Електронний журнал «Державне управління: удосконалення та розвиток» включено до переліку наукових фахових видань України з державного управління (Категорія «Б», Наказ Міністерства освіти і науки України № 1643 від 28.12.2019). Спеціальність – 281.

Державне управління: удосконалення та розвиток. 2025. № 5.

DOI: http://doi.org/10.32702/2307-2156.2025.5.11

УДК 351:004

Б. В. Дзюндзюк,

к. держ. упр.

ORCID ID: https://orcid.org/0000-0001-9066-2849

БЕЗПЕКА СМАРТ-КОНТРАКТІВ У ПУБЛІЧНОМУ СЕКТОРІ

B. Dziundziuk,

PhD in Public Administration

SECURITY OF SMART CONTRACTS IN THE PUBLIC SECTOR

Проаналізовано типові вразливості смарт-контрактів, такі як помилки в логіці виконання, проблеми з видимістю функцій, арифметичні вразливості та ризики, пов'язані з взаємодією з зовнішніми сервісами. Наголошено на критичній важливості розробки високих стандартів безпечного програмування смарт-контрактів для мінімізації ризиків та негативних наслідків експлуатації вразливостей у публічному секторі.

Розглянуто ключові підходи до забезпечення безпеки смарт-контрактів, зокрема дотримання принципу найменших привілеїв, модульність та простота коду, використання перевірених бібліотек та шаблонів проєктування, ретельне тестування на різних рівнях. Підкреслено важливість аудиту безпеки із залученням незалежних експертів,

впровадження формальної верифікації, а також постійного моніторингу роботи смарт-контрактів після їх розгортання.

Наголошено на необхідності розвитку культури безпеки та відповідального ставлення до розробки смарт-контрактів у публічному секторі. Це вимагає інвестицій у навчання персоналу, впровадження ефективних процесів співпраці між різними командами, а також тісної взаємодії урядових організацій, розробників блокчейн-рішень та професійних спільнот для обміну знаннями та досвідом.

Розглянуто також специфічні виклики забезпечення безпеки смарт-контрактів у публічній сфері, такі як відповідність регуляторним вимогам, захист персональних даних, управління криптографічними ключами та ідентифікація користувачів, а також людський фактор. Запропоновано можливі шляхи подолання цих викликів через співпрацю з регуляторами, використання передових практик шифрування та контролю доступу, підвищення обізнаності та цифрової грамотності всіх залучених сторін.

Typical vulnerabilities of smart contracts are analyzed, such as errors in execution logic, problems with function visibility, arithmetic vulnerabilities and risks associated with interaction with external services. The critical importance of developing high standards of secure programming of smart contracts is emphasized to minimize the risks and negative consequences of exploiting vulnerabilities in the public sector.

Key approaches to ensuring the security of smart contracts are considered, in particular, adherence to the principle of least privilege, modularity and simplicity of code, use of proven libraries and design patterns, thorough testing at different levels. The importance of security audits involving independent experts, the introduction of formal verification, as well as constant monitoring of the operation of smart contracts after their deployment is emphasized.

The need to develop a security culture and a responsible attitude to the development of smart contracts in the public sector is emphasized. This requires

investment in staff training, the implementation of effective collaboration processes between different teams, as well as close interaction between government organizations, blockchain developers and professional communities to share knowledge and experience.

The specific challenges of ensuring the security of smart contracts in the public sphere are also considered, such as regulatory compliance, personal data protection, cryptographic key management and user identification, as well as the human factor. Possible ways to overcome these challenges are proposed through cooperation with regulators, the use of best practices for encryption and access control, and increasing awareness and digital literacy of all parties involved.

The article aims to draw attention to the critical importance of security issues when developing and implementing smart contract-based solutions in the public sector, as well as to stimulate further research, discussion, and exchange of experience in this area.

Ключові слова: *смарт-контракти, безпека, блокчейн, публічне управління, публічний сектор*.

Keywords: *smart contracts, security, blockchain, public administration, public sector.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Дослідження безпеки смарт-контрактів у публічному секторі є надзвичайно важливою темою, враховуючи потенціал технології блокчейн для трансформації та оптимізації процесів публічного управління. Смарт-контракти, які по суті є автоматизованими угодами з умовами, закодованими безпосередньо в коді, мають здатність покращити такі сфери як надання адміністративних послуг, управління публічними реєстрами, проведення закупівель, розподіл грантів та субсидій тощо. Однак, поряд з перевагами ефективності, прозорості та автоматизації, які надають смарт-контракти, виникають і серйозні питання

щодо забезпечення їх безпеки, особливо коли мова йде про такі чутливі сфери як публічне управління.

Враховуючи, що смарт-контракти після розгортання в блокчейні стають незмінними і автономними, будь-які помилки або вразливості в їхньому коді можуть призвести до катастрофічних наслідків – від фінансових втрат до порушення роботи критичних публічних сервісів та підриву довіри громадян до системи державного управління в цілому. Саме тому ретельне дослідження потенційних ризиків безпеки смарт-контрактів, розробка стандартів їх безпечного програмування та впровадження комплексної методології аудиту є першочерговими завданнями для органів влади, що розглядають можливості використання блокчейну.

Аналіз останніх досліджень і публікацій. Питання застосування технології блокчейн розглядаються у працях багатьох українських і зарубіжних науковців, зокрема, таких як О. Балан, В. Воробець, Е. Гофманн, В. Дрешпак, І. Клименко, С. Олнес, Р. Мазур, К. Хаккі, Ц. Чен та ін. Проте все ще недостатньо уваги приділено питанню безпеки смарт-контрактів в публічному секторі.

Формулювання цілей статті (постановка завдання). Мета статті полягає в тому, щоб розглянути питання безпеки використання смарт-контрактів у публічному секторі.

Виклад основного матеріалу дослідження. Якщо проаналізувати найбільш типові вразливості смарт-контрактів, то можна виділити кілька основних категорій. Перш за все, це помилки в логіці виконання контракту, такі як некоректне використання умовних операторів, циклів, неправильна обробка виняткових ситуацій тощо. Так звані «логічні баги» можуть спричинити непередбачувану поведінку контракту і створити лазівки для зловмисників.

Іншим поширеним типом вразливостей є проблеми з видимістю і областю дії функцій та змінних всередині контракту. Якщо критичні функції або змінні, що зберігають важливі дані, помилково оголошені як публічні або

не мають належного контролю доступу, це може дозволити атакуючим змінювати логіку контракту або викрадати кошти.

Смарт-контракти, які оперують криптовалютами та іншими цифровими активами, також схильні до вразливостей, пов’язаних з арифметичними операціями, таких як переповнення цілих чисел, втрата точності при операціях з дробовими числами тощо. Експлуатуючи ці недоліки, зловмисники можуть генерувати величезні суми коштів буквально з повітря або викликати помилки в розрахунках.

Ще одним серйозним джерелом ризиків є взаємодія смарт-контрактів з іншими контрактами або зовнішніми сервісами. Якщо смарт-контракт покладається на дані або логіку, що надходять ззовні, і не проводить належної перевірки і фільтрації вхідних параметрів, зловмисники можуть маніпулювати його поведінкою або вводити шкідливий код.

Також смарт-контракти, як і будь-який інший програмний код, схильні до вразливостей, пов’язаних з відсутністю або недостатністю контролю доступу, перевірок вхідних даних, безпечного управління ключами тощо. Атакуючі можуть експлуатувати ці слабкі місця, щоб отримати несанкціонований доступ до функцій контракту, маніпулювати даними або здійснювати інші шкідливі дії.

Усвідомлюючи потенційні ризики, пов’язані з цими вразливостями, стає очевидним, що розробка смарт-контрактів для використання в публічному секторі вимагає особливої уваги та відповідальності. Експлуатація вразливостей в смарт-контрактах, що забезпечують роботу державних сервісів та систем, може мати надзвичайно негативні наслідки для великої кількості громадян, підривати довіру до державних інституцій та призводити до серйозних репутаційних і фінансових втрат [5].

Саме тому розробка і впровадження високих стандартів безпечного програмування смарт-контрактів має стати одним з найважливіших пріоритетів для команд розробників та керівників блокчейн проєктів у публічному секторі. Ці стандарти повинні враховувати передовий досвід і

рекомендації експертної спільноти, а також специфічні вимоги і контекст застосування блокчейну в державному управлінні.

Перш за все, при проєктуванні архітектури смарт-контрактів необхідно керуватися принципом найменших привілеїв, тобто надавати смарт-контрактам та окремим функціям всередині них мінімально необхідний рівень доступу і повноважень для виконання своїх завдань. Критично важливі функції, що відповідають за переказ коштів або зміну стану контракту, повинні бути захищені надійними механізмами автентифікації та авторизації, наприклад, з використанням мультипідпису або розподіленого контролю доступу.

Також важливо забезпечити модульність і простоту коду смарт-контрактів, уникати надмірно складних конструкцій та великих монолітних контрактів. Замість цього, краще розбивати функціональність на менші, незалежні і добре документовані модулі, що значно полегшує аналіз коду, пошук помилок та подальшу підтримку і модифікацію контрактів.

При написанні коду смарт-контрактів слід використовувати перевірені часом шаблони проєктування, бібліотеки та інструменти, рекомендовані професійною спільнотою розробників блокчейн. Спеціалізовані фреймворки для розробки смарт-контрактів, такі як OpenZeppelin, надають готові і ретельно протестовані компоненти для найбільш типових завдань, таких як управління доступом, робота з токенами, математичні операції тощо. Використання таких перевірених рішень дозволяє мінімізувати ризики помилок та вразливостей, а також забезпечує сумісність і можливість інтеграції з іншими компонентами блокчейн-екосистеми.

Невід’ємною частиною процесу розробки безпечних смарт-контрактів є також комплексне тестування на різних рівнях. Від модульного тестування окремих функцій до інтеграційного тестування взаємодії з іншими контрактами та системного тестування в умовах, максимально наближених до реального середовища. Особливу увагу слід приділяти тестам на граничні

значення, обробку виняткових ситуацій, перевірку коректності математичних операцій тощо [3].

Дуже корисним інструментом є також тести проникнення або баг-баунті, коли незалежні експерти з безпеки намагаються знайти вразливості в смарт-контрактах, імітуючи потенційні атаки. Такий підхід дозволяє виявити недоліки, які могли залишитися непоміченими під час внутрішнього тестування, і вчасно їх виправити до розгортання контрактів у робочому середовищі.

Окрім власне практик безпечного програмування, надзвичайно важливим для смарт-контрактів у публічній сфері є впровадження належної культури документування та рецензування коду. Кожен смарт-контракт повинен супроводжуватися детальною документацією, що описує його призначення, логіку роботи, інтерфейси взаємодії, відомі обмеження та потенційні ризики.

Перед інтеграцією до основної кодової бази та розгортанням смарт-контракту, його код обов’язково має пройти ретельне рецензування декількома незалежними експертами. Під час рецензування перевіряється не тільки функціональна коректність коду, але й дотримання стандартів безпеки, відсутність антипатернів та потенційних вразливостей. Всі зауваження і рекомендації рецензентів повинні бути задокументовані та відпрацьовані перед затвердженням змін.

Незважаючи на всі заходи безпечної розробки, для смарт-контрактів, які планується використовувати в реальних додатках у публічному секторі, необхідно також проводити ретельний аудит безпеки із залученням незалежних професійних аудиторських компаній або досвідчених фахівців з інформаційної безпеки. Методологія такого аудиту повинна включати комбінацію ручного аналізу коду досвідченими експертами, статичного аналізу з використанням спеціалізованих інструментів для виявлення типових вразливостей та антипатернів, динамічного аналізу поведінки контрактів у тестовому блокчейн-середовищі, а також перевірку відповідності бізнес-

логіки і функціональних вимог до контракту загальній архітектурі рішення та нормативним документам [7].

Перспективним підходом є також формальна верифікація смарт-контрактів, що передбачає використання математичних методів для доведення коректності та безпечності певних властивостей контракту ще на етапі проєктування. Хоча формальна верифікація поки що не дуже поширена через свою складність, вона може стати потужним інструментом забезпечення безпеки особливо критичних смарт-контрактів з високими вимогами до надійності.

За результатами аудиту безпеки складається детальний звіт, що містить перелік виявлених недоліків та вразливостей, оцінку їх критичності та потенційного впливу, а також рекомендації щодо їх усунення або мінімізації ризиків. Цей звіт стає основою для подальшої роботи розробників над виправленням проблем та вдосконаленням контракту перед запуском.

Але навіть успішне проходження аудиту не означає абсолютної гарантії безпеки смарт-контракту, адже в динамічному середовищі блокчейну завжди можуть виникати нові загрози і вразливості. Тому найкращою практикою є впровадження процесів постійного моніторингу та аналізу роботи смарт-контрактів після розгортання, збирання даних про потенційні інциденти чи аномальну поведінку, підтримка відкритих каналів зв’язку з користувачами та дослідниками безпеки для своєчасного виявлення та реагування на можливі проблеми [1].

Забезпечення безпеки смарт-контрактів для застосування у сфері публічного управління є комплексним завданням, що вимагає відповідального ставлення та глибокої експертизи на всіх етапах – від проєктування архітектури та розробки до тестування, аудиту та моніторингу розгорнутих рішень. Тільки за умови впровадження наскрізних практик безпечного програмування, дотримання високих стандартів якості коду, залучення незалежних фахівців для рецензування та аудиту, а також підтримки прозорої співпраці з професійною спільнотою дослідників безпеки блокчейн-проєктів,

публічний сектор зможе повною мірою скористатися перевагами смарт-контрактів, мінімізувавши при цьому ризики та забезпечивши надійний захист інтересів громадян і держави.

Це безумовно вимагатиме значних зусиль, ресурсів та зміни усталених підходів до розробки та впровадження інформаційних систем у публічному секторі, але потенційні переваги від використання смарт-контрактів, такі як підвищення ефективності, прозорості, підзвітності та довіри, безумовно варті цих інвестицій.

Саме тому уряди та організації публічного сектору, які прагнуть реалізувати потенціал блокчейну та смарт-контрактів, повинні від самого початку зробити безпеку одним з найважливіших пріоритетів та інтегрувати кращі практики безпечної розробки у всі аспекти своїх проєктів. Це включає не лише технічні рішення та інструменти, але й відповідну підготовку та навчання персоналу, налагодження ефективних процесів комунікації та співпраці між різними командами та зацікавленими сторонами, а також формування культури відповідального ставлення до безпеки на всіх рівнях організації [2].

При цьому важливо розуміти, що забезпечення безпеки смарт-контрактів – це не одноразова дія, а безперервний процес, який повинен адаптуватися та вдосконалюватися разом зі змінами у технологіях, регуляторних вимогах та середовищі загроз. Тому організаціям, які впроваджують блокчейн-рішення, необхідно виділяти достатньо ресурсів не лише на початкові етапи розробки та аудиту, але й на підтримку і постійне вдосконалення систем безпеки протягом всього життєвого циклу смарт-контрактів.

Нарешті, забезпечення високого рівня безпеки смарт-контрактів у публічному секторі вимагає також тісної співпраці та обміну знаннями між урядовими організаціями, розробниками блокчейн-рішень, науковими установами та професійними спільнотами. Адже тільки об’єднавши зусилля та експертизу різних зацікавлених сторін, ми зможемо розробити дійсно надійні

та ефективні стандарти, методології та інструменти для захисту смарт-контрактів, які стануть основою для широкого впровадження цієї перспективної технології на благо суспільства [4].

Саме тому дослідження, подібні до цього, що всебічно розглядають різні аспекти безпеки смарт-контрактів у контексті публічного сектору, є вкрай важливими для формування відповідної бази знань, підвищення обізнаності про потенційні ризики та розробки ефективних стратегій їх мінімізації. Вони можуть стати відправною точкою для подальших дискусій, обміну практичним досвідом та вироблення галузевих стандартів і регуляторних норм, які сприятимуть безпечному та відповідальному використанню смарт-контрактів для вирішення нагальних суспільних проблем та підвищення якості публічних послуг.

Забезпечення високого рівня безпеки смарт-контрактів є одним з ключових факторів успішного впровадження блокчейн-технологій у публічному секторі. Це вимагає комплексного підходу, що поєднує в собі використання передових технічних рішень та інструментів безпечної розробки, дотримання стандартів якості коду та процесів управління життєвим циклом смарт-контрактів, залучення висококваліфікованих фахівців для аудиту та постійного моніторингу, а також тісної співпраці між різними зацікавленими сторонами для обміну знаннями та досвідом.

Тільки за умови відповідального ставлення до питань безпеки на всіх етапах реалізації блокчейн-проєктів, від ідеї до розгортання та супроводу, публічний сектор зможе повною мірою розкрити потенціал смарт-контрактів для підвищення ефективності, прозорості та довіри, водночас забезпечуючи надійний захист цифрових активів та інтересів громадян. А подальші дослідження та дискусії в цій сфері допоможуть сформувати необхідну базу знань та кращих практик для безпечного та відповідального використання цієї перспективної технології на благо суспільства.

Продовжуючи тему безпеки смарт-контрактів у публічному секторі, важливо більш детально розглянути деякі специфічні аспекти та виклики, з якими можуть стикнутися організації при впровадженні цієї технології.

Одним з таких аспектів є забезпечення відповідності смарт-контрактів існуючим регуляторним вимогам та правовим нормам. Враховуючи, що технологія блокчейн та смарт-контракти все ще перебувають на відносно ранньому етапі розвитку, багато країн поки що не мають чітких законодавчих рамок, які б регулювали їх використання в публічній сфері. Це створює певну невизначеність для організацій, які хочуть впроваджувати ці інноваційні рішення, адже їм доводиться діяти в умовах правового вакууму або намагатися самостійно інтерпретувати існуючі норми.

В такій ситуації надзвичайно важливо, щоб розробники смарт-контрактів тісно співпрацювали з юристами та фахівцями з комплаєнсу, щоб забезпечити відповідність своїх рішень духу та букві закону. Це може включати ретельний аналіз існуючих нормативних вимог у відповідній галузі, консультації з регуляторними органами, а також розробку додаткових механізмів контролю та аудиту, які б дозволяли відстежувати та підтверджувати дотримання встановлених правил та процедур.

З іншого боку, розвиток технології смарт-контрактів також ставить перед регуляторами нові виклики та вимагає модернізації існуючих правових рамок. Зокрема, необхідно виробити чіткі та зрозумілі правила щодо правового статусу смарт-контрактів, їх юридичної сили та механізмів вирішення спорів. Важливо забезпечити, щоб ці правила, з одного боку, створювали сприятливі умови для інновацій та ефективного використання нових технологій, а з іншого – надійно захищали права та інтереси всіх залучених сторін [6].

Окрім правових аспектів, важливим фактором безпеки смарт-контрактів у публічному секторі є також забезпечення належного рівня конфіденційності та захисту персональних даних. Враховуючи, що багато додатків на основі смарт-контрактів можуть оперувати чутливою інформацією про громадян,

такою як їхні ідентифікаційні дані, медичні записи, фінансова інформація тощо, надзвичайно важливо забезпечити відповідність цих рішень вимогам законодавства про захист даних, зокрема GDPR.

Це передбачає впровадження надійних механізмів шифрування та контролю доступу до даних, використання передових методів анонімізації та псевдонімізації, а також забезпечення можливості для користувачів реалізувати свої права, такі як право на доступ до своїх даних, їх виправлення або видалення. При розробці смарт-контрактів необхідно враховувати вимоги щодо конфіденційності та захисту даних вже на етапі проєктування архітектури рішення.

Ще одним важливим аспектом забезпечення безпеки смарт-контрактів у публічному секторі є управління ключами та ідентифікацією користувачів. Зважаючи на те, що доступ до функціоналу смарт-контрактів та можливість ініціювати транзакції зазвичай контролюються за допомогою криптографічних ключів, ефективне управління цими ключами стає критично важливим для запобігання несанкціонованому доступу та шахрайським діям.

Організаціям, які впроваджують рішення на основі смарт-контрактів, необхідно розробити та дотримуватись чітких політик та процедур управління ключами, що регламентують їх створення, зберігання, використання та знищення. Особливу увагу слід приділяти безпеці приватних ключів, які по суті є найслабшою ланкою в системі і можуть стати об’єктом атак зловмисників. Зберігання приватних ключів на апаратних носіях, використання схем розподілу секрету та мультипідпису, а також регулярна ротація ключів – це лише деякі з рекомендованих практик для мінімізації ризиків.

Також важливо забезпечити надійну ідентифікацію та автентифікацію користувачів смарт-контрактів, особливо коли мова йде про додатки, що надають доступ до чутливих даних або дозволяють здійснювати юридично значущі дії. Впровадження таких механізмів, як двофакторна автентифікація, використання цифрових підписів та сертифікатів, а також інтеграція з

існуючими системами електронної ідентифікації (наприклад, Mobile ID або цифрові паспорти) можуть значно підвищити рівень безпеки та довіри до блокчейн-рішень у публічній сфері.

Нарешті, не можна недооцінювати роль людського фактору у забезпеченні безпеки смарт-контрактів. Як би ретельно не були розроблені та перевірені технічні рішення, вони все одно можуть бути вразливими до помилок або зловмисних дій з боку людей, які з ними взаємодіють – розробників, адміністраторів, користувачів. Саме тому надзвичайно важливо приділяти належну увагу навчанню та підвищенню обізнаності всіх залучених сторін щодо потенційних ризиків та кращих практик безпеки.

Розробники смарт-контрактів повинні постійно вдосконалювати свої навички та бути в курсі останніх досягнень і рекомендацій в сфері безпечної розробки блокчейн-рішень. Адміністратори та операційний персонал повинні чітко розуміти свої обов’язки та дотримуватись встановлених політик безпеки при роботі з смарт-контрактами. А користувачі повинні бути поінформовані про основні правила «цифрової гігієни», такі як безпечне зберігання приватних ключів, використання надійних каналів зв’язку, перевірка автентичності джерела даних тощо.

Підвищення цифрової грамотності та культури кібербезпеки серед усіх учасників екосистеми блокчейн-рішень у публічному секторі є запорукою мінімізації ризиків, пов’язаних з людським фактором, і, відповідно, забезпечення загальної надійності та стійкості цих систем.

Висновки та перспективи подальших розвідок у даному напрямі. Забезпечення безпеки смарт-контрактів є ключовим фактором успішного впровадження блокчейну в публічному управлінні. Дотримання стандартів безпечного програмування та регулярний експертний аудит коду смарт-контрактів дозволить мінімізувати ризики експлуатації вразливостей і створить надійний фундамент для розгортання блокчейн рішень в публічному секторі.

Реалізація запропонованих практик з аналізу вразливостей, впровадження стандартів безпечної розробки та комплексної методології аудиту, дозволить органам публічної влади контрольовано і безпечно застосовувати переваги смарт-контрактів для оптимізації управлінських процесів, підвищення прозорості та довіри у взаємодії з громадянами і бізнесом.

Темою для подальших досліджень має стати аналіз практичних кейсів з покращення безпеки впровадження смарт-контрактів у публічному секторі.

Література

1. Hofmann, Erik, Urs Magnus Strewe, and Nicola Bosia, “Supply Chain Finance and Blockchain Technology: The Case of Reverse Securitisation.” Science Research International. 2018. 2. Pp. 235–249.
2. Khaqqi, Khairul Azmi, Juho Järvinen, Dimitrios Pammet, and Tapio Systä, “Incorporating Seller/Buyer Reputation-Based System in Blockchain-Enabled Emission Trading Application.” Journal of Cleaner Production. 2018. 205. Pp. 103–116.
3. Ølnes, Svein, Jolien Ubacht, and Marijn Janssen, “Blockchain in Government: Benefits and Implications of Distributed Ledger Technology for Information Sharing.” Government Information Quarterly. 2017. 34. Pp. 355–364.
4. Pazaitis, Alex, Primavera De Filippi, and Vasilis Kostakis, “Blockchain and Value Systems in the Sharing Economy: The Illustrative Case of Backfeed.” Technological Forecasting and Social Change. 2017. 125. Pp. 105–115.
5. Sun, Tao, and Jianming Ye, “A Blockchain-Based Smart Contract for the Electric Vehicle Charging System.” IEEE Access. 2019. 7. Pp. 546–558.
6. Tan, Edwin, Sante Mahula, and Joep Crompvoets, “Blockchain Governance in the Public Sector: A Conceptual Framework for Public Management.” Government Information Quarterly. 2021. 3. Pp. 325–333.

7. Zheng, Zibin, Shaoan Xie, Hong-Ning Dai, Xiangping Chen, and Huaimin Wang, “Blockchain Challenges and Opportunities: A Survey.” International Journal of Web and Grid Services. 2018.14. Pp. 352–375.

References

1. Hofmann, E., Strewe, U. M., & Bosia, N. (2018), “Supply Chain Finance and Blockchain Technology: The Case of Reverse Securitisation”, *Science Research International*, vol. 2, pp. 235–249.

2. Khaqqi, K. A., Järvinen, J., Pammet, D., & Systä, T. (2018), “Incorporating Seller/Buyer Reputation-Based System in Blockchain-Enabled Emission Trading Application”, *Journal of Cleaner Production*, vol. 205, pp. 103–116.

3. Ølnes, S., Ubacht, J., & Janssen, M. (2017), “Blockchain in Government: Benefits and Implications of Distributed Ledger Technology for Information Sharing”, *Government Information Quarterly*, vol. 34, pp. 355–364.

4. Pazaitis, A., De Filippi, P., & Kostakis, V. (2017), “Blockchain and Value Systems in the Sharing Economy: The Illustrative Case of Backfeed”, *Technological Forecasting and Social Change*, vol. 125, pp. 105–115.

5. Sun, T., & Ye, J. (2019), “A Blockchain-Based Smart Contract for the Electric Vehicle Charging System”, *IEEE Access*, vol. 7, pp. 546–558.

6. Tan, E., Mahula, S., & Crompvoets, J. (2021), “Blockchain Governance in the Public Sector: A Conceptual Framework for Public Management”, *Government Information Quarterly*, vol. 3, pp. 325–333.

7. Zheng, Z., Xie, S., Dai, H.-N., Chen, X., & Wang, H. (2018), “Blockchain Challenges and Opportunities: A Survey”, *International Journal of Web and Grid Services*, vol. 14, pp. 352–375.

Стаття надійшла до редакції 23.04.2025 р.