана в більшості випадків показує високий рівень спадної монотонності, а коефіцієнт Пірсона показує слабку силу негативної лінійної залежності. Такі значення коефіцієнтів відповідають наявності нелінійної залежності між досліджуваними випадковими величинами. Беручи до уваги напрямок монотонності можна підтвердити, що підвищення розміру комісії зменшує час обробки транзакції.

В обраних послідовних блоках також зустрічаються блоки, що не показали високих показників коефіцієнтів Спірмана і Пірсона, що стверджує про відсутність залежності, проте таку поведінку можна пояснити тим, що розмір мемпулу змінюється протягом досліджуваного періоду.

Таблиця 2 – Результати аналізу для періоду високої завантаженості мережі. Початок спостереження – 05.02.2026 16:00.

Коефіцієнт Спірмана	Коефіцієнт Пірсона	Номер блоку
-0.5499	-0.0773	935131
-0.1190	0.0092	935132
-0.5863	-0.0965	935133
-0.3898	-0.0572	935134
-0.0311	0.0262	935135
-0.1140	-0.0219	935136
-0.2847	-0.2484	935137
-0.5010	0.0185	935138
-0.0877	0.0257	935139
-0.3085	-0.0770	935140

Коефіцієнти Спірмана та Пірсона для блоків обраних в період високої завантаженості мережі зберігають спадаючу монотонність та нелінійний характер, але сила монотонності знижується до середніх показників. Такі результати можна пояснити більш різноманітними розмірами вищих комісій, які важче спрогнозувати.

Таблиця 3 – Результати аналізу для періоду низької завантаженості мережі. Початок спостереження – 24.02.2026 20:00.

Коефіцієнт Спірмана	Коефіцієнт Пірсона	Номер блоку
-0.0953	0.0246	938160
-0.7687	-0.1030	938161
-0.2466	-0.0567	938162
-0.6889	-0.2151	938163
-0.1581	0.0111	938164
-0.1561	-0.0024	938165

-0.1760	-0.0482	938166
-0.4691	-0.1015	938167
-0.2588	-0.0178	938168
-0.6440	-0.1449	938169

Для блоків, що були обрані в період низької завантаженості мережі, зберігається спадна монотонність і нелінійний характер залежності. Значення коефіцієнтів є нижчими ніж для блоків в період середньої завантаженості, що можна пояснити тим, що майнери не мають великого набору транзакцій в мемпулі, що спонукає їх опрацьовувати транзакції з низьким пріоритетом, тому в блоках з'являється більше транзакцій з низькою комісією та високим часом очікування. Також ці показники є вищими ніж в період високого завантаження, що можна пояснити тим, що розмір комісіє є менш різноманітним.

Результатом даної роботи є підтвердження існування та уточнення характеру статистичної залежності між часом обробки транзакцій і розміром комісії. Обчислені коефіцієнти Спірмана та Пірсона для обраних блоків показали наявність спадної монотонної залежності з нелінійним характером зв'язку. Подальший аналіз цієї залежності показав, що найточніше її описує нелінійна регресійна модель, представлена степеневими або логарифмічними функціями. Це дає змогу уточнити формулу ймовірності успіху атаки випередження типу заміщення шляхом більш точного опису параметра λ.

1. Kiffer, L., Levin, D., & Mislove, A. (2021). Selfish & opaque transaction ordering in the Bitcoin blockchain: The case for chain neutrality. arXiv. https://doi.org/10.48550/arXiv.2110.11740

2. Li, Y., Jiang, S., Peng, X., & Cui, Z. (2019). Measurement and analysis of the Bitcoin networks: A view from mining pools. arXiv. https://arxiv.org/abs/1902.07549

3. Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L., & Juels, A. (2020). Flash Boys 2.0: Frontrunning, transaction reordering, and consensus instability in decentralized exchanges. In 2020 IEEE Symposium on Security and Privacy (SP) (pp. 910–927). IEEE. https://doi.org/10.1109/SP40000.2020.00040

4. Zhang, L., Zhou, R., Liu, Q., Liu, C., & Babar, M. A. (2024). Transaction fee estimation in the Bitcoin system (arXiv:2405.15293). arXiv. https://doi.org/10.48550/arXiv.2405.15293

5. Gündlach, R., Stoepker, I. V., Kapodistria, S., & Resing, J. A. C. (2024). A holistic approach for Bitcoin confirmation times & optimal fee selection. arXiv. https://doi.org/10.48550/arXiv.2402.17474

6. Kovalchuk, L., & Vykhlo, A. (2024). Estimation of the probability of success of a frontrunning attack on smart contracts. Cybernetics and Systems Analysis, 60(4), 881–890. https://doi.org/10.1007/s10559-024-00725-z

7. Winter, J., Gosling, S., & Potter, J. (2016). Comparing the Pearson and Spearman correlation coefficients across distributions and sample sizes: A tutorial using simulations and empirical data. Psychological Methods, 21(3), 273–290. https://doi.org/10.1037/met0000079

М.Ю. Родінко

БЕЗПЕКА СМАРТ-КОНТРАКТІВ У ДЕЦЕНТРАЛІЗОВАНИХ ЕНЕРГЕТИЧНИХ МЕРЕЖАХ

1. Вступ

Перехід до концепції Smart Grid та децентралізованих енергетичних ринків (P2P-торгівля електроенергією) нерозривно пов'язаний із впровадженням технології блокчейну. Смарт-контракти в енергетиці оперують значними активами та керують критичною інфраструктурою [1]. Проте вразливості в коді контрактів можуть призвести не лише до фінансових втрат, а й до блокування енергорозподілу або маніпулювання цінами на енергоресурси.

Статистика за I квартал 2024 року свідчить, що експлойти смарт-контрактів призвели до втрат майже $45 мільйонів [2]. Основними викликами є наступні:

- незмінність коду (баги неможливо виправити після розгортання в мережі);
- фінансові ризики (зафіксована вартість активів під управлінням контрактів сягає мільярдів доларів);
- історичні прецеденти (інциденти типу TheDAO Hack та Parity Wallet Bug).

2. Ключові категорії вразливостей та їх вплив на енергетичні системи

Для енергетичного сектору найбільш небезпечними є наступні типи атак [3].

Повторний вхід (Re-entrancy). Повторний виклик функції виводу коштів до оновлення стану балансу. В енергетиці це може призвести до несанкціонованого «подвійного списання» токенів.

Маніпуляція оракулами. Спотворення цінових потоків для штучного завищення або заниження вартості електроенергії.

Атака випередження (Front-Running). Зловмисник спостерігає за пулом транзакцій і надсилає свою з вищою комісією, щоб першим викупити вигідний енергетичний лот.

Відмова в обслуговуванні (DoS). Блокування функцій контракту через вичерпання газу або несподівані помилки, що в енергомережах може призвести до зупинки розрахунків між споживачами та постачальниками.

Слабка випадковість. Використання детермінованих параметрів блоку для лотерей або розподілу ресурсів, що дозволяє майнерам маніпулювати результатами.

3. Методи забезпечення стійкості енергетичних блокчейн-платформ

Для мінімізації ризиків необхідно впроваджувати комплексні заходи безпеки на етапі розробки.

Апаратні та архітектурні патерни: Checks-Effects-Interactions. Критично важливо спочатку змінювати стан (баланс), а потім виконувати зовнішній виклик.

ReentrancyGuard. Використання модифікаторів блокування (Mutex) від перевірених бібліотек (наприклад, OpenZeppelin).

Pull over Push. Використання патерна «запиту» виплат самими користувачами замість автоматичного «надсилання» контрактом для запобігання DoS-атакам.

Криптографічні та програмні засоби: SafeMath та Solidity 0.8.0+. Запобігання переповненню цілих чисел, що критично для точності обліку кВт-годин.

Commit-Reveal схеми. Приховування деталей транзакцій для захисту від front-running-атак на енергоринках.

VRF. Використання децентралізованих оракулів випадковості для прозорого розподілу навантаження або ресурсів.

4. Рекомендації щодо науково-практичного впровадження

Для створення надійної енергетичної інфраструктури пропонується:

- прагнути до 100% покриття тестами (branch coverage) та застосовувати фаззінг-тестування;
- використовувати інструменти статичного аналізу (Slither) та символьного виконання для пошуку вразливостей перед деплоєм;
- проводити регулярні професійні аудити сторонніми компаніями;
- обмежувати привілеї функцій (принцип POLP) та використовувати MultiSig гаманці для критичного управління енергосистемою.

5. Висновок

Безпека смарт-контрактів є фундаментом довіри до децентралізованої енергетики. Хоча лише близько 0,30 % активів під ризиком було реально експлуатовано зловмисниками, потенційні наслідки для критичної інфраструктури вимагають суворого дотримання найкращих практик розробки та криптографічного захисту.

1. Vionis, P., & Kotsilieris, T. (2023). The potential of blockchain technology and smart contracts in the energy sector: a review. *Applied sciences*, *14*(1), 253.

2. Web3 Security Report Q1 2024 / Hacken. 2024. https://hacken.io/insights/q1-2024-security-report/ (дата звернення: 17.03.2026).

3. Atzei, N., Bartoletti, M., & Cimoli, T. (2017, March). A survey of attacks on ethereum smart contracts (sok). In *International conference on principles of security and trust* (pp. 164-186). Berlin, Heidelberg: Springer Berlin Heidelberg.

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

РОЗРОБКА ДЕЦЕНТРАЛІЗОВАНОГО МОБІЛЬНОГО ЗАСТОСУНКУ ДЛЯ P2P ТОРГІВЛІ ЗЕЛЕНОЮ ЕНЕРГІЄЮ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ REACTNATIVE ТА БІБЛІОТЕКИ ETHERS.JS

React — це популярна JavaScript-бібліотека з відкритим вихідним кодом, створена для ефективної розробки інтерфейсів користувача (frontend) у сучасних вебдодатках. Її головна особливість полягає у використанні віртуального DOM (Virtual DOM), що дозволяє мінімізувати прямі звернення до реального дерева сторінки та суттєво оптимізувати швидкість рендерингу і раціональне використання ресурсів браузера. Компонентна архітектура React базується на створенні незалежних, ізольованих модулів інтерфейсу, які можна багаторазово використовувати в різних частинах проєкту. Серед беззаперечних переваг цієї технології варто виділити декларативний підхід до опису UI, механізм миттєвого оновлення коду без втрати стану (Fast Refresh / Hot Reloading), передбачуваність управління даними, а також величезну екосистему готових рішень, підтримувану багатомільйонною спільнотою розробників.

React Native — це передовий кросплатформний фреймворк від компанії Meta, призначений для створення мобільних застосунків (iOS та Android) з використанням єдиної кодової бази. На відміну від гібридних рішень, що працюють через WebView, React Native транслює JavaScript-код у нативні компоненти операційної системи, забезпечуючи високу продуктивність, наближену до додатків, написаних мовами Swift або Kotlin. В основі його архітектури лежить той самий компонентний підхід, що й у вебверсії React. Завдяки інкапсуляції логіки, стилів та стану всередині кожного компонента, розробники можуть легко декомпозувати складні екрани на прості та керовані елементи — від базових кнопок та текстових полів до складних навігаційних панелей та динамічних списків. Це робить архітектуру мобільного додатка прозорою та легко масштабованою.

Платформа Expo та її мобільний клієнт Expo Go формують потужну комплексну екосистему інструментів і сервісів, побудовану поверх React Native, яка радикально оптимізує весь життєвий цикл розробки мобільних додатків. Використання Expo абстрагує розробників від складного налаштування нативних середовищ (таких як Android Studio чи Xcode), суттєво знижуючи поріг входу. Клієнт Expo Go дає змогу миттєво тестувати прототипи на реальних фізичних пристроях шляхом простого сканування QR-коду. Інфраструктура Expo надає багатий набір універсальних, готових API для роботи з апаратними модулями смартфона (камера, геолокація, файлова система). Крім того, екосистема пропонує механізми безпровідного оновлення (Over-The-Air, OTA), що дозволяє миттєво доставляти

виправлення користувачам, а також значно спрощує процеси компіляції та публікації у маркетах додатків.

Ethers.js — це оптимізована, безпечна та легковагова JavaScript/TypeScript-бібліотека, яка стала галузевим стандартом для взаємодії клієнтських додатків із блокчейном Ethereum та іншими EVM-сумісними мережами. Вона відіграє роль критичного моста між традиційним фронтендом (Web2) та децентралізованими технологіями (Web3). Інструментарій Ethers.js охоплює безпечне управління криптографічними ключами, створення та підписання транзакцій, а також взаємодію зі смарт-контрактами (через їхній ABI). Бібліотека забезпечує надійне з'єднання з блокчейн-вузлами через інфраструктурних RPC-провайдерів, таких як Infura чи Alchemy, або безпосередньо через браузерні гаманці на кшталт MetaMask. Її модульна структура та вбудована типізація роблять її ідеальним вибором для розробки захищених децентралізованих застосунків (dApps).

Таким чином, враховуючи, що в ролі бекенду (backend) виступають децентралізовані смарт-контракти, написані мовою Solidity, обрання запропонованого технологічного стеку створює максимально синергетичне середовище. Оскільки в основі як вебверсії, так і мобільного застосунку лежить єдина парадигма React, команди програмістів отримують можливість вести паралельну розробку обох платформ. Це дозволяє перевикористовувати значну частину бізнес-логіки, архітектурних шаблонів та функцій взаємодії з блокчейном. Такий підхід не лише мінімізує обсяг дубльованого коду, але й значно полегшує процеси командної співпраці, прискорює розгортання проєкту та підвищує загальну надійність і зручність тестування розроблюваного програмного забезпечення.

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. React. The library for web and native user interfaces https://react.dev/
2. Create native apps for Android, iOS, and more using React https://reactnative.dev/
3. Expo Go is a learning environment and sandbox for getting started https://expo.dev/go
4. The ethers.js library https://docs.ethers.org/v6/

М.Д. Стрєльніков

POST-QUANTUM SECURE POLYNOMIAL SECRET SHARING WITH FRI COMMITMENTS

1. Introduction

Verifiable Secret Sharing (VSS) [1, 2] is a cryptographic primitive utilized in blockchain for distributed key generation [3], threshold signature schemes [4], and safeguarding of private keys in modern blockchain wallets [5]. This thesis introduces a post-quantum VSS scheme with non-interactive Fast Reed-Solomon Interactive Oracle Proofs (FRI) based on hash pre-image forging assumptions. We view Shamir's Secret Sharing as a Reed-Solomon code [6] to ensure compatibility with FRI commitments and provide Byzantine fault tolerance without peer-to-peer communication overhead. The usage of FRI commitments enables efficient erasure coding by deterministic identification of corrupted shares. Downsides of the approachs are larger proof sizes compared to elliptic curve commitments (e.g., KZG) [7] and requiring the share count n to be a power of 2 for FRI domains [8, 9, 10].

2. Shamir Secret Sharing Scheme

Definition 1.1 (Shamir Secret Sharing [11, 12]). Let F_p be a finite field order $p > n$. The dealer picks a random degree $k-1$ polynomial $f(x)$ with $f(0) = s$ for n distinct points $\alpha_i \in F_p$. A share is $(\alpha_i, f(\alpha_i))$, coinciding with a Generalized Reed-Solomon (GRS) code evaluation points[13, 14]:

$$C_{GRS} = \{(f(\alpha_1), \dots, f(\alpha_n)) : f \in F_p[x], \deg(f) < k\} \quad (1)$$

Definition 1.2 (Passive Adversary [15]). Intercepts $e < k$ shares to learn s.

Lemma 1.1. An adversary with $e < k$ shares faces an $e \times k$ underdetermined Vandermonde subsystem:

$$\begin{pmatrix} y_{i_1} \\ \vdots \\ y_{i_e} \end{pmatrix} = \begin{pmatrix} 1 & \alpha_{i_1} & \cdots & \alpha_{i_1}^{k-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_{i_e} & \cdots & \alpha_{i_e}^{k-1} \end{pmatrix} \begin{pmatrix} s \\ b_1 \\ \vdots \\ b_{k-1} \end{pmatrix} \quad (2)$$

where matrix G_E constisting from distinct evaluation points has full row rank e. By the Kronecker–Capelli theorem, there are p^{k-e} solution candidtes. The free variables leave s unconstrained implying that any $s' \in F_p$ is equally likely. ■

Corollary (Point Independence). The resulting security depends on full row rank, providing a perfect secrecy for point selection even if chosen not randomly. Applying this property, we require shares be selected as

$(\omega_i, f(\omega_i))$ where ω_i are n-th power roots of unity to ensure compatibility with standard Reed-Solomon code and FRI-commitments without losing in security [16].

Definition 1.3 (Active Adversary [15]). Interferes with normal protocol execution by supplying incorrect shares $y_i' \neq f(\alpha_i)$ to affect the reconstruction of the secret.

Theorem 1.1 (Byzantine Fault Tolerance [17]). Unique reconstruction under $e < k$ corrupted shares requires:

$$n \geq k + 2e \Leftrightarrow e \leq \lfloor \frac{n-k}{2} \rfloor \quad (3)$$

corresponding to the generalized Reed-Solomon error correction capability. But Shamir secret scheme with Lagrange decoder does not provide an efficient way to detect corrupted shares unless attempted to reconstruct.

Lemma 1.2 (Lagrange decoder search space [18]). Brute-force checking share combinations to find k valid shares yields:

$$\binom{n}{k} \approx \frac{2^{n \cdot H(k/n)}}{\sqrt{2\pi k(1-k/n)n}} \quad (4)$$

where $H(p)$ is the binary entropy function for $p = k/n$. For maximum fault tolerance ($k = n/2$), growth is $\binom{n}{n/2} \sim \Theta(2^n/\sqrt{n})$, making naive decoding computationally infeasible on practice.■

2. Fast Reed-Solomon Interactive Oracle Proofs (FRI)

We introduce polynomial oracle proofs to detect corrupted shares by avoiding combinatorial search of consistent shares. Polynomial oracle proofs allows to obtain post-quantum secure FRI-commitments from the same secret sharing polynomial.

Definition 2.1 (Interactive Oracle Proof [19]). A public-coin query protocol where the Prover commits to a function f asserting proximity to an RS codeword, and the Verifier issues random challenges and queries points.

FRI tests polynomial degree [20] without evaluating all k coefficients:

1. Fold to halve the degree of original polynomial f
2. Check consistency providing random challenges
3. Verify the final constant directly.

Definition 2.2 (Folding). For a polynomial $f(x)$ of degree d evaluated at n points (power of 2):

1. Split polynomial by even and odd additives $f(x) = g(x^2) + x \cdot h(x^2)$ with $\deg(g), \deg(h) < d/2$
2. Fold by halving the evaluation domain for even powers $\{\omega^0, \omega^2, \omega^4, \dots\}$
3. Verifier provides random challenges β into $f'(z) = g(z) + \beta \cdot h(z)$

Honesty preserves $\deg(f') < d/2$. Cheating attempts yield contradictions with probability $d/|F_p|$ provided by the Schwartz-Zippel lemma [21, 22, 23].

Iterative folding yields a constant polynomial at the end $\deg(f) \to \deg(f') \to \cdots \to 0$. The verification requires checking $O(\log_2 n)$ points across $O(\log_2 d)$ rounds reduces verification to $O(\log^2 n)$ time instead of all *n* points.

Definition 3.1 (FRI Output Transcript [24]). The output of the non-interactive FRI protocol is a transcript $T = \left(\{c_i\}_{i=0}^{L}, f_{final}, Q\right)$, containing:

1. $L + 1$ Merkle tree roots c_i representing evaluations of folded polynomials f_i at each layer
2. constant value f_{final} of the fully folded polynomial.
3. A set of query authentication paths Q proving the evaluations of $f_0, \ldots, f_{L-1}$ at ℓ pseudorandomly derived indices t_j and $-t_j$.

Algorithm 3.1 (Commitment Verification [20]). Given the transcript T:

1. Reconstruct folding challenges $\beta_i = hash(T_{i-1})$ and query indices $t_j = hash(T, j)$.
2. Verify all Merkle paths in Q against their respective roots c_i.
3. For each query index across all layers $i \in \{0, \ldots, L-1\}$, verify the algebraic folding relation:
$$f_{i+1}(z^2) = \frac{f_i(z)+f_i(-z)}{2} + \beta_i \frac{f_i(z)-f_i(-z)}{2z} \quad (5)$$
4. Ensure the evaluations at the last layer exactly match the committed constant f_{final}.

Exponential increase of query number ℓ results in linearly increase of verification.

Lookup for Table — 1 for all FRI commitment parameters.

3. Verifiable Polynomial Secret Sharing with FRI Commitments

Using the Fiat-Shamir transform [15] we obtain non-interactive FRI by replacing verifier provided random challenges with deterministic ones β_i obtained from chain of transcript T_i hashes ($\beta_i = hash(T_{i-1})$), binding queries without exposing any additional information (refer to Appendix, Table — 2 for the challenge generation breakdown).

Verifiable secret sharing protocol requires evaluations over the n-th power roots of unity domain $D_0 = \{\omega^0, \ldots, \omega^{n-1}\}$:

1. Dealer evaluates degree k polynomial $f(x)$ to distribute shares.
2. Dealer provides an FRI-commitment proving low-degree structure.
3. Participants independently verify the proof offline.

The failure probability is a disjunctiove sum of events combining list decoding [25, 26], Schwartz-Zippel, and FRI folding terms:

$$\epsilon_{total} = \left(\frac{\delta}{\delta-\tau}\right)^{\ell} + \frac{\ell \cdot k}{F_p} + \ell(1-\rho)^L \qquad (6)$$

where $\tau = 1 - \sqrt{\rho}$ is the Johnson bound, $\rho = k/n$ is the code rate, and $L = \lceil \log_2 k \rceil$. A valid FRI transcript serves as an unforgeable cryptographic receipt.

Verifiable secret reconstruction:

1. Authenticate individual shares via Merkle proofs [27] against the dealer's original commitment.
2. Ensure polynomial consistency via the verified FRI transcript.
3. Reconstruct secret via Lagrange interpolation on k or more authenticated shares.

Invalid share filtering downgrades Byzantine errors into standard erasures, allowing interpolation without combinatorial searches. FRI guarantees the commitment is δ-close to a valid polynomial, ensuring the true polynomial is extracted.

Conclusions

In this work we interpreted Shamir's VSS scheme through modern coding theory viewing secret sharing polynomial as an Reed-Solomon code to add verification layer with Fast Reed-Solomon Interactive Oracle Proofs (FRI). The proposed design inspired by Feldman's [2] and Pedersen's VSS protocol for simplicity and absence of peer-to-peer communication by replacing vulnerable discrete logarithm primitives with Merkle Tree commitments in quantum computation model.

The proposed protocol relies exclusively on hashes, oppose to SNARK-based VSS which often rely on trusted setups or elliptic curve pairings (KZG [7]) or more complex Lattice-based secret sharing (requires noise-management and massive evaluation keys) [29]. When evaluated against similar STARK-based secret sharing schemes [30], our distinction is the separation of Byzantine error detection from algebraic correction avoiding construction of locator polynomials (e.g., Berlekamp-Welch or Gao [17, 28]). Instead, corrupted shares are deterministically filtered out in logarithmical time by utilizing Merkle Tree commitments. FRI proximity ensures the secret polynomial is close to a valid low-degree polynomial. Byzantine fault tolerance is reduced to erasure decoding provided by deterministic Merkle filtering of corrupted shares using classic standard Lagrange interpolation.

1. Chor, B., Goldwasser, S., Micali, S., & Awerbuch, B. (1985). Verifiable secret sharing and achieving simultaneity in the presence of faults. In *26th Annual Symposium on Foundations of Computer Science* (pp. 383–395). IEEE. https://doi.org/10.1109/SFCS.1985.64

2. Feldman, P. (1987). A practical scheme for non-interactive verifiable secret sharing. In *28th Annual Symposium on Foundations of Computer Science* (pp. 427–438). IEEE. https://doi.org/10.1109/SFCS.1987.4

3. Gennaro, R., Jarecki, S., Krawczyk, H., & Rabin, T. (2007). Secure distributed key generation for discrete-log based cryptosystems. *Journal of Cryptology*, *20*(1), 51–83. https://doi.org/10.1007/s00145-006-0347-1

4. Komlo, C., & Goldberg, I. (2020). FROST: Flexible Round-Optimized Schnorr Threshold Signatures. In *Selected Areas in Cryptography – SAC 2020* (pp. 34–65). Springer. https://doi.org/10.1007/978-3-030-81652-0_2

5. Goldfeder, S., Gennaro, R., Kalodner, H., Bonneau, J., Kroll, J. A., Felten, E. W., & Narayanan, A. (2015). Securing Bitcoin wallets via a new DSA/ECDSA threshold signature scheme. *IACR Cryptology ePrint Archive*, Report 2015/096. https://eprint.iacr.org/2015/096

6. McEliece, R. J., & Sarwate, D. V. (1981). On sharing secrets and Reed-Solomon codes. *Communications of the ACM*, *24*(9), 583–584. https://doi.org/10.1145/358746.358762

7. Vlasov, A., & Panarin, K. (2019). Transparent polynomial commitment scheme with polylogarithmic communication complexity. *Cryptology ePrint Archive*, *2019*, 1020. https://eprint.iacr.org/2019/1020

8. Cooley, J. W., & Tukey, J. W. (1965). An algorithm for the machine calculation of complex Fourier series. *Mathematics of Computation*, *19*(90), 297–301. https://doi.org/10.1090/S0025-5718-1965-0178586-1

9. Pollard, J. M. (1971). The fast Fourier transform in a finite field. *Mathematics of Computation*, *25*(114), 365–374. https://doi.org/10.1090/S0025-5718-1971-0301966-0

10. Haböck, U. (2022). A summary on the FRI low degree test. *Cryptology ePrint Archive*, *2022*, 1216. https://eprint.iacr.org/2022/1216

11. Shamir, A. (1979). How to share a secret. *Communications of the ACM*, *22*(11), 612–613. https://doi.org/10.1145/359168.359176

12. Blakley, G. R. (1979). Safeguarding cryptographic keys. In *Proceedings of the 1979 AFIPS National Computer Conference* (pp. 313–317). https://doi.org/10.1109/MARK.1979.8817296

13. Reed, I. S., & Solomon, G. (1960). Polynomial codes over certain finite fields. *Journal of the Society for Industrial and Applied Mathematics*, *8*(2), 300–304. https://doi.org/10.1137/0108018

14. Loidreau, P., & Overbeck, R. (2013). On generalized Reed-Solomon codes over commutative and noncommutative rings. *IEEE Transactions on Information Theory*, *59*(9), 5903–5925. https://doi.org/10.1109/TIT.2013.2264797

15. Katz, J., & Lindell, Y. (2014). *Introduction to modern cryptography* (2nd ed.). CRC Press. https://doi.org/10.1201/9781351133036

16. Massey, J. L. (1993). Minimal codewords and secret sharing. In *Proc. 6th Joint Swedish-Russian Int. Workshop on Information Theory* (pp. 276–279). https://www.semanticscholar.org/paper/Minimal-Codewords-and-Secret-Sharing-Massey/9f4bb6d9608aa18d86697253f51f984dd735c02a

17. Berlekamp, E. R. (1968). *Algebraic coding theory*. McGraw-Hill. https://doi.org/10.1142/9407

18. Cover, T. M., & Thomas, J. A. (2006). *Elements of information theory* (2nd ed.). Wiley-Interscience.

19. Ben-Sasson, E., Chiesa, A., & Spooner, N. (2016). Interactive oracle proofs. In *Theory of Cryptography Conference* (pp. 31–60). Springer. https://doi.org/10.1007/978-3-662-53644-5_2

20. Ben-Sasson, E., Bentov, I., Damgård, I., Goldberg, L., Halevi, S., Horesh, Y., … & Silberstein, M. (2018). Fast Reed-Solomon interactive oracle proofs of proximity. *IACR Cryptology ePrint Archive, 2018*, 46. https://eprint.iacr.org/2018/046

21. DeMillo, R. A., & Lipton, R. J. (1978). A probabilistic remark on algebraic program testing. *Information Processing Letters, 7*(4), 193–195. https://doi.org/10.1016/0020-0190(78)90067-4

22. Schwartz, J. T. (1980). Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM, 27*(4), 701–717. https://doi.org/10.1145/322217.322228

23. Zippel, R. (1979). Probabilistic algorithms for sparse polynomials. In *Symbolic and algebraic computation* (pp. 216–226). Springer. https://doi.org/10.1007/3-540-09519-5_73

24. Ben-Sasson, E., Carmon, D., Kopparty, S., & Levit, D. (2020). Scalable and transparent proofs over all large fields, via elliptic curves (DEEP-FRI). *IACR Cryptology ePrint Archive, 2020*, 654. https://eprint.iacr.org/2020/654

25. Guruswami, V., & Sudan, M. (1999). Improved decoding of Reed-Solomon and algebraic-geometry codes. *IEEE Transactions on Information Theory, 45*(6), 1757–1767. https://doi.org/10.1109/18.782097

26. Guruswami, V., & Rudra, A. (2008). Explicit codes achieving list decoding capacity: Error-correction with optimal redundancy. *IEEE Transactions on Information Theory, 54*(1), 135–150. https://doi.org/10.1109/TIT.2007.911222

27. Merkle, R. C. (1980). Protocols for public key cryptosystems. In *IEEE Symposium on Security and Privacy* (pp. 122–133). IEEE. https://doi.org/10.1109/SP.1980.10006

28. Gao, S. (2003). A new algorithm for decoding Reed-Solomon codes. In *Communications, information and network security* (pp. 55–68). Springer. https://www.semanticscholar.org/paper/A-New-Algorithm-for-Decoding-Reed-Solomon-Codes-Gao/63443556477273b8f64ed63bf7eb86b0ad1dbca5

29. Abdolmaleki, B., Clark, J., Foroutani, M., Khazaei, S., & Nasirzadeh, S. (2025). A Generic Framework for Practical Lattice-Based Non-interactive Publicly Verifiable Secret Sharing. *Cryptology ePrint Archive*, Report 2025/901. https://ia.cr/2025/901

30. Das, S., Xiang, Z., Tomescu, A., Spiegelman, A., Pinkas, B., & Ren, L. (2025). Verifiable Secret Sharing Simplified. *Proceedings - 46th IEEE Symposium on Security and Privacy, SP 2025* (pp. 633-651). https://doi.org/10.1109/SP61157.2025.00046

APPENDIX

Table — 1. FRI Protocol Parameters

Parameter	Symbol	Description	Typical Value
Blowup Factor	$\lambda = n/k$	Ratio of domain size to polynomial	4-8

		degree	
Folding Factor	η	Degree reduction per round	2 (halving)
Number of Rounds	L	Folding iterations until constant	$\lceil \log_2(k) \rceil$
Query Complexity	ℓ	Number of random query repetitions	20-100
Soundness Error	ϵ	Probability of accepting bad proof	$2^{-\lambda \cdot \ell}$ for $\lambda > 0$
Code Rate	$\rho = k/n$	Ratio of message to codeword	0.25 (rate-1/4)
Proximity Bound	$1 - \sqrt{\rho}$	Johnson list-decoding radius	0.5 for $\rho = 0.25$

Table — 2**.** FRI Challenge generation for interactive and non-interactive regimes

Step	Interactive	Non-Interactive
Commit c_0	Prover sends c_0	Prover sends c_0
Challenge β_0	Verifier sends random β_0	$\beta_0 = hash(c_0)$
Commit c_1	Prover sends c_1	Prover sends c_1
Challenge β_1	Verifier sends random β_1	$\beta_1 = hash(c_0, c_1)$
…	…	…
Query positions	Verifier queries random t_j	$t_j = hash(T, j)$

І.В. Чаус

АНАЛІЗ ОСОБЛИВОСТЕЙ ІСНУЮЧИХ ТА ІННОВАЦІЙНИХ РІШЕНЬ В ЕНЕРГЕТИЧНІЙ ГАЛУЗІ, ЩО ВИКОРИСТОВУЮТЬ БЛОКЧЕЙН

Енергетична галузь у XXI столітті перебуває на перетині глобальних викликів та інноваційних можливостей. Зростання попиту на енергію, необхідність переходу до відновлюваних джерел, проблеми екологічної безпеки та кіберзагроз формують нову парадигму розвитку енергетики. Традиційні моделі управління та ринкової взаємодії вже не відповідають сучасним потребам, що стимулює пошук технологій, здатних забезпечити прозорість, ефективність та стійкість енергетичних систем [1].

Однією з таких технологій є блокчейн, який спочатку був розроблений для фінансової сфери, але поступово знайшов застосування у багатьох галузях, включно з енергетикою. Його ключові характеристики — децентралізація, незмінність записів, прозорість та високий рівень безпеки — роблять блокчейн перспективним інструментом для управління енергетичними процесами [2].

Використання блокчейну в енергетиці охоплює широкий спектр рішень: від смарт-контрактів для автоматизації угод до створення децентралізованих ринків електроенергії, інтеграції відновлюваних джерел та управління мікромережами. Ці інновації дозволяють не лише оптимізувати процеси, але й формують нову модель взаємодії між виробниками, споживачами та державними інституціями [3].

Актуальність дослідження визначається кількома чинниками:

- глобальним переходом до «зеленої» економіки та відновлюваних джерел енергії;
- потребою у підвищенні прозорості та безпеки енергетичних транзакцій;
- розвитком децентралізованих ринків, які змінюють традиційні моделі торгівлі електроенергією;
- необхідністю інтеграції України у світовий енергетичний простір та впровадження сучасних технологій.

Таким чином, аналіз існуючих та інноваційних рішень у сфері енергетики, що базуються на блокчейн-технологіях, є важливим завданням як для наукової спільноти, так і для практиків, адже він дозволяє визначити перспективи розвитку галузі, окреслити проблеми та сформувати рекомендації щодо їх подолання.

1. Існуючі рішення у сфері енергетики на основі блокчейну

1.1. Смарт-контракти для укладання договорів

Смарт-контракти — це програмні алгоритми, які автоматично виконують умови угоди після настання визначених подій. У сфері енергетики вони застосовуються для:

- автоматизації процесів купівлі-продажу електроенергії;

• зменшення транзакційних витрат;

• уникнення посередників між виробниками та споживачами;

• забезпечення прозорості та незмінності умов договорів.

Приклад: у Німеччині та Австралії діють пілотні проекти, де споживачі укладають угоди на постачання електроенергії через блокчейн-платформи, що гарантує чесність і швидкість транзакцій [2].

1.2. Децентралізовані ринки електроенергії

Блокчейн дозволяє створювати peer-to-peer моделі торгівлі енергією, де кожен учасник може бути одночасно виробником і споживачем.

• Це зменшує залежність від великих енергетичних компаній.

• Забезпечує гнучкість і конкурентність ринку.

• Дозволяє інтегрувати відновлювані джерела енергії у локальні системи.

Приклад: проект Power Ledger у Німеччині та Австралії дає можливість мешканцям обмінюватися надлишковою енергією з сонячних панелей напряму через блокчейн [2].

1.3. Токенізація енергії

Енергія може виступати у вигляді цифрових токенів, що спрощує її облік та торгівлю.

• Токени відображають певну кількість виробленої або спожитої енергії.

• Вони можуть бути використані для внутрішніх розрахунків у мікромережах.

• Це створює нові фінансові інструменти для інвесторів та споживачів.

Приклад: у США та ЄС розробляються моделі, де токенізована енергія використовується для торгівлі на локальних ринках [1].

1.4. Управління мікромережами (microgrids)

Мікромережі — це локальні енергетичні системи, які можуть працювати автономно або бути інтегрованими у загальну мережу.

• Блокчейн забезпечує прозорий облік виробленої та спожитої енергії.

• Дозволяє оптимізувати баланс між виробниками та споживачами.

• Підвищує стійкість системи до збоїв та атак.

Приклад: у США блокчейн використовується для управління мікромережами у містах, що активно застосовують сонячну енергію [3].

1.5. Сертифікація «зеленої» енергії

Блокчейн дозволяє створювати прозорі системи сертифікації відновлюваної енергії.

• Кожна одиниця виробленої енергії може бути підтверджена у блокчейні.

• Це забезпечує довіру споживачів та інвесторів.

• Сприяє розвитку «зеленої» економіки.

Приклад: Європейський Союз активно впроваджує блокчейн для сертифікації відновлюваної енергії, що підвищує її конкурентоспроможність на ринку [1].

2. Інноваційні рішення та перспективи розвитку

2.1. Інтеграція блокчейну з відновлюваними джерелами енергії

• Прозорий облік виробленої енергії. Блокчейн дозволяє фіксувати кожну одиницю виробленої енергії у децентралізованому реєстрі.

• Сертифікація «зеленої» енергії. Кожен кіловат може бути підтверджений як «чистий», що підвищує довіру споживачів та інвесторів.

• Приклад: ЄС активно впроваджує блокчейн для підтвердження походження енергії з сонячних та вітрових електростанцій [1].

2.2. Токенізація енергетичних ресурсів

• Енергія як цифровий актив. Токенізація дозволяє перетворювати енергію на цифрові токени, які можна купувати, продавати або обмінювати.

• Фінансові інновації. Токени можуть використовуватися як інвестиційний інструмент, що відкриває нові можливості для фінансових ринків.

• Приклад: у США розробляються моделі, де токенізована енергія використовується для торгівлі на локальних ринках [2].

2.3. Розвиток мікромереж (microgrids)

• Автономність локальних систем. Мікромережі дозволяють громадам виробляти та споживати власну енергію.

• Оптимізація балансу. Блокчейн забезпечує прозорий облік виробництва та споживання, що знижує втрати.

• Стійкість до криз. Мікромережі можуть працювати автономно у випадку збоїв у центральній системі.

• Приклад: у Нью-Йорку діють пілотні проекти з управління мікромережами на основі блокчейну [3].

2.4. Інтелектуальні енергетичні системи (Smart Grids)

• Інтеграція ШІ та блокчейну. Поєднання технологій дозволяє прогнозувати споживання та оптимізувати розподіл енергії.

• Автоматизоване управління. Смарт-контракти можуть регулювати тарифи залежно від часу доби та навантаження.

• Приклад: у Японії блокчейн інтегрується у smart grids для оптимізації розподілу електроенергії [1].

2.5. Енергетичні платформи для споживачів

• Peer-to-peer торгівля. Споживачі можуть напряму продавати надлишкову енергію сусідам.

• Мобільні додатки. Платформи дозволяють керувати енергоспоживанням у режимі реального часу.

• Приклад: австралійська компанія Power Ledger створила платформу для обміну енергією між домогосподарствами [2].

2.6. Перспективи розвитку

• Глобальна децентралізація. Ринки електроенергії поступово переходять до децентралізованих моделей.

• Інтеграція з «зеленою» економікою. Блокчейн стає ключовим інструментом для розвитку відновлюваних джерел.

• Український контекст. Україна має потенціал для впровадження блокчейн-рішень у сфері сонячної та вітрової енергетики, але потребує інвестицій та нормативної підтримки [3].

3. Проблеми та виклики впровадження блокчейну в енергетиці

3.1. Технічні бар'єри

• Висока вартість впровадження. Реалізація блокчейн-рішень потребує значних інвестицій у програмне забезпечення, обладнання та інфраструктуру.

• Масштабованість систем. Блокчейн-платформи стикаються з проблемою обробки великої кількості транзакцій у реальному часі, що критично для енергетики.

• Інтеграція з існуючими системами. Традиційні енергетичні мережі часто не сумісні з новими цифровими платформами, що ускладнює їх модернізацію [1].

3.2. Кадрові проблеми

• Дефіцит спеціалістів. Недостатня кількість фахівців у сфері блокчейн, кібербезпеки та енергетики.

• Необхідність перепідготовки персоналу. Працівники енергетичних компаній потребують нових компетенцій для роботи з цифровими технологіями.

• Опір змінам. Частина менеджерів та персоналу не готова до впровадження інновацій через страх втрати роботи або складність адаптації [2].

3.3. Кіберзагрози та безпека

• Атаки на смарт-контракти. Уразливості в коді можуть призвести до фінансових втрат та порушення роботи систем.

• Загроза критичній інфраструктурі. Енергетичні системи є одними з найбільш вразливих до кібератак, що може мати катастрофічні наслідки.

• Приклад: у 2021 році було зафіксовано кілька атак на блокчейн-проекти у сфері енергетики, що призвело до втрати інвестицій [3].

3.4. Правові та регуляторні виклики

• Відсутність законодавчої бази. У багатьох країнах немає чітких правил щодо використання блокчейну в енергетиці.

• Міжнародна стандартизація. Різні країни застосовують різні підходи, що ускладнює інтеграцію ринків.

• Етичні питання. Використання блокчейну потребує вирішення проблеми прозорості алгоритмів та захисту персональних даних [1].

3.5. Організаційні виклики

• Зміна управлінських моделей. Перехід від централізованих систем до децентралізованих потребує нових стратегій управління.

• Формування культури інновацій. Не всі компанії готові до впровадження інноваційних практик.

• Управління ризиками. Нові технології створюють нові типи ризиків, які потребують комплексного аналізу та контролю [2].

4. Глобальні тенденції розвитку

4.1. Європейський Союз

• Сертифікація «зеленої» енергії. ЄС активно впроваджує блокчейн для підтвердження походження електроенергії з відновлюваних джерел. Це забезпечує прозорість та довіру споживачів.

• Децентралізовані ринки. У країнах ЄС розробляються моделі peer-to-peer торгівлі енергією, що дозволяють громадянам напряму купувати та продавати електроенергію.

• Приклад: у Німеччині та Франції діють пілотні проекти з використання блокчейну для управління локальними енергетичними системами [1].

4.2. США

• Мікромережі та smart grids. У США блокчейн інтегрується у системи управління мікромережами, що підвищує їхню автономність та стійкість.

• Інноваційні платформи. Американські компанії активно розробляють блокчейн-рішення для оптимізації розподілу енергії та зниження витрат.

• Приклад: у Нью-Йорку та Каліфорнії діють пілотні проекти з використання блокчейну для управління сонячними електростанціями [2].

4.3. Китай

• Масштабні інвестиції. Китай активно інвестує у блокчейн-проекти для енергетики, інтегруючи їх у державну політику.

• Інтеграція з «зеленою» економікою. Блокчейн використовується для контролю за виробництвом та споживанням відновлюваної енергії.

• Приклад: у Шанхаї створено блокчейн-платформи для управління енергетичними ресурсами на рівні мегаполісу [3].

4.4. Україна

• Потенціал розвитку. Україна має значні можливості для впровадження блокчейн-рішень у сфері сонячної та вітрової енергетики.

• Державні ініціативи. Міністерство енергетики України розглядає можливість використання блокчейну для сертифікації «зеленої» енергії та управління локальними ринками.

• Виклики. Основними проблемами залишаються недостатня інфраструктура, брак інвестицій та відсутність законодавчої бази.

4.5. Загальні тенденції

• Глобальна децентралізація. Ринки електроенергії поступово переходять від централізованих моделей до децентралізованих peer-to-peer систем.

• Інтеграція блокчейну з відновлюваними джерелами. Це стає стандартом для країн, що прагнуть до «зеленої» економіки.

• Поєднання блокчейну та штучного інтелекту. Використання ШІ для прогнозування споживання та оптимізації розподілу енергії у поєднанні з блокчейном формує нову парадигму управління.

• Міжнародна стандартизація. Зростає потреба у створенні єдиних стандартів для використання блокчейну в енергетиці, що забезпечить інтеграцію ринків.

Висновки

1. Блокчейн як стратегічний інструмент трансформації енергетики.

Технологія блокчейн довела свою ефективність у забезпеченні прозорості, безпеки та децентралізації енергетичних процесів. Вона дозволяє автоматизувати угоди, створювати децентралізовані ринки електроенергії та інтегрувати відновлювані джерела у глобальні енергетичні системи [1].

2. Існуючі рішення вже формують нову парадигму.

Смарт-контракти, токенізація енергії, управління мікромережами та сертифікація «зеленої» енергії — це не лише експериментальні моделі, а реальні практики, які застосовуються у ЄС, США, Китаї та інших країнах. Вони створюють основу для переходу від централізованих до децентралізованих ринків [2].

3. Інноваційні підходи відкривають перспективи сталого розвитку.

Інтеграція блокчейну з відновлюваними джерелами, розвиток smart grids та використання штучного інтелекту у поєднанні з блокчейном формують нову модель енергетики, орієнтовану на ефективність, екологічність та адаптивність [3].

4. Проблеми та виклики залишаються значними.

Технічні бар'єри (масштабованість, інтеграція, вартість), кадровий дефіцит, кіберзагрози та відсутність чіткої законодавчої бази є ключовими факторами, що стримують широке впровадження блокчейну в енергетиці. Їх подолання потребує комплексного підходу, який включає інвестиції, освітні програми та міжнародну координацію [1].

5. Глобальні тенденції визначають напрям розвитку.

ЄС, США та Китай демонструють різні моделі впровадження блокчейну в енергетиці, але всі вони спрямовані на децентралізацію, прозорість та інтеграцію «зеленої» енергії. Україна має можливість використати цей досвід, адаптувати його до власних умов та стати частиною міжнародного енергетичного простору [2].

6. Рекомендації для України.

• Розробити законодавчу базу для використання блокчейну в енергетиці.

• Стимулювати інвестиції у цифрову інфраструктуру та відновлювані джерела.

• Запровадити освітні програми для підготовки фахівців у сфері блокчейн та енергетики.

• Розвивати пілотні проекти з токенізації енергії та управління мікромережами.

• Забезпечити кіберзахист критичної інфраструктури.

Таким чином, блокчейн-технології стають не лише інструментом оптимізації енергетичних процесів, а й фундаментом для формування нової моделі енергетики, де ключовими принципами є прозорість, децентралізація, інноваційність та сталий розвиток.

1. Andoni, M., Robu, V., Flynn, D., et al. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. Renewable and Sustainable Energy Reviews, 2019.

2. Power Ledger. Decentralized Energy Trading Solutions. Official Reports, 2022.

3. Міністерство енергетики України. Інноваційні технології в енергетиці: перспективи блокчейн-рішень. Київ, 2023.

П.С. Чернишов, М.М. Ковальов, П.К. Нестеров

ТОКЕНІЗОВАНИЙ ОБІГ СКЛЯНОЇ ТАРИ ІЗ ЗАСТОСУВАННЯМ БЛОКЧЕЙН ТЕХНОЛОГІЙ ЯК ІНСТРУМЕНТ СТАЛОГО РОЗВИТКУ ЕНЕРГЕТИКИ

Актуальність теми. Виробництво нової скляної тари є одним з найбільш енергоємних процесів у пакувальній галузі: температура плавлення сировини становить 1400–1600 °C, та разом з тим тара має короткий термін застосування. Зниження енергоспоживання вирішується повторним використанням скляної тари і забезпеченням її повторного обігу. За даними Life-cycle assessment (ZWE, FEVE, EPA), кожна тонна нової скляної тари генерує приблизно на 670 кг CO_2 більше, ніж повторне використання вже існуючої тари [1, 2]. Кожне повторне використання скляної пляшки або банки економить 30–40 % енергії. При 25 і більше циклах загальна економія енергії сягає до 85 % порівняно з одноразовою тарою.

Однак традиційна система обігу тари неефективна, а саме відсутність прозорості та мотивації призводить до низького рівня повернення; непередбачувані логістичні затримки змушують виробників постійно випускати нову тару, що збільшує енергоспоживання та викиди CO_2; класичні депозитні системи складні та дорогі в адмініструванні.

Базові терміни.

Блокчейн = інструмент організації процесу в енергетиці.

Токен = носій енергетичної вартості.

Тара = фізичний об’єкт обліку енергії

Мета та завдання дослідження. Створення децентралізованої блокчейн-системи QR-токенізованого обігу скляної тари [3]. Це дозволить суттєво знизити енергоспоживання, зменшити викиди CO_2, забезпечити прозорість і стимулювати споживачів без використання депозитної системи.

Постановка проблеми (енергетичний фокус).

- Скляна тара → енергоємне виробництво (до 1600°C).
- Втрата циклів обігу = втрата енергії.
- Відсутність контролю обігу → неконтрольоване виробництво нової тари.
- Проблема енергетики: енергія не прив’язана до життєвого циклу продукту.

Гіпотеза. Якщо кожну одиницю тари зробити цифровим активом, тоді:

- кожен цикл = зафіксована енергія;
- кожне повернення = підтверджена економія;
- кожна операція = запис у блокчейні.

Отже є можливість забезпечити обіг тари децентралізованою системою обліку енергії із використанням одиниці вимірювання "токен".

Блокчейн як інфраструктура процесу. RamosesX реалізує:

- смарт-контракт = логіка обігу;

- QR-код = ідентифікатор активу;
- токен = одиниця обігу;
- блокчейн = незмінний журнал циклів.

Кожна дія містить: → купівля→ повернення→ переробка= транзакція в системі. Життєвий цикл складає 25+ циклів:

- виробництво → створення QR-активу;
- купівля → активація (50% токенів);
- повернення → завершення циклу (50%);
- повторне використання;
- завершення → переробка + бонус (адресне повернення тари споживачеві, причому споживач матиме можливість залишити повідомлення або іншу інформацію для наступного споживача).

Собівартість токена $C_{токена}$ як носія енергії складається з базової компоненти + еквівалента заощадженої енергії на нову тару:

$$C_{токена} = C_{базова} + \frac{E_{заощаджена} + S_{сировина} + V_{інші\ витрати}}{N}, \quad (1)$$

де $C_{базова}$ - базова вартість; $E_{заощаджена}$ - енергія зекономлена завдяки повторному використанню тари; $S_{сировина}$ - заощаджена сировина; $V_{інші\ витрати}$ - інші зекономлені витрати; N - кількість активних токенів.

Рисунок 1 – Зразок оцифрованої тари

Ідея полягає в тому, що токен не є спекулятивним - він прив'язаний до заощадженої енергії, зменшеного CO_2 та збереженої сировини. Кількісний ефект при 25+ циклах:

- енергія: –28%;

- CO_2: –35%;
- нове виробництво: суттєво зменшується;
- стабільність обігу: +83%.

Ключовим є те, що економія стає вимірюваною і підтвердженою.

Висновок. Створення децентралізованої блокчейн-системи QR-токенізованого обігу скляної тари дозволяє перевести енергію в облік, облік - в токен, токен - в економіку. Головний результат: фізичний об'єкт інтегрується в цифрову економіку, керований обіг = керована енергія. Робота виконана в рамках розробки концепції "ЄCity" [4-7].

1. FEVE (European Container Glass Federation) (2016). Why glass always has a happy CO_2 ending. LCA study by PE International. https://feve.org/wp-content/uploads/2016/04/FEVE-brochure-Recycling-Why-glass-always-has-a-happy-CO2-ending-.pdf

2. Zero Waste Europe & ReLoop Platform (2020). Reusable vs Single-Use Packaging: A Review of Environmental Impacts. University of Utrecht. https://zerowasteeurope.eu/wp-content/uploads/2020/12/zwe_reloop_report_reusable-vs-single-use-packaging-a-review-of-environmental-impact_en.pdf

3. Чернишов П.С. Система цифрового маркування та токенізованого обігу тари. Свідоцтво №142340 про реєстрацію авторського права на твір, дата реєстрації 11 лютого 2026 р.

4. Чернишов П.С. ECity - опис проекту. Цифрові послуги інфраструктури та/або їх оплати. Свідоцтво №119571 про реєстрацію авторського права на твір, дата реєстрації 5 червня 2023 р., опубл. 31.07.2023, бюллетень №76

5. Чернишов П.С. Концепція послуги IT бронювання паркомісць, цифрова безпека пішоходів, онлайн-туризм "ЄCity" ("ЄCity"). Свідоцтво №130840 про реєстрацію авторського права на твір, дата реєстрації 22 жовтня 2024 р., опубл. 29.11.2024, бюллетень №84

6. Концепція впровадження IT рішень у проєкті "ЄCity". https://ramosesx.com/

7. Чернишов П.С., Ковальов М.М. Єcity: блокчейн-архітектура як основа децентралізованого управління енергоспоживанням та мобільністю у смартмістах / П.С. Чернишов, М.М. Ковальов // Використання блокчейн технологій в енергетиці – 2025 : збірник матеріалів науково-практичної конференції (Київ, 26 березня 2025 р.) - Київ: Інститут проблем моделювання в енергетиці імені Г.Є. Пухова НАН України. - 2025. - с.45-46. https://ipme.kiev.ua/konferencii/naukovo-praktichna-konferenciya-bte-2025/

O.O. Haisha, V.Y. Kandala

ANALYSIS OF PATHWAYS LEADING TO ERRONEOUS DECISIONS BY MODERN NEURAL NETWORKS IN IMAGE RECOGNITION

Contemporary neural networks occupy a pivotal position in the domain of image recognition, being extensively employed in fields such as medicine, autonomous transportation systems, security, and other areas of artificial intelligence. In particular, neural network technologies are increasingly implemented for authentication purposes, including within access control systems for critical infrastructure components. Despite substantial advancements in their development, these systems continue to exhibit susceptibility to specific categories of errors, which may ultimately result in serious consequences. Accordingly, the investigation of mechanisms that give rise to incorrect decisions is of paramount importance for enhancing the reliability and efficiency of artificial neural networks.

A consideration of the principal factors contributing to the emergence of errors in modern neural networks reveals several key causes underlying inaccuracies in image recognition:

a) adversarial attacks, the essence of which lies in the fact that minor yet deliberately engineered perturbations of image pixels can induce a neural network to misclassify an object. Such attacks exploit inherent vulnerabilities of deep architectures and demonstrate that these systems do not always rely on essential object features, instead depending on subtle patterns within input data;

b) variations in lighting conditions and viewing angles, to which neural networks often lack sufficient robustness, as well as sensitivity to environmental changes, including scale (distance to the object), rotation, and perspective distortions. These factors can significantly degrade recognition accuracy, particularly in real-world deployment scenarios;

c) insufficiency of representative data, whereby a training dataset lacking adequate samples of a given class or insufficient diversity of object variations leads to diminished performance on real-world inputs. This issue is especially pronounced in medical imaging, where the availability of anomalous cases for training is inherently limited;

d) generalization errors, manifested in the tendency of deep neural networks to rely excessively on specific patterns or textures rather than on the structural or geometric properties of objects. This may result in incorrect classifications driven by spurious correlations present in the training data;

e) architectural characteristics of neural networks, as certain architectures, particularly highly deep models, are prone to issues such as “dead neurons” or the vanishing gradient problem. These phenomena can cause instability during training and lead to unpredictable errors during classification.

Examples of neural networks that are actively employed for image recognition and may exhibit the aforementioned errors include the following:

- AlexNet – one of the earliest deep neural network architectures for image classification, which demonstrated high performance in the ImageNet Challenge. However, it remains susceptible to adversarial attacks and variations in illumination conditions;

- VGGNet (VGG16, VGG19) – robust architectures designed for image classification tasks, yet due to their considerable depth, they suffer from the vanishing gradient problem, which may lead to errors during the training process;

- Inception (GoogLeNet, InceptionV3) – an efficient model for recognizing complex visual patterns, although its architectural complexity renders it sensitive to variations in viewpoint and lighting conditions;

- EfficientNet – one of the most advanced architectures that achieves a balance between efficiency and accuracy, yet it can still be vulnerable to adversarial perturbations;

- YOLO (You Only Look Once) – a widely used neural network for real-time image processing, frequently applied in autonomous systems, but it may encounter difficulties in object detection under challenging environmental conditions.

To mitigate the aforementioned challenges, several approaches may be implemented to reduce the likelihood of errors in neural network-based image recognition processes:

- expansion and balancing of training datasets, as increasing diversity within training images enhances the model’s capacity for generalization;

- application of adversarial defense techniques, including the incorporation of deliberately modified images during training to improve robustness against attacks;

- integration of interpretability mechanisms, particularly feature visualization methods such as Grad-CAM, which facilitate analysis of the regions and attributes the network prioritizes during classification;

- optimization of model architecture, for instance through the use of residual blocks (ResNet) or data normalization techniques, which can alleviate gradient-related issues and improve classification accuracy.

Thus, notwithstanding the considerable progress achieved in the field of neural networks, the issue of erroneous decision-making remains highly relevant, including in object recognition systems employed for the protection of critical infrastructure. A thorough examination of error-inducing mechanisms enables the development of more resilient and reliable models, which is especially crucial for safety-critical applications. Future research in this domain should be directed toward enhancing model interpretability and reducing sensitivity to external perturbations.

1. Redmon, J., & Farhadi, A. (2016). YOLO9000: Better, faster, stronger. arXiv. https://arxiv.org/abs/1612.08242

2. Tan, M., & Le, Q. V. (2019). EfficientNet: Rethinking model scaling for convolutional neural networks. arXiv. https://arxiv.org/abs/1905.11946

Х.І. Дрогобицька

СМАРТ-КОНТРАКТИ ЯК ФОРМА УКЛАДЕННЯ ЕНЕРГЕТИЧНИХ ДОГОВОРІВ: ЮРИДИЧНА ПРИРОДА ТА ПРОБЛЕМИ ПРАВОЗАСТОСУВАННЯ

Сучасний етап розвитку цифрової економіки характеризується активним впровадженням інноваційних технологій у різні сфери суспільних відносин, зокрема у сферу енергетики. Одним із найбільш перспективних інструментів цифровізації є смарт-контракти, які функціонують на основі технології блокчейн і забезпечують автоматичне виконання договірних зобов'язань без залучення посередників. Актуальність дослідження зумовлена необхідністю підвищення ефективності правового регулювання енергетичних відносин, а також потребою адаптації національного законодавства до сучасних цифрових викликів.

Смарт-контракт у загальному розумінні являє собою програмний код, який містить умови договору та автоматично забезпечує їх виконання за настання визначених обставин. Його специфіка полягає у самовиконуваності, незмінності після розміщення в системі блокчейн та відсутності потреби у сторонньому контролі за виконанням. У науковій доктрині сформувалися різні підходи до визначення юридичної природи смарт-контрактів [1]. З одного боку, вони розглядаються як виключно технічний інструмент, що не має самостійного правового значення, а з іншого - як різновид цивільно-правового договору. Найбільш обґрунтованим є комплексний підхід, відповідно до якого смарт-контракт поєднує у собі правову та технологічну складові.

Відповідно до статті 626 Цивільного кодексу України договором є домовленість двох або більше сторін, спрямована на встановлення, зміну або припинення цивільних прав та обов'язків. Смарт-контракт відповідає цим ознакам, оскільки передбачає погодження волі сторін, визначає їх права та обов'язки і спрямований на досягнення конкретного правового результату. З огляду на це, він може розглядатися як форма електронного договору. Такий висновок узгоджується з положеннями статті 207 Цивільного кодексу України, яка допускає укладення правочинів у письмовій формі, у тому числі з використанням електронних засобів [2]. Додаткове нормативне підґрунтя становлять Закон України «Про електронні документи та електронний документообіг» та Закон України «Про електронні довірчі послуги», які визначають правовий режим електронних правочинів та порядок ідентифікації їх учасників.

Застосування смарт-контрактів у сфері енергетики відкриває нові можливості для трансформації ринку електроенергії. Вони можуть використовуватися для автоматичного виконання договорів купівлі-продажу електричної енергії, здійснення розрахунків між учасниками ринку, управління балансуванням енергосистеми, а також для реалізації моделей

децентралізованої торгівлі електроенергією. Особливого значення набуває їх використання у відносинах між малими виробниками електроенергії та споживачами, що відповідає сучасним тенденціям розвитку «розумних мереж». Використання смарт-контрактів сприяє зниженню транзакційних витрат, підвищенню прозорості операцій та мінімізації впливу людського фактора.

Разом з тим, впровадження смарт-контрактів супроводжується низкою суттєвих проблем правозастосування. Насамперед слід зазначити відсутність спеціального законодавчого регулювання, яке б визначало поняття смарт-контракту, його правовий статус та особливості застосування. Це зумовлює необхідність застосування загальних норм цивільного права за аналогією, що не завжди забезпечує належний рівень правової визначеності. Важливою проблемою є також ідентифікація сторін, оскільки у блокчейн-системах вони можуть виступати у вигляді анонімних цифрових адрес, що ускладнює встановлення їх правового статусу та суперечить вимогам законодавства щодо ідентифікації учасників правочинів.

Окрему увагу слід приділити обмеженим можливостям смарт-контрактів щодо врахування оціночних категорій, таких як добросовісність, розумність та справедливість. Зазначені категорії є фундаментальними для цивільного права, однак вони не можуть бути повною мірою відтворені у програмному коді. Це обмежує сферу застосування смарт-контрактів і вимагає їх поєднання з традиційними формами договірного регулювання. Крім того, виникають складнощі у визначенні відповідальності у разі помилок у коді або неналежного виконання смарт-контракту. За відсутності спеціального регулювання такі питання вирішуються на підставі загальних положень про відповідальність за порушення зобов’язань, закріплених у статтях 610–625 Цивільного кодексу України.

Суттєвим викликом є також використання так званих «оракулів», які забезпечують надходження зовнішніх даних для функціонування смарт-контрактів. Від достовірності таких даних залежить правильність виконання договору, що зумовлює необхідність визначення правового статусу постачальників інформації та їх відповідальності [3]. Не менш важливими є юрисдикційні проблеми, пов’язані з транснаціональним характером блокчейн-технологій, що ускладнює визначення застосовного права, підсудності спорів та виконання судових рішень.

У зв’язку з цим актуальним є вдосконалення правового регулювання смарт-контрактів в Україні. Доцільним видається нормативне закріплення їх поняття та правового статусу, визначення програмного коду як форми вираження умов договору, а також забезпечення інтеграції смарт-контрактів із системами електронної ідентифікації. Перспективним напрямом є використання гібридних моделей, які поєднують традиційний текстовий договір із програмним кодом, що дозволяє врахувати як юридичні, так і технічні аспекти правовідносин. Важливим є також врахування міжнародного досвіду та гармонізація національного законодавства з правом Європейського Союзу у сфері цифрових технологій.

Отже, смарт-контракти є інноваційною формою укладення договорів, яка має значний потенціал для розвитку енергетичного сектору. Вони забезпечують автоматизацію виконання зобов'язань, підвищення прозорості та ефективності правовідносин. Водночас їх впровадження потребує належного нормативного забезпечення та вирішення низки правових проблем. У сучасних умовах доцільним є розгляд смарт-контрактів як різновиду електронних договорів, що функціонують у межах чинного цивільного законодавства, однак потребують подальшої правової деталізації та адаптації до специфіки цифрового середовища.

1. Що таке смарт-контракт та який принцип його роботи | АО "Бачинський та партнери". *АО "Бачинський та партнери"*. URL: https://legalaid.ua/ua/shho-take-smart-kontrakty-i-yaki-prynczypy-yih-roboty/ (дата звернення: 17.03.2026).

2. Цивільний кодекс України : Кодекс України від 16.01.2003 № 435-IV : станом на 1 лют. 2026 р. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text (дата звернення: 17.03.2026).

3. Що таке блокчейн-оракули: підключення смарт-контрактів до реальних даних. *Medium*. URL: https://surl.li/pbbvwt (дата звернення: 17.03.2026).

В.Ю. Зубок

ФОРМУВАННЯ ВИМОГ ДО ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ ВЗАЄМОДІЇ УЧАСНИКІВ ДЕЦЕНТРАЛІЗОВАНОГО РИНКУ ЕЛЕКТРОЕНЕРГІЇ

Вступ. Серед основних принципів, що закладаються в концепцію нової децентралізованої енергетичної системи, є децентралізація та цифрова трансформація [1].

Децентралізація - це процес перерозподілу частини централізованого управління (технологічного, організаційного та ринкового) та розвитку розподіленої генерації із використанням ВДЕ, з метою забезпечення електроенергією споживачів, в першу чергу, підприємствам об'єктам критичної інфраструктури, від роботи яких залежить життєдіяльність громад. Вона дозволяє створювати нові можливості децентралізованої торгівлі електричної енергії між виробниками та споживачами (P2P), а також посилення гнучкості регіональної (локальної) енергосистеми, у тому числі в умовах мілітарних загроз.

Актуальна проблема підвищення ефективності, зменшення втрат в розподільчих мережах та забезпечення стійкості регіональної (локальної) енергетичної системи потребує цифрової трансформації [1], а саме - впровадження цифрових технологій (Smart Grid, Micro Grid, смарт-контракти, штучний інтелект, блокчейн, тощо) для оптимізації процесів у сфері виробництва, розподілу, споживання та управління енергетичними ресурсами на регіональному рівні. Проблематика предметної області включає дослідження розвитку децентралізованих ринків та P2P-контрактів [2], проблеми безконфліктного обробляння даних в розгалужених системах [3], можливості та безпечності використання блокчейн-технологій [4]. Шляхи вирішення проблеми потребують

Методологія. Діаграма на рис. 1 демонструє структуру взаємодії учасників децентралізованого ринку електроенергії.

Обчислювальна система для обробки смартконтрактів у децентралізованій енергетичній мережі має забезпечувати високу продуктивність, низьку затримку, безпечне виконання та масштабованість, а також інтеграцію з енергетичною інфраструктурою та механізми резервування. Це особливо важливо в умовах, коли система повинна функціонувати безперервно навіть під час збоїв зв'язку чи зовнішніх атак. Сильні та слабкі сторони сучасних інфраструктурних рішень для розподілених масштабованих обчислювальних систем проаналізовано в [5]. Поєднання блокчейн- та хмарних технологій у реалізації смартконтрактів базується на комплексній архітектурі, де взаємодія обчислювальних нод, гнучке використання швидких і повільних сховищ, географічна розподіленість, інструменти оркестрації та динамічне масштабування забезпечують стійкість, масштабованість і високу доступність системи.

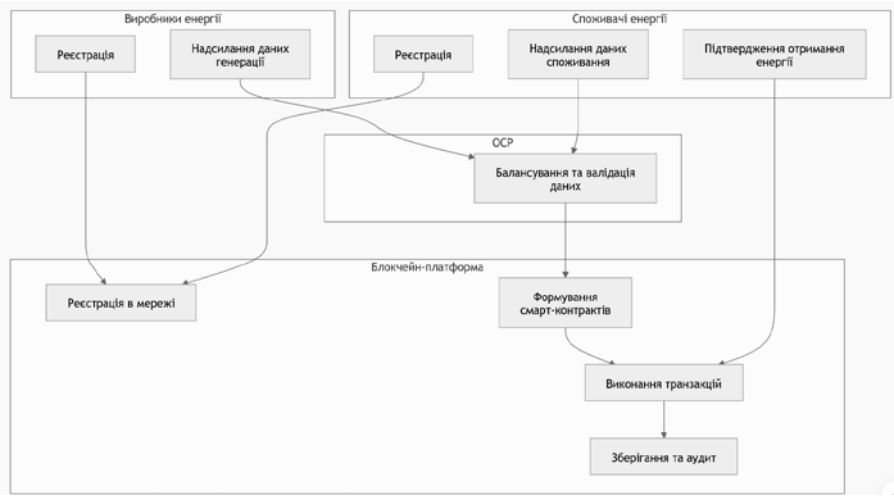

Рисунок 1 - Структура децентралізованого ринку електроенергії.

Обчислювальні ноди. Однією з ключових вимог є наявність розподіленої мережі обчислювальних вузлів, які можуть виконувати роль повних або легких нод. Повні вузли (full nodes) повинні зберігати повну копію блокчейну та брати участь у верифікації транзакцій і виконанні смарт-контрактів. Їх рекомендується розгортати на рівні fog- або cloud-інфраструктури. Легкі вузли (lightweight nodes) можуть функціонувати на периферії (так званий edge-рівень) — без зберігання повного ланцюга, з покладанням на довірені вузли для перевірки даних. Це дозволяє інтегрувати блокчейн з пристроями Smart Grid без надмірного навантаження. Кожна обчислювальна нода у блокчейн-мережі повинна мати достатню обчислювальну потужність для виконання алгоритмів консенсусу, перевірки транзакцій і запуску смартконтрактів у віртуальній машині (наприклад, EVM у Ethereum). При цьому у хмарі обчислювальні ноди можуть бути розміщені у різних регіонах для зменшення затримок у доступі та підвищення стійкості до відмов.

Залежно від обраної моделі блокчейну (публічної чи приватної), система має забезпечувати необхідну обчислювальну підтримку відповідного механізму консенсусу. У приватних або консорціумних мережах доцільно використовувати енергоефективні алгоритми — Proof-of-Authority (PoA), Practical Byzantine Fault Tolerance (PBFT), Raft тощо. Вони дозволяють досягати швидкої фіналізації транзакцій за мінімального обчислювального навантаження, що є важливим у контексті обмежених ресурсів на периферії.

Підсистема зберігання даних. Для ефективної роботи необхідно використовувати дві категорії сховищ. Перша категорія – «швидке сховище» (NVMe SSD, in-memory storage) — для зберігання так званих “data in motion”,

тобто активних даних, журналів транзакцій та тимчасових структур, які часто використовуються під час обробки смартконтрактів.

Друга категорія – «повільне сховище» (на HDD чи спеціальних архівних сховищах у хмарних провайдерів) для так званих “data in rest”, тобто зберігання історичних блоків, резервних копій та архівів.

Мережева інфраструктура. Наявність обчислювальних нод у різних географічних регіонах дозволяє мінімізувати затримки у виконанні транзакцій і забезпечити безперервну роботу у разі локальних відмов. Для цього необхідні низьколатентні канали зв’язку між регіонами та механізми балансування навантаження. Оскільки блокчейн є мережею з розподіленим консенсусом, критичною є наявність надійних каналів зв’язку з низькою затримкою між вузлами. Підтримка peer-to-peer з’єднань, захищених тунелів (VPN), протоколів QoS і шифрування трафіку є обов’язковими. У випадках використання fog-архітектури, необхідно передбачити можливість автономної роботи вузлів у разі втрати зв’язку з хмарою.

Вимоги до оркестрації ресурсів. Використання інструментів оркестрації (наприклад, Kubernetes, HashiCorp Nomad) дозволяє централізовано керувати життєвим циклом обчислювальних нод, автоматично розгортати нові екземпляри для виконання смартконтрактів та оптимізувати розподіл ресурсів.

Масштабованість. Оскільки навантаження на мережу блокчейну та обробку смартконтрактів може бути нерівномірним, обчислювальна інфраструктура повинна підтримувати автоматичне масштабування — як вертикальне (збільшення ресурсів ноди), так і горизонтальне (додавання нових нод у пул). Рекомендується використання механізмів шардінгу, sidechains або сегментування мережі на кластери за територіальним або функціональним принципом.

Інтеграція з інфраструктурою учасників ринку. Інформаційна архітектура має включати API-шлюзи для інтеграції з SCADA-системами, платформами моніторингу та IoT-пристроями. Підтримка протоколів MQTT та REST дозволяє забезпечити взаємодію блокчейн-системи з зовнішніми енергетичними компонентами, забезпечуючи автоматизацію обміну даними та запуску смарт-контрактів на основі фактичних показників споживання чи генерації.

Безпека та відповідність вимогам (комплаєнс). Обробка смартконтрактів у хмарному середовищі вимагає реалізації багаторівневого захисту, включаючи ізоляцію середовищ виконання, контроль доступу до швидкого і повільного сховищ, шифрування даних у транзиті та у стані спокою. Особливе місце займає питання *суверенності даних*, яке набуває стратегічного значення в умовах геополітичної нестабільності. Для національної енергетичної системи критично важливо, щоб дані зберігалися та оброблялися відповідно до норм національного законодавства, а контроль над інформаційною інфраструктурою залишався у юрисдикції держави. Суверенність даних визначає не тільки технічні вимоги, але й формує вимоги до вибору моделі розгортання — локальної, хмарної чи гібридної.

Використання іноземних хмарних сервісів, попри їхню високу технологічність, пов'язане з ризиками доступності та конфіденційності, а також можливими геополітичними ризиками, тоді як локальна інфраструктура забезпечує контроль, але вимагає значних ресурсів для масштабування та підтримки.

1. O. Sukhodolya "Principles of developing a new energy system of Ukraine", Articles for National Institute of Strategic Studies. Mediacenter. https://niss.gov.ua/sites/default/files/2026-01/principi-rozbudovi-energetiki-sayt.pdf

2. V. Evdokimov, A. Polukhin, D. Tsvilii, Y. Lukashevych & O. Havva "Decentralized Energy Markets and P2P Contracts: New Opportunities for Automating Energy Exchange", Grassroots Journal of Natural Resources, 8(2), 2025, pp. 856-884. https://doi.org/10.33002/nr2581.6853.080240

3. A. Prymushko, I. Puchko, M. Yaroshynskyi, D. Sinko, H. Kravtsov, & V. Artemchuk (2025). "Efficient State Synchronization in Distributed Electrical Grid Systems Using Conflict-Free Replicated Data Types". IoT, 6(1), 6. https://doi.org/10.3390/iot6010006

4. A. Vykhlo, & L. Kovalchuk "Estimation of the Probability of Success of a Suppression Attack". Theoretical and Applied Cybersecurity, 7(1), 2025, p. 65-70. https://doi.org/10.20535/tacs.2664-29132025.1.332340

5. В.В. Зубок, Р.С. Драгунцов, В.Ю. Зубок. Резильєнтність ERP-систем в умовах енергетичної кризи. Кібербезпека енергетики, науково-практична конференція Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України : матеріали, 29 травня 2024 р. Київ : ІПМЕ ім. Г.Є.Пухова. – с. 13-16.

М.С. Кондратенко

АНАЛІЗ АТАК НА СМАРТ-КОНТРАКТИ ТА МЕТОДИ ЗАБЕЗПЕЧЕННЯ ЇХ БЕЗПЕКИ

Вступ. Розвиток децентралізованих технологій, зокрема, блокчейну зумовив трансформацію традиційних підходів до виконання договірних зобов'язань. Слід зазначити, що блокчейн – це децентралізована база даних (P2P — "Peer-To-Peer"), в якій вся інформація розміщується на великій кількості вузлів, які можуть знаходитись у будь-якій точці світу, при чому, в такій топології головний сервер відсутній. Блокчейн використовує криптографічні алгоритми, в тому числі розумні контракти для забезпечення роботи всієї системи. [1] Тому на сьогодні смарт-контракти набувають значного поширення як ефективний та зручний інструмент автоматизації бізнес-процесів, фінансових транзакцій та управління цифровими активами. Згідно з дослідженнями, смарт-контракт визначається як програмний код, що функціонує в середовищі блокчейн і забезпечує автоматичне виконання умов договору при настанні визначених подій-тригерів [2]. Попри високий ступінь автономності та прозорості, впровадження смарт-контрактів супроводжується низкою технічних та юридичних викликів. Оскільки смарт-контракти існують у нерозривному взаємозв'язку з архітектурою блокчейну, питання їхньої безпеки регулюється не лише якістю коду, а й відповідними нормативно-правовими актами та стандартами безпеки [3].

Юридичний статус та математична природа смарт-контрактів. Аналіз юридичного статусу смарт-контрактів свідчить про складність їх адаптації до правового поля України. Основна проблема полягає у визначенні моменту укладання угоди та ідентифікації сторін у децентралізованих мережах [2]. Важливим аспектом є узгодження математичних алгоритмів, що лежать в основі коду, з юридичними нормами, які регулюють договірні відносини. Саме математична логіка контракту має гарантувати виконання правових намірів сторін, що вимагає глибокого аналізу математичних та юридичних аспектів при їх проектуванні [3].

Класифікація та аналіз кібер-атак на смарт-контракти. Вразливість смарт-контрактів обумовлена публічністю їхнього коду та незворотністю транзакцій у блокчейні. На відміну від традиційного програмного забезпечення, виявлена помилка в розгорнутому смарт-контракті часто не може бути виправлена без перенесення даних у новий контракт.

До основних типів атак належать:

1. **Reentrancy (Повторний вхід).** Ця атака виникає, коли зовнішній контракт здійснює виклик до вразливого контракту до того, як перший завершив виконання поточної операції (наприклад, оновлення балансу). *Історичний приклад:* Найвідомішим випадком є злам **The DAO у 2016 році**,

коли зловмисники викрали близько 3,6 млн ETH, що призвело до хардфорку мережі Ethereum. [4]

2. **Integer Overflow та Underflow (Переповнення цілих чисел).** Виникає, коли арифметична операція перевищує максимальне або мінімальне значення типу даних. У старих версіях мови Solidity (до 0.8.0) це дозволяло зловмисникам маніпулювати балансами токенів.

3. **Denial of Service (DoS).** Атаки, спрямовані на те, щоб зробити контракт непрацездатним. Це може бути реалізовано через перевищення ліміту газу (Gas Limit) або блокування функцій контракту шляхом навмисного виклику помилок у критичних циклах.

4. **Front-running.** Атака на рівні блокчейн-транзакцій, де зловмисник бачить транзакцію в мемпулі (черзі на обробку) і виставляє вищу комісію за газ для своєї транзакції, щоб вона була оброблена першою. Це часто використовується для маніпуляцій на децентралізованих біржах (DEX).

5. **Вразливості логіки доступу.** Помилки в модифікаторах функцій (наприклад, onlyOwner), які дозволяють неавторизованим користувачам отримувати контроль над адміністративними функціями. *Історичний приклад:* Злам гаманця **Parity Multi-sig (2017)**, де через помилку в коді бібліотеки було заблоковано понад 500 000 ETH [5].

Методи захисту та забезпечення безпеки. Забезпечення безпеки смарт-контрактів потребує комплексного підходу, що поєднує технічний аудит та дотримання міжнародних стандартів [3].

- **Аудит безпеки коду.** Проведення незалежного аналізу смарт-контракту спеціалізованими компаніями перед його розгортанням в основній мережі.
- **Формальна верифікація.** Математичний метод доведення коректності алгоритмів контракту відносно заданих специфікацій. Цей метод дозволяє переконатися, що код працює саме так, як було задумано юридично та технічно [3].
- **Використання перевірених бібліотек.** Застосування стандартів (наприклад, OpenZeppelin), що вже пройшли багаторазову перевірку спільнотою.
- **Bug Bounty програми.** Залучення "білих" хакерів для пошуку вразливостей за винагороду після розгортання контракту.
- **Механізми Circuit Breakers (Пауза).** Впровадження функцій, які дозволяють адміністратору тимчасово зупинити роботу контракту в разі виявлення аномальної активності.

Висновок

Смарт-контракти є потужним інструментом цифровізації економіки, проте їхнє використання несе значні ризики через потенційні кібер-атаки. Аналіз показав, що більшість критичних вразливостей виникає внаслідок помилок логіки у коді та невідповідності математичних моделей правовим

вимогам. Для мінімізації ризиків необхідно впроваджувати суворі стандарти аудиту, використовувати методи формальної верифікації та працювати над удосконаленням нормативно-правової бази, яка б чітко визначала статус смарт-контрактів в Україні. Тільки за умови синергії математичної точності та юридичної визначеності смарт-контракти зможуть стати надійним фундаментом для майбутньої цифрової інфраструктури.

1. Кондратенко, М. С. (2023). Використання технології блокчейну для побудови ієрархічної структури на множині державних реєстрів з метою захисту від підробки інформації. Theoretical And Applied Cybersecurity. Перша Всеукраїнська науково-практична конференція, присвячена 100-річному ювілею академіка В.М. Глушкова. Матеріали конференції, с.228–232.

2. Ковальчук, Л. В, Кондратенко, М.С. (2023). Аналіз юридичного статусу смарт-контрактів та проблем, які виникають при узгодженні їх з законодавством України. Міжнародна Науково-практична конференція живучість та резильєнтність – 2023. Матеріали конференції, с.18–20.

3. Кондратенко, М.С. (2023). Узгодження математичних та юридичних аспектів при використанні смартконтрактів. Наукові праці ДонНТУ Серія “Інформатика, кібернетика та обчислювальна техніка”, 2 (37), с.54–66. Нормативно-правові акти і стандарти в контексті безпеки смарт-контактів в Blockchain

4. DAO Hack Explained: How a Vulnerability Split Ethereum. Cryptopedia. Your trusted source for all things crypto. https://www.gemini.com/cryptopedia/the-dao-hack-makerdao

5. The Parity Wallet Hack Explained. Openzeppelin. https://www.openzeppelin.com/news/on-the-parity-wallet-multisig-hack-405a8c12e8f7

Н.В. Кучинська

ПОСТКВАНТОВА СТІЙКІСТЬ ДЕЦЕНТРАЛІЗОВАНИХ ЕНЕРГЕТИЧНИХ РИНКІВ: ЗАГРОЗИ ДЛЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН ТА СМАРТ-КОНТРАКТІВ

Актуальність та динаміка ринку децентралізованої енергетики. Децентралізовані енергетичні ринки проходять етап інтенсивного масштабування, перетворюючись із експериментальних моделей на фундамент сучасної енергосистеми. За прогнозними даними, світовий ринок блокчейну в енергетиці має продемонструвати стрімке зростання з приблизно 2 млрд доларів США у 2025 році до 170 млрд доларів США до 2035 року. [1] Географічно лідером залишатиметься Європа з часткою 30–34% завдяки високому регуляторному інтересу та підтримці інновацій, тоді як Північна Америка та Азіатсько-Тихоокеанський регіон сукупно займають понад 50% ринку через активне впровадження комерційних демо-мереж. Наразі близько 59% ринку контролюється п'ятьма провідними компаніями, серед яких Siemens, IBM, Accenture, Oracle та Power Ledger, що забезпечує технологічну стабільність галузі.

Практичне застосування цих технологій демонструють такі успішні кейси, як проєкт Brooklyn Microgrid (реалізований LO3 Energy спільно з Siemens), де мешканці Нью-Йорка використовують блокчейн для P2P-торгівлі надлишками сонячної енергії в межах одного району, а також платформа Power Ledger, що автоматизує розрахунки між прозюмерами в Австралії, Таїланді та Індії. Зростаюче впровадження стратегій токенізації дозволяє енергетичним компаніям, таким як Iberdrola, конвертувати фізичні активи відновлюваної енергетики в торгові цифрові одиниці, що відкриває нові канали фінансування та спрощує верифікацію походження енергії через «зелені» сертифікати. Автоматизація виконання угод про купівлю-продаж електроенергії через смарт-контракти суттєво зменшує адміністративне навантаження та усуває потенційні суперечки, що дозволяє знизити комісії за транзакції [2]. Це робить технологію привабливою для масштабного впровадження, проте водночас висуває жорсткі вимоги до криптографічної стійкості смарт-контрактів, які в умовах 2026 року повинні бути адаптовані до майбутніх квантових загроз для захисту активів.

Аналіз стійкості децентралізованих мереж та логіки смарт-контрактів у контексті розвитку квантових обчислювальних систем. Центральним елементом досліджень щодо криптографічних загроз у 2026 році є врахування дати наближення «Q-Day» — гіпотетичного моменту у майбутньому, коли квантові комп'ютери стануть достатньо потужними, щоб виконувати злам сучасних криптографічних алгоритмів. Згідно з планом NIST, а також суміжними директивами (зокрема Меморандумом Білого дому M-22-18[3] та Актом про квантову готовність[4]), повне завершення міграції має відбутись у 2030–2035 роках, за рекомендаціями BSI [5] - до 2030 року, що вже зумовило появу регуляторних мандатів США та ЄС щодо

обов’язкового переходу критичної інфраструктури на постквантові криптографічні стандарти (PQC) саме до цього терміну.

Оцінка часової деградації стійкості систем проводиться за методологією М. Моски [6], де критичною умовою безпеки є нерівність

$$X + Y > Z,$$

де параметр X визначає тривалість життєвого циклу даних тобто час, впродовж якого дані мають залишатися конфіденційними, Y — час, необхідний для повної міграції інфраструктури на нові постквантові алгоритми, а Z — прогнозований час до появи криптографічно релевантного квантового комп’ютера (CRQC). Оскільки життєвий цикл енергетичних об'єктів та контрактів іноді сягає 15–20 років, невиконання нерівності Моска вказує на те, що архітектура сучасних децентралізованих систем в енергоринку потребує невідкладного впровадження постквантових криптографічних алгоритмів, за потреби оновленого механізму консенсусу та передусім «криптографічної гнучкості» (crypto-agility) - здатності системи до оперативної заміни скомпрометованих алгоритмів без зупинки операційних процесів та втрати активів.

Основним вектором атаки, за умови появи криптографічно релевантного квантового комп’ютера, виступає алгоритм Шора, що робить вразливими криптографічні алгоритми, які ґрунтуються на задачі дискретного логарифмування. Це створює пряму загрозу для найбільш поширених у секторі енергетики платформ, зокрема Energy Web Chain, яка використовує алгоритми сімейства ECDSA для ідентифікації пристроїв, та мереж на базі Ethereum чи Hyperledger Besu, де підписи BLS та ECDSA є фундаментом консенсусу та безпеки смарт-контрактів. Водночас за появи CRQC та застосування алгоритму Гровера, який дозволяє вдвічі знизити бітову стійкість поширених симетричних блокових алгоритмів та хеш-функцій, зокрема таких як SHA-256 (використовується в Bitcoin та багатьох приватних децентралізованих системах енергомереж), виникає проблема впровадження та використання довших ключів для блокових алгоритмів шифрування та переходу на SHA-512 або AES-256.

Для децентралізованих енергоринків вказані криптографічні вразливості є релевантними також для смарт-контрактів. Серед найбільш небезпечних є сценарії «збирай зараз-дешифруй пізніше» (HNDL, Harvest Now, Decrypt Later) та «збирай зараз, підроблюй поізніше» (HNFL, Harvest Now, Forge Later). У рамках вказаних атак конфіденційні дані про умови довгострокових енергетичних контрактів можуть бути викрадені вже сьогодні з метою їх дешифрування (HNDL) або підробки (HNFL) в майбутньому. Крім того, поява CRQC відкриває шлях до підміни ідентичності в реальному часі (Real-Time Identity Spoofing), що дає змогу зловмиснику втручатися в транзакції безпосередньо в момент їх формування.

Критичну вразливість у структурі децентралізованих енергоринків демонструють смарт-контракти, що автоматизують розрахунки та виконання

прямих угод купівлі-продажу електроенергії (PPA). Поява криптографічно релевантного квантового комп'ютера загрожує не лише розкриттю приватних ключів гаманців та підробці цифрових підписів, а й загрожує логіці виконання смарт-контрактів. Оскільки термін дії таких контрактів може становити до 15–20 років, вони підпадають під пряму дію сценарію «HNDL». Використання в існуючих мережах (зокрема на базі Energy Web) протоколів конфіденційності zk-SNARKs створює ризик несанкціонованої модифікації архівних даних та умов постачання, що були зафіксовані на початку дії багаторічної угоди. Таким чином, архітектурна стійкість системи має базуватись на стійких постквантових криптографічних алгоритмах, здатних забезпечити незмінність логіки контракту протягом усього терміну його життєвого циклу.

Оцінювання криптографічної гнучкості. Проведений аналіз підтверджує, що децентралізована енергетика перебуває у зоні високого ризику. Енергетичний сектор потребує негайного переходу на PQC-стандарти [3,4], впровадження гібридних схем підпису та адаптації баз даних до значно більших розмірів параметрів постквантових алгоритмів. Оскільки процеси модернізації в криптографії та в енергетичній галузі, зокрема, є високоінертними, заходи із забезпечення стійкості системи мають реалізовуватися на поточному етапі проєктування мереж.

Також постає нагальна потреба у розробці комплексної методології оцінки стійкості блокчейн-інфраструктури до загроз від CRQC. Методологія оцінки криптографічної гнучкості повинна корелювати з рекомендаціями NIST SP 1800-38B [7], зокрема в частині створення специфікації криптографічних активів (CBOM, Cryptography Bill of Materials). Це дозволить здійснювати безперервний моніторинг вразливих вузлів енергосистеми та автоматизувати процес заміни алгоритмів відповідно до принципів «квантової готовності» (Quantum Readiness). Кількісні показники криптографічної гнучкості мають стати обов'язковим елементом технічного аудиту енергетичних платформ для визначення їхнього ресурсу безпеки та готовності до міграції.

Висновки та рекомендації. Забезпечення постквантової стійкості блокчейн в енергетичному секторі не може бути обмежене лише заміною алгоритмів; воно вимагає створення нових стандартів розробки смарт-контрактів із вбудованими механізмами оновлення криптографічного стеку. Формування методології оцінки «квантової готовності» є критичною умовою для мінімізації ризиків сценаріїв HNDL та HNFL у довгострокових угодах PPA. Розробка загального методу кількісної оцінки криптографічної гнучкості створить підґрунтя для забезпечення системної стійкості та прогнозованості ризиків децентралізованих енергетичних мереж.

1. WattCrop. (2025, February 24). Blockchain and the energy sector in 2025: From disruption to infrastructure and why we need to start paying attention. https://wattcrop.com/blockchain-and-the-energy-sector-in-2025-from-disruption-to-infrastructure-and-why-we-need-to-start-paying-attention/

2. Energy Web Foundation. (2025). *Energy Web Yellow Paper: A next-generation blockchain for the energy sector*. https://cdn.prod.website-files.com/65e5b22cf7f0480a007420fc/6931c85a28afe861c9b8b6a1_EnergyWeb_YellowPaper2025.pdf

3. The White House. (2022). *Memorandum M-22-18: Migrating to post-quantum cryptography*. Office of Management and Budget. https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-Memos-on-Migrating-to-Post-Quantum-Cryptography.pdf

4. Quantum Computing Cybersecurity Preparedness Act, H.R. 7535, 117th Cong. (2022). https://www.congress.gov/bill/117th-congress/house-bill/7535

5. Federal Office for Information Security (BSI). (2024). Status of Quantum Computer Development. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/Entwicklungstand_QC_V_2_1.pdf?__blob=publicationFile&v=3

6. Mosca, M. (2018). *Cybersecurity in an era with quantum computers: Will we be ready?* https://eprint.iacr.org/2015/1075

7. Barker, W., Polk, W. T., Rogas, M. J., & Souppaya, M. P. (2023). *Quantum readiness: Migration to post-quantum cryptography* (NIST Special Publication 1800-38B Preliminary Draft). National Institute of Standards and Technology. https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38b-preliminary-draft.pdf

О.Є. Максименко

МЕТОДИ КІБЕРЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ТРАНСФОРМАЦІЇ НОРМАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

Цифрова трансформація суспільства, розвиток інформаційно-телекомунікаційних технологій та зростання залежності ключових секторів економіки від інформаційних систем зумовлюють необхідність формування ефективної системи кіберзахисту держави. Особливої актуальності ця проблема набуває у контексті забезпечення стійкості об'єктів критичної інфраструктури, функціонування яких має визначальне значення для економічної стабільності, обороноздатності держави та безпеки населення.

У сучасних умовах кіберпростір став одним із ключових доменів ведення гібридної війни. Кібератаки можуть бути спрямовані на порушення функціонування енергетичних систем, фінансового сектору, транспортної інфраструктури, телекомунікаційних мереж та інших критично важливих об'єктів. Відповідно, формування ефективної системи кіберзахисту критичної інфраструктури є одним із пріоритетних завдань державної політики у сфері національної безпеки.

Водночас ефективне впровадження сучасних методів кіберзахисту неможливе без належного нормативно-правового забезпечення. Упродовж останніх років в Україні відбувається суттєва модернізація законодавства у сфері кібербезпеки, що створює передумови для впровадження нових організаційних та технічних підходів до забезпечення кіберстійкості критичної інфраструктури.

Критична інфраструктура держави охоплює системи, мережі та об'єкти, порушення функціонування яких може призвести до значних негативних наслідків для економіки, безпеки населення та національної безпеки. У сучасних умовах більшість таких об'єктів функціонує на основі складних інформаційно-комунікаційних систем та автоматизованих систем управління технологічними процесами.

Це зумовлює підвищену вразливість критичної інфраструктури до кіберзагроз, зокрема до атак на промислові системи управління (ICS/SCADA), інформаційні системи управління підприємствами, телекомунікаційні мережі та хмарні сервіси.

Разом з тим тривалий час нормативно-правове забезпечення кібербезпеки України не повною мірою відповідало сучасним викликам. Відсутність комплексного законодавчого регулювання обмежувала можливості впровадження сучасних підходів до кіберзахисту, зокрема системного управління кіберризиками, централізованого реагування на кіберінциденти, створення спеціалізованих підрозділів кібербезпеки та впровадження механізмів кіберстійкості.

Особливістю функціонування системи захисту критичної інфраструктури є те, що значна частина таких об'єктів перебуває у державній або комунальній власності. Відповідно діяльність органів державної влади у цій сфері повинна здійснюватися виключно у межах визначених законодавством повноважень.

Цей принцип закріплений у статті 19 Конституції України [1], відповідно до якої:

органи державної влади та органи місцевого самоврядування, їх посадові особи зобов'язані діяти лише на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами України.

Зазначене положення відображає фундаментальний принцип публічного права, який у правовій доктрині формулюється як правило: «органам державної влади дозволено лише те, що прямо передбачено законом». Саме тому впровадження нових методів кіберзахисту критичної інфраструктури потребує відповідного нормативно-правового закріплення.

Основу законодавства України у сфері кібербезпеки становить Закон України «Про основні засади забезпечення кібербезпеки України» №2163-VIII [2]. Важливим етапом розвитку нормативної бази стало внесення змін до цього закону у 2025 році, спрямованих на посилення захисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури.

Законодавчі зміни передбачали:

– уточнення термінологічного апарату у сфері кіберзахисту;

– посилення вимог до захисту державних інформаційних систем;

– запровадження обов'язкових процедур управління кіберризиками;

– визначення відповідальних посадових осіб за кібербезпеку;

– створення спеціалізованих підрозділів кіберзахисту.

Зазначені зміни також узгоджуються із положеннями Закону України «Про критичну інфраструктуру» №1882-IX [3], який визначає правові та організаційні засади функціонування національної системи захисту критичної інфраструктури.

Фактично розвиток законодавства створив правові передумови для впровадження сучасних механізмів кіберзахисту, які раніше було складно реалізувати у практичній діяльності органів державної влади через відсутність чітко визначених повноважень та процедур.

Сучасні підходи до кіберзахисту критичної інфраструктури передбачають комплексне застосування організаційних, технічних та управлінських методів [7].

Одним із ключових елементів забезпечення кібербезпеки є впровадження систем управління кіберризиками. Такий підхід передбачає систематичну ідентифікацію загроз, оцінку їх потенційного впливу на функціонування критичної інфраструктури та розроблення заходів щодо мінімізації ризиків.

Важливим елементом сучасних систем кіберзахисту є створення центрів моніторингу кібербезпеки та або реагування на комп'ютерні інциденти (Security Operations Center — SOC, Computer Security Incident Response Team – CSIRT), які забезпечують безперервний аналіз подій інформаційної безпеки та оперативне реагування на кіберінциденти.

Для об'єктів критичної інфраструктури особливе значення має відокремлення технологічних мереж від корпоративних та публічних інформаційних систем. Такий підхід дозволяє зменшити ризик поширення кіберзагроз на системи управління технологічними процесами.

Застосування сучасних криптографічних алгоритмів, та навіть прикладної криптографії у формі блок-чейну в енергетиці та інших критичних секторах, забезпечує захист інформації від несанкціонованого доступу (наприклад підміни даних сенсорів АЕС) та гарантує її цілісність і конфіденційність, забезпечуючи управління ідентифікацією та безпеки оновлень програмного забезпечення.

Ключовою характеристикою сучасних інформаційних систем є їх здатність зберігати функціональність навіть в умовах кіберінцидентів. Концепція кіберстійкості передбачає використання резервування, відмовостійких архітектур та механізмів швидкого відновлення систем [7,8].

Подальший розвиток законодавства України у сфері кібербезпеки буде тісно пов'язаний із процесами європейської інтеграції. У рамках імплементації права Європейського Союзу очікується адаптація національного законодавства до сучасних європейських нормативних актів у сфері кібербезпеки та захисту критичної інфраструктури.

Зокрема, йдеться про врахування положень:

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities (CER Directive) — Директиви щодо стійкості критичних суб'єктів [4];

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive) — Директиви про заходи для забезпечення високого спільного рівня кібербезпеки в Європейському Союзі [5];

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (Digital Operational Resilience Act — DORA) — Регламенту про цифрову операційну стійкість фінансового сектору [6].

Імплементація положень цих нормативних актів у національне законодавство сприятиме подальшому розвитку системи кіберзахисту критичної інфраструктури України та її інтеграції до європейського простору кібербезпеки.

Висновки

Проведений аналіз свідчить про суттєву трансформацію нормативно-правового забезпечення кібербезпеки України. Прийняття нових

законодавчих актів та внесення змін до чинного законодавства створили правові передумови для впровадження сучасних методів кіберзахисту критичної інфраструктури.

До внесення відповідних законодавчих змін значна частина таких методів не могла бути повноцінно реалізована через відсутність належного нормативного підґрунтя. З урахуванням того, що діяльність органів державної влади повинна здійснюватися виключно у межах повноважень, визначених законодавством, формування відповідної нормативної бази стало необхідною передумовою для практичного впровадження нових підходів до забезпечення кібербезпеки.

Подальший розвиток законодавства у цій сфері буде пов’язаний із процесами гармонізації національного права з правом Європейського Союзу, зокрема імплементацією положень директив CER та NIS2, а також регламенту DORA. Це сприятиме підвищенню рівня кіберстійкості держави та забезпеченню ефективного захисту критичної інфраструктури в умовах сучасних кіберзагроз.

1. Конституція України. https://www.president.gov.ua/documents/constitution
2. Закон України «Про основні засади забезпечення кібербезпеки України». https://zakon.rada.gov.ua/laws/show/2163-19#Text
3. Закон України «Про критичну інфраструктуру». https://zakon.rada.gov.ua/laws/show/2163-19#Text
4. Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2). https://eur-lex.europa.eu/eli/dir/2022/2555/oj
5. Directive (EU) 2022/2557 on the resilience of critical entities (CER). http://data.europa.eu/eli/dir/2022/2557/oj
6. Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA). https://eur-lex.europa.eu/eli/reg/2022/2554/oj
7. ENISA. Cybersecurity and resilience of critical infrastructures. https://www.enisa.europa.eu/topics/cybersecurity-of-critical-sectors
8. NIST Cybersecurity Framework. https://www.nist.gov/cyberframework

О.Є. Максименко

SCADA. СИСТЕМИ УПРАВЛІННЯ ТЕХНОЛОГІЧНИМИ ПРОЦЕСАМИ

Стрімка цифровізація енергетичної галузі та активне впровадження автоматизованих систем управління технологічними процесами сприяють підвищенню ефективності виробництва, передачі та розподілу енергоресурсів. Одночасно це призводить до зростання залежності енергетичної інфраструктури від інформаційно-комунікаційних технологій та промислових систем управління [1].

Невід'ємною складовою сучасних промислових систем управління є SCADA-системи, які забезпечують централізований моніторинг, диспетчеризацію, візуалізацію стану обладнання та дистанційне управління технологічними процесами в режимі реального часу. Саме тому навіть короткочасне порушення функціонування систем управління може призводити до значних технічних та економічних наслідків для енергетичної інфраструктури.

Для України проблема захисту SCADA-систем набула особливої актуальності в умовах повномасштабної війни. У сучасних умовах кіберпростір став одним із ключових напрямів ведення гібридної війни, де атаки на об'єкти критичної енергетичної інфраструктури використовуються з метою дестабілізації роботи держави та порушення функціонування критично важливих систем.

Одним із найбільш показових прикладів реалізації кібератаки на енергетичну інфраструктуру України стала атака, виявлена у жовтні 2022 року під час повномасштабної війни. Основною метою зловмисників було порушення функціонування енергосистеми України шляхом втручання в роботу промислових систем управління та дестабілізація процесів постачання електроенергії [2][3].

Для реалізації атаки використовувалося модифіковане шкідливе програмне забезпечення Industroyer2, спеціально адаптоване для взаємодії з промисловими протоколами та SCADA-компонентами енергетичних систем. На відміну від звичайного шкідливого програмного забезпечення, Industroyer2 було орієнтоване саме на промислове середовище та мало можливість надсилати команди безпосередньо обладнанню електричних підстанцій через протоколи IEC 60870-5-104 [2][3].

За інформацією фахівців із кібербезпеки, проникнення до мережі енергетичного підприємства відбулося завчасно, а зловмисники тривалий час перебували всередині інфраструктури, здійснюючи збір інформації про конфігурацію мережі, SCADA-системи та обладнання підстанцій. Після отримання необхідного доступу було підготовлено сценарій віддаленого відключення енергетичного обладнання шляхом надсилання команд на комутаційні пристрої підстанцій [2][3].

Завдяки оперативним діям українських фахівців із кібербезпеки та CERT-UA атаку вдалося своєчасно виявити, локалізувати та запобігти масштабним відключенням електроенергії. Події жовтня 2022 року продемонстрували, що сучасні SCADA-системи є одними з ключових цілей кібератак у період військових конфліктів, а їх захист має критичне значення для забезпечення енергетичної безпеки держави [3].

Проте для розуміння причин успішності таких атак і вибору ефективних заходів захисту необхідно чітко окреслити внутрішні вразливості SCADA-систем.

До основних ключових проблем, які створюють сприятливі умови для проникнення та ескалації інцидентів SCADA-систем, можна віднести:

1. Переважна більшість SCADA-компонентів використовують застарілі промислові протоколи обміну даними які не підтримують сучасні механізми шифрування та автентифікації, а також мають обмежені можливості оновлення програмного забезпечення.

2. Поєднання IT-мереж та OT-середовища (Operational Technology) та використання віддаленого доступу значно розширює поверхню атаки та створює можливість проникнення зловмисників до критичної інфраструктури через менш захищені сегменти мережі.

3. Відсутність або недостатній моніторинг мережевого трафіку в промислових мережах. У багатьох випадках такі системи виявлення вторгнень та аналізу аномальної активності або взагалі відсутні, або мають обмежений функціонал через специфіку промислового середовища, що в свою чергу ускладнює своєчасне виявлення несанкціонованого доступу, прихованої активності зловмисників та атак на промислові протоколи обміну даними.

4. Складність тестування змін у режимі реального часу. SCADA-системи функціонують безперервно та забезпечують управління критично важливими технологічними процесами, тому навіть незначні помилки під час зміни конфігурації можуть призвести до порушення стабільності роботи енергетичної інфраструктури.

5. Людський фактор. Є однією з ключових проблем кібербезпеки SCADA-систем. Значна частина кіберінцидентів пов’язана з використанням слабких паролів, порушенням політик інформаційної безпеки, помилками персоналу та недостатнім рівнем підготовки операторів промислових систем.

Аналізуючи вище зазначені ризики можна прийти до висновку, що для забезпечення ефективного захисту SCADA-систем, мінімізації ризиків реалізації кібератак та їх впливу на систему, необхідне комплексне застосування організаційних, технічних та програмних методів кіберзахисту,

Одним із основних способів зниження ризиків, пов’язаних із використанням застарілих промислових протоколів, є впровадження сучасних засобів шифрування, VPN-технологій та механізмів багатофакторної автентифікації для захисту віддаленого доступу до

SCADA-систем. Для промислових мереж також доцільним є поступовий перехід до більш захищених версій протоколів обміну даними та впровадження концепції Zero Trust Architecture[1].

До ключових принципів захисту ICS при інтеграції IT та OT-середовища є сегментація мережі та ізоляція технологічного середовища від корпоративних і публічних мереж. Використання міжмережевих екранів, демілітаризованих зон, систем контролю доступу дозволяє суттєво знизити ризик несанкціонованого проникнення до критичних компонентів інфраструктури.

Впровадження систем моніторингу та виявлення аномальної активності дозволяють своєчасно виявляти підозрілу активність і реагувати на кіберінциденти у роботі SCADA-систем. Сучасні системи SIEM, IDS/IPS та засоби аналізу мережевого трафіку активно використовують алгоритми машинного навчання, статистичні методи аналізу даних та системи прогнозування кіберінцидентів. Використання математичних моделей дозволяє виявляти нетипову поведінку обладнання та прогнозувати можливі загрози ще до моменту реалізації атаки.

Технологія UEBA (User and Entity Behavior Analytics) доповнює традиційні SIEM і IDS тим, що фокусується не на сигнатурах, а на поведінкових моделях користувачів і пристроїв: системи будують базову лінію нормальної активності і виявляють відхилення за допомогою алгоритмів машинного навчання - автоенкодерів, кластеризації, дерев рішень або нейромереж. У контексті SCADA це дозволяє помічати складні, контекстуальні атаки - латеральний рух, підміни команд, аномальні послідовності телеметрії - які не завжди мають відомі сигнатури.

Перспективним напрямом розвитку систем захисту є використання цифрових двійників (Digital Twin) - це високодеталізована віртуальна копія енергетичної системи, яка відтворює топологію мережі, поведінку обладнання, логіку контролерів і потоки телеметрії. У безпечному середовищі двійник дозволяє інжектувати реалістичні вектори атак: фішинг, підміни команд PLC/RTU, затримки телеметрії або шкідливі команди реле і спостерігати фізичні наслідки віртуально: перевантаження, каскадні відключення або збої в логіці захисту. Серед практичних переваг: раннє виявлення вразливостей, можливість тестувати контрзаходи до їхнього впровадження, скорочення часу відновлення після інциденту та підвищення готовності персоналу.

Мінімізація ризиків, пов’язаних із людським фактором, потребує регулярного навчання персоналу та підвищення рівня кібергігієни операторів промислових систем.

Важливими заходами є:

– використання складних паролів та багатофакторної автентифікації;

– розмежування прав доступу користувачів;

– регулярний аудит дій операторів;

– проведення тренувань із реагування на кіберінциденти;

– навчання персоналу методам протидії соціальній інженерії.

Ефективний захист SCADA-систем також потребує належного нормативно-правового забезпечення. В Україні основою державної політики у сфері кібербезпеки є Закон України «Про основні засади забезпечення кібербезпеки України» [4] та Закон України «Про критичну інфраструктуру» [5].

Одним із ключових міжнародних стандартів у сфері захисту промислових систем є серія стандартів IEC 62443, яка визначає вимоги до кібербезпеки промислових автоматизованих систем і мереж. Важливе значення також має Directive (EU) 2022/2555 (NIS2 Directive), що встановлює сучасні вимоги до забезпечення кіберстійкості критичної інфраструктури [6].

Висновки

SCADA-системи є критично важливим елементом сучасної енергетичної інфраструктури, однак їх висока інтеграція з інформаційними технологіями створює значні кіберризики. Основними причинами вразливості таких систем є використання застарілих технологій, інтеграція IT та OT-середовища, складність оновлення промислового обладнання та людський фактор.

Сучасні кіберзагрози для енергетичної галузі потребують комплексного підходу до забезпечення безпеки промислових систем управління, що включає сегментацію мереж, моніторинг аномальної активності, контроль доступу, використання алгоритмів машинного навчання, навчання персоналу та впровадження міжнародних стандартів кібербезпеки.

Перспективним напрямом подальшої наукової роботи являються дослідження розробки та впровадження технології цифрових двійників (Digital Twin) для моделювання роботи SCADA-систем, прогнозування кіберзагроз, тестування механізмів захисту та відпрацювання сценаріїв реагування на кіберінциденти без ризику для реальної критичної інфраструктури. Особливий інтерес становить інтеграція технологій штучного інтелекту та поведінкового аналізу для створення адаптивних систем кіберзахисту промислових мереж.

1. ENISA — Cybersecurity and resilience of critical infrastructures. https://www.enisa.europa.eu/topics/cybersecurity-of-critical-sector
2. ESET — technical analysis and reports. https://www.welivesecurity.com/
3. CERT-UA — офіційні повідомлення та аналітика щодо інцидентів в Україні. https://cert.gov.ua/
4. Закон України «Про основні засади забезпечення кібербезпеки України». https://zakon.rada.gov.ua/laws/show/2163-19#Text
5. Закон України «Про критичну інфраструктуру». https://zakon.rada.gov.ua/laws/show/2163-19#Text
6. Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2). https://eur-lex.europa.eu/eli/dir/2022/2555/oj

Д.О. Рибачок, О.С. Кушнір

ПОТОКОВИЙ КОНВЕЄР ЗБОРУ ДАНИХ ENTSO-E ДЛЯ МЕРЕЖЕВОГО МОДЕЛЮВАННЯ ЕНЕРГОРИНКІВ

Сучасні форми ринкової взаємодії в енергетиці, зокрема децентралізовані ринки електроенергії [4], можуть бути використані для забезпечення ефективного та безперебійного доступу до енергомереж в умовах безпекових ризиків. Перехід до нових форм взаємодії може призводити до впровадження нових технологічних рішень і як наслідок виникнення потреби в імітаційному моделюванні. Однією з проблем зазначеного підходу до моделювання ринкових взаємодій є доступ до даних. Наразі в Україні доступ до даних в енергетиці обмежено [1,2]. Як наслідок відсутності даних за вітчизняними ринками для моделювання можуть бути використані відкриті дані інших країн.

ENTSO-E Transparency Platform (TP) - це офіційний європейський цифрова платформа збору, агрегування та публікації енергетичних даних, який функціонує в якості центрального вузла інформаційної інфраструктури внутрішнього ринку електроенергії Європейського Союзу. Функціонування платформи ґрунтується на вимогах Регламенту (ЄС) №543/2013, що визначає обов'язковість публікації фундаментальних показників генерації, навантаження, передачі та балансування. TP забезпечує:

- уніфікований доступ до даних від операторів систем передачі (TSO), бірж та інших кваліфікованих постачальників інформації;
- стандартизовані формати даних, визначені у Manual of Procedures та Detailed Data Descriptions;
- публікацію в реальному часі або з регламентованою затримкою ключових показників роботи енергосистем.

Зокрема, TP виконує функції забезпечення прозорості європейських енергетичних ринків, а саме публікація щільних даних щодо: обсягів генерації за типами технологій, прогнозами та фактичним навантаженням, доступності та використання мережевих інфраструктур, балансуючих обсягів та цін. Варто зауважити, що подібна відкритість запобігає можливим зловживанням ринковою владою.

Платформа ENTSO-E Transparency Platform надає програмний доступ до даних через REST API з авторизацією за персональним токеном. Кожен запит адресує конкретний тип документа згідно з кодифікацією ENTSO-E: A44 (ціни ринку «на добу наперед», Day-Ahead), A11 (фізичні транскордонні перетоки електроенергії), A65 (прогнози навантаження на добу наперед). Бідингові зони ідентифікуються за кодами EIC (Energy Identification Codes) – стандартизованими міжнародними ідентифікаторами учасників та об'єктів енергоринку. Відповіді повертаються у форматі XML зі структурою Publication_MarketDocument → TimeSeries → Period → Point, де кожна точка містить значення відповідного показника з часовою міткою та роздільною

здатністю (зазвичай PT60M – погодинні дані). На основі зазначеного API розроблено потоковий програмний конвеєр EnergyNetDA, що реалізує автоматизований збір, обробку та передачу ринкових даних у реальному часі. Конвеєр побудовано мовою Scala 3 із застосуванням екосистеми Typelevel: бібліотека Cats Effect 3 забезпечує безпечну конкурентну обробку на основі алгебраїчних ефектів, http4s – формування та виконання HTTP-запитів, fs2 – функціональну потокову обробку даних, fs2-kafka – інтеграцію з брокером повідомлень Apache Kafka, circe – серіалізацію доменних об'єктів у JSON. Загальна архітектура передбачає двоетапний ланцюг: Scala-конвеєр здійснює збір та публікацію даних у Kafka, а Python-споживач підключається до Kafka-топіків для побудови мережевих моделей та аналітичної обробки.

Вибір Scala 3 як основної мови реалізації зумовлено кількома чинниками. По-перше, система типів Scala дозволяє на етапі компіляції контролювати коректність доменної моделі – кожний тип ринкових даних (DayAheadPrice, CrossBorderFlow, LoadForecast, MarketSnapshot) представлено окремим типобезпечним класом. По-друге, модель конкурентності на основі Cats Effect забезпечує легковагове паралельне виконання HTTP-запитів до ENTSO-E API без створення потоків операційної системи. По-третє, бібліотека fs2 надає абстракцію нескінченних функціональних потоків із вбудованою обробкою зворотного тиску (backpressure), що є принципово важливим для безперервного збору даних.

Доменна модель конвеєра охоплює 10 бідингових зон: три українські (UA_IPS – об'єднана енергосистема України, UA_BEI – Бурштинський енергоострів, UA_DOBTPP – Добротвірська ТЕС) та сім сусідніх (Польща, Словаччина, Угорщина, Румунія, Молдова, Німеччина-Люксембург, Чехія, Австрія). Для кожної зони задано відповідний EIC-код, що використовується при формуванні запитів до API. Модель також описує 14 міждержавних інтерконекторів – фізичних з'єднань між зонами, за якими здійснюється транскордонний переток електроенергії. Серед них: UA_IPS–PL, UA_IPS–SK, UA_IPS–HU, UA_IPS–RO, UA_IPS–MD, а також з'єднання між сусідніми державами (PL–DE_LU, PL–CZ, SK–HU, SK–CZ, HU–RO, HU–AT, DE_LU–AT, DE_LU–CZ).

Для кожного типу даних клієнт ENTSO-E формує параметризований HTTP-запит, що включає тип документа, EIC-коди зон, початок та кінець часового періоду. Отримані XML-відповіді обробляються спеціалізованим парсером, який витягує часові ряди з погодинною роздільною здатністю. У разі перевищення ліміту запитів (HTTP-статус 429 Too Many Requests) конвеєр зчитує заголовок Retry-After і виконує повторну спробу після вказаної затримки, що забезпечує стійкість до обмежень rate limiting.

Ядром потокової архітектури є бібліотека fs2 Stream. Конвеєр створює два нескінченні потоки: потік цін Day-Ahead та потік транскордонних перетоків. Кожен потік із заданою періодичністю (за замовчуванням – 1 година) генерує набір запитів для всіх цільових зон або інтерконекторів, виконує їх паралельно (parEvalMapUnordered з рівнем паралелізму 4) та публікує отримані записи у відповідні Kafka-топіки. Два потоки об'єднуються

оператором merge і виконуються конкурентно в межах одного процесу. Конвеєр визначає чотири Kafka-топіки: entsoe.day-ahead-prices (погодинні ціни), entsoe.cross-border-flows (транскордонні перетоки), entsoe.load-forecasts (прогнози навантаження), entsoe.market-snapshots (агреговані знімки ринку). Продюсер Kafka налаштовано з увімкненою ідемпотентністю (enable.idempotence = true), що гарантує доставку кожного повідомлення рівно один раз (exactly-once semantics). Записи серіалізуються у формат JSON із використанням бібліотеки circe та конвертацією назв полів у snake_case для сумісності з Python-споживачем.

Apache Kafka в даній архітектурі виконує роль сполучної ланки між Scala-конвеєром збору даних та Python-модулем аналітики. Такий підхід забезпечує розділення відповідальності: Scala-частина оптимізована для надійного конкурентного збору з type-safe гарантіями, тоді як Python-споживач використовує екосистему бібліотек для наукових обчислень (NumPy, pandas, NetworkX) для побудови та аналізу мережевих моделей. Kafka також надає буферизацію, що дозволяє споживачу обробляти дані у власному темпі, та забезпечує персистентність повідомлень для повторної обробки за потреби.

Зібрані дані природним чином утворюють мережеву структуру.[5] Бідингові зони відповідають вершинам графа, а інтерконектори – ребрам, ваги яких визначаються обсягами фізичних перетоків електроенергії (у МВт). Така структура формує мультишаровий граф: шар фізичних перетоків відображає реальні потоки електроенергії між зонами, а шар цінових кореляцій – ступінь взаємозв'язку між ціновими динаміками суміжних ринків. Оскільки дані надходять з погодинною роздільною здатністю, мережева модель являє собою послідовність часових зрізів, кожен з яких фіксує стан енергоринку в конкретний момент часу.

Таким чином, потоковий конвеєр EnergyNetDA забезпечує автоматизований збір реальних ринкових даних з платформи ENTSO-E Transparency Platform та їх підготовку для подальшого мережевого моделювання. Конвеєр створює інформаційну основу для дослідження структурних властивостей європейського енергоринку – виявлення вузлів-концентраторів, аналізу динаміки транскордонних перетоків, оцінки впливу цінових шоків на суміжні ринки. Запропонований підхід може бути адаптований для українських енергетичних ринків у міру розширення відкритості даних та інтеграції української енергосистеми в європейський ринок ENTSO-E.

1. Оператор ринку, Щодо публікації інформації про торги електричною енергією на РДН та ВДР під час воєнного стану, 2024, URL: https://www.oree.com.ua/index.php/newsctr/n/26150

2. Українська енергетична біржа, Припинення публікації аукціонних бюлетенів та бюлетенів середньозважених цін на період дії воєнного стану, 2024, URL: https://www.ueex.com.ua/presscenter/news/prypynennya-publikatsii-auktsionnyh-buleteniv-ta-buleteniv-sered/

3. European Commission, Commission Regulation (EU) No 543/2013 of 14 June 2013 on submission and publication of data in electricity markets. *Official Journal of the European Union*, 2013, URL: https://eur-lex.europa.eu/eli/reg/2013/543/oj/eng

4. Горбачук В.М., Бардадим Т.О., Дунаєвський М.С., Годлюк В.В., Рибачок Д.О. Основи децентралізованих ринків електроенергії. Науково-практична конференція, 2025.

5. Рибачок Д.О. Мережеві структури в комп'ютерних науках та економіці. Математичне та програмне забезпечення інтелектуальних систем, 2024.

Є.О. Сенюк, В.Е. Мельничук

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ МОНІТОРИНГУ ТА ESG УПРАВЛІННЯ

В умовах посилення вимог до прозорості та звітності компаній, ESG-управління стає ключовим елементом стратегії сталого розвитку. ШІ надає інструменти для автоматичного збору даних, їх обробки в режимі реального часу та прогнозування трендів, що дозволяє підвищити точність моніторингу, знизити витрати та прискорити прийняття управлінських рішень.

Для оцінки ESG використовуються різноманітні джерела такі як сенсорні мережі (викиди, якість повітря, води), супутникові знімки, промислові телеметричні дані, внутрішні ERP/IoT системи, а також неструктуровані джерела — новинні стрічки, звіти, соціальні мережі. Методи ШІ включають машинне навчання для прогнозування, комп'ютерний зір для аналізу знімків, NLP (обробка природної мови) для аналізу тексту та алгоритми аномалії - детекції для виявлення відхилень у показниках.

Аналізуючи прикладну функцію ШІ, варто зазначити що в межах сфери ESG управління можливо виокремити три пріоритетні напрямки:

1. Екологічний моніторинг (E) — автоматичний аналіз даних з датчиків викидів та супутникових даних для виявлення витоків і оцінки впливу на навколишнє середовище.

2. Соціальний моніторинг (S) — аналіз зворотного зв'язку співробітників і громадськості, індекси задоволеності, розриви в оплаті праці.

3. Управління (G) — автоматизація контролю за дотриманням політик, виявлення ризикової поведінки та аналіз корпоративних документів за допомогою NLP [1, 2].

Станом на сьогодні, існує велика кількість моделей оцінки ESG для бізнесу. Один із підходів до агрегування даних — обчислення зваженого ESG-індексу як лінійної комбінації компонентів E, S та G:

$$ESG\_\{score\} = w\_E * E + w\_S * S + w\_G * G \quad (1)$$

Тут w_E, w_S, w_G — вагові коефіцієнти компонентів; E, S, G — нормалізовані значення екологічного, соціального та управлінського індексів відповідно. Вагові коефіцієнти встановлюються з урахуванням пріоритетів стейкхолдерів або нормативних вимог [3].

Приклад підбору показників представлено у таблиці 1.

Таблиця 1 – Ключові показники ESG та методи збору даних

Показник	**Метрика / Одиниця**	**Джерело даних**
Викиди CO2	тонн/рік	Датчики, супутники, баланс потужностей
Споживання води	м³	Інтелектуальні лічильники, IoT
Індекс задоволеності персоналу	бал	Опитування, HR-системи
Кібербезпека	кількість інцидентів	SIEM, журнали подій

Варто зазначити, що незважаючи на переваги, існують значні виклики щодо впровадження моніторингу даних на основі ШІ, а саме якість даних (неповні або упереджені набори даних), прозорість алгоритмів, захист персональних даних, а також ризики маніпуляції показниками. Впровадження повинно супроводжуватися аудитом моделей, пояснювальною аналітикою та політиками з управління даними [3].

Для успішної реалізації використання ШІ для моніторингу в умовах ESG управління, варто розподілити процеси впровадження на етапи:

1. Розробити політику якості даних і механізми валідації.
2. Використовувати комбіновані підходи (моделі + експертна оцінка).
3. Забезпечити прозорість і відстежуваність прийнятих рішень.
4. Інтегрувати інструменти ШІ та аудит алгоритмів.
5. Планувати навчальні програми для персоналу щодо інтерпретації результатів ШІ.

Висновки. ШІ трансформує ESG з пасивної звітності на інструмент стратегічного прогнозування. Завдяки автоматизації збору даних із тисяч неструктурованих джерел — від супутникових знімків для моніторингу викидів до аналізу настроїв у соцмережах — компанії отримують точну картину свого впливу в режимі реального часу, що мінімізує ризик людських помилок і значно підвищує швидкість підготовки аудитів.

Інтеграція алгоритмів машинного навчання дозволяє не лише фіксувати поточний стан, а й моделювати майбутні кліматичні та операційні ризики. Даний підхід надає бізнесу можливість оптимізувати використання ресурсів, прогнозувати ланцюги постачання та вибудовувати стійку модель розвитку, що підвищує привабливість компанії для інвесторів. Прозорість, яку забезпечує ШІ, стає надійним захистом від звинувачень у грінвошингу.

Водночас успішне впровадження ШІ вимагає суворого дотримання етичних норм та контролю за якістю вхідних даних. Алгоритми мають бути прозорими та зрозумілими для регуляторів, щоб уникнути упередженості в оцінках. Кінцева ефективність технології залежить від балансу між потужністю обчислень та відповідальним підходом до управління цифровими ризиками.

1. Dai, A., & Smith, B. (2021). Artificial Intelligence for Environmental Monitoring. Journal of Sustainable Computing, 12(3), 45–63.

2. Khan, S., & Lee, J. (2020). Machine Learning Approaches for ESG Risk Assessment. Sustainability Analytics, 8(2), 101–119.

3. ДСТУ 3008-2015. Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання. – На заміну ДСТУ 3008–95; чинний з 2017–07–01.

НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

«ВИКОРИСТАННЯ БЛОКЧЕЙН ТЕХНОЛОГІЙ В ЕНЕРГЕТИЦІ – 2026»

Збірник матеріалів конференції

25 березня 2026 р.

Usage of blockchain technologies in energetics – 2026 : collection of materials of the scientific and practical conference, Kyiv, March 25, 2026, PIMEE of NAS of Ukraine. - 2026. - 66 p.

Використання блокчейн технологій в енергетиці – 2026: збірник матеріалів науково-практичної конференції, м. Київ, 25 березня 2026 р., ІПМЕ ім. Г.Є. Пухова НАН України. – 2026. – 66 с.