№ 6(34) 2024
НАУКА і ТЕХНІКА СЬОГОДНІ
серії: право, економіка, педагогіка, техніка, фізико-математичні науки

УДК 004.056:004.7:658.5

https://doi.org/10.52058/2786-6025-2024-6(34)-958-970

Лучко Юлія Іванівна кандидат педагогічних наук, доцент кафедри правових та інформаційних технологій, Відокремлений структурний підрозділ закладу вищої освіти «Відкритого міжнародного університету розвитку людини «Україна» Хмельницький інститут соціальних технологій, вул. Заводська, 63/1, м. Хмельницький, 29007, https://orcid.org/0000-0002-2714-9425

Кульчій Інна Олексіївна кандидат наук з державного управління, доцент, завідувач кафедрою публічного управління, адміністрування та права, Національний університет «Полтавська політехніка імені Юрія Кондратюка», вул. Анни Ярославни, 8-А, м. Полтава, 36003, https://orcid.org/0000-0002-0063-6493

Іваненко Руслан Олександрович старший науковий співробітник, Український науково-дослідний інститут спеціальної техніки та судових експертиз, вул. Володимирська, 33, м. Київ, 01601, https://orcid.org/0000-0002-1447-6275

РОЛЬ БЛОКЧЕЙН ТЕХНОЛОГІЙ У ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ

Анотація. Роль блокчейн технологій у забезпеченні кібербезпеки визначається їх здатністю до створення безпечних і незмінних записів даних. Використання децентралізованої архітектури блокчейну дає змогу уникнути централізованих точок вразливості, підвищуючи стійкість до кібератак. Це дослідження спрямоване на розкриття ролі блокчейн технологій у забезпеченні кібербезпеки, а також наданні рекомендацій, які допоможуть захистити їх від атак або пом'якшити їх наслідки. Дослідження проведено за допомогою загальнонаукових методів, зокрема використано методи систематизації, опису й узагальнення, метод порівняння, а також методи індукції і дедукції. З'ясовано, що кількість кібератак і кіберзлочинів в Україні постійно зростає, охоплюючи різні сфери діяльності, тому використання блокчейн технологій набуває все більшою розповсюдженості серед українських компаній. Окреслено, що технологія блокчейну базується на трьох основних принципах, які відрізняють її від інших технологій: децентралізація, незмінність, прозорість. Визначено, що роль блокчейн технологій проявляється через сукупність його можливостей, таких як: децентралізація, цілісність даних і прозорість, криптографічний захист, автоматизація через смарт-контракти, незмінність даних, стійкість до DDoS-

атак, підвищена ефективність й відсутність посередників тощо. Також в процесі дослідження було надано рекомендації, які допоможуть захистити блокчейн технології від атак, такі як використання управління, специфічного для блокчейн технологій, що забезпечує підтримку цілісності й доступності інформації, мінімізація даних у ланцюжку, застосування криптографічних алгоритмів для захисту даних від несанкціонованого доступу і проведення ретельного аудиту безпеки. Подальші дослідження можуть бути спрямовані на вдосконалення механізмів захисту від нових типів кіберзагроз, враховуючи динамічний характер технологій блокчейну та постійні зміни у кібербезпеці.

Ключові слова: кіберзагрози, кібератаки, децентралізованість, незмінність, прозорість, криптографічний захист, смарт-контракти.

Luchko Yuliia Ivanivna Candidate in Pedagogy, Associate Professor Department of Legal and Information Technology, Separate Structural Subdivision of the Higher Education Institution «Open International University of Human Development «Ukraine» Khmelnytskyi Institute of Social Technologies, St. Zavodska, 63/1, Khmelnytskyi, 29007, https://orcid.org/0000-0002-2714-9425

Kulchii Inna Oleksiivna Candidate of Public Administration, Associate Professor, Head of the Department of Public Management, Administration and Law, National University «Yuri Kondratyuk Poltava Polytechnic», St. Anna Yaroslavna, 8-A, Poltava, 36003, https://orcid.org/0000-0002-0063-6493

Ivanenko Ruslan Oleksandrovych Senior Research Scientist, The Ukrainian Scientific and Research Institute of Special Equipment and Forensic Expertise, St. Volodymyrska, 33, Kyiv, 01601, https://orcid.org/0000-0002-1447-6275

THE ROLE OF BLOCKCHAIN TECHNOLOGY IN ENSURING CYBERSECURITY

Abstract. The role of blockchain technologies in ensuring cybersecurity is determined by their ability to create secure and immutable data records. The use of a decentralised blockchain architecture avoids centralised points of vulnerability, increasing resilience to cyberattacks. This study aims to reveal the role of blockchain technologies in ensuring cybersecurity, as well as provide recommendations that will help protect them from attacks or mitigate their consequences. The study was conducted using general scientific methods, in particular, the methods of systematisation, description and generalisation, the method of comparison, as well as the methods of induction and deduction. It is found that the number of cyberattacks and cybercrimes in Ukraine is constantly growing, covering various areas of activity, so the use of blockchain technologies is becoming increasingly

common among Ukrainian companies. It is outlined that blockchain technology is based on three main principles that distinguish it from other technologies: decentralisation, immutability, and transparency. It is determined that the role of blockchain technology is manifested through a combination of its capabilities, such as: decentralisation, data integrity and transparency, cryptographic protection, automation through smart contracts, data immutability, resistance to DDoS attacks, increased efficiency and absence of intermediaries, etc. The study also provided recommendations that will help protect blockchain technologies from attacks, such as the use of blockchain-specific controls to maintain the integrity and availability of information, minimising data in the chain, using cryptographic algorithms to protect data from unauthorised access, and conducting a thorough security audit. Further research may be aimed at improving mechanisms to protect against new types of cyber threats, given the dynamic nature of blockchain technologies and constant changes in cybersecurity.

Keywords: cyber threats, cyber attacks, decentralisation, immutability, transparency, cryptographic protection, smart contracts.

Постановка проблеми. Блокчейн технологія, спочатку відома як основа для криптовалют, набула значної уваги завдяки своїм унікальним властивостям і потенціалу для трансформації багатьох сфер діяльності, включаючи кібербезпеку. У сучасному цифровому світі, де інформаційні системи й дані стають цінішими за традиційні ресурси, питання кібербезпеки виходить на перший план. Адже кібератаки стають дедалі складнішими й частішими, що ставить під загрозу конфіденційність, цілісність і доступність даних. У цьому контексті блокчейн технології виступають, як перспективна технологія для покращення захисту інформаційних систем.

Отже, одним з ключових аспектів блокчейну є його здатність до забезпечення цілісності даних і невідворотності записів, що є важливим у кібербезпеці. Використання смарт-контрактів дає змогу автоматизувати процеси контролю й верифікації, що підвищує ефективність системи і знижує людський фактор. Усе це робить блокчейн привабливим інструментом для організацій, які прагнуть підвищити рівень кібербезпеки й захистити свої дані від кібератак.

Аналіз останніх досліджень і публікацій. Зацікавленість цією проблемою засвідчують численні праці сучасних закордонних і вітчизняних авторів. Так, Яровенко Г. та Ковач В. досліджували перспективи використання блокчейну у системах кібербезпеки банків, підкреслюючи потенціал цієї технології для захисту фінансових установ [1].

В своєму науковому дослідженні Балацька В. та Опірський І. здійснили аналіз можливостей блокчейну для забезпечення конфіденційності персональних даних і підтримки кібербезпеки, демонструючи, як ця технологія може бути інтегрована у сучасні системи захисту інформації [2].

Цікаві погляди надали в своєму науковому дослідженні Mir,S. та інші. Автори в своїй статті представили концепцію блокчейн-орієнтованої федеративної ідентичності й аудиту, підкреслюючи важливість блокчейну у забезпеченні надійного управління ідентифікацією й збереженням цілісності даних [3].

Куліковський А. описував блокчейн як складову інформаційної безпеки, акцентуючи увагу на його ролі у захисті від кіберзагроз [4].

Автори Lee S. та Kim S. дослідили можливості й виклики використання блокчейну як засобу кіберзахисту, пропонуючи огляд сфер застосування й перспектив розвитку цієї технології [5].

Шахматов І. О. розглядав блокчейн як інструмент протидії неправомірному використанню доступу до вебсайтів, що підкреслює актуальність цієї технології для захисту онлайн-ресурсів [6].

Таким чином, незважаючи на те, що останнім часом зростає кількість наукових робіт, присвячених окресленій проблематиці, залишаються недостатньо досліджуваними роль блокчейн у забезпеченні кібербезпеки.

Мета статті полягає в розкритті ролі блокчейн технологій у забезпеченні кібербезпеки, а також наданні рекомендацій які допоможуть захистити блокчейн технології від атак, або пом'якшити їх наслідки.

Згідно мети перед дослідженням постають такі завдання:

- дати оцінку сучасному стану кіберзлочинів і кібератак в Україні;
- з'ясувати особливості блокчейн технологій, а також систематизувати можливості і ризики від їх використання у забезпеченні кібербезпеки;
- надати рекомендації, які допоможуть захистити блокчейн технології від атак, або пом'якшити їх наслідки.

Виклад основного матеріалу. Кібербезпека в Україні регулюється законодавчими і організаційними нормами, спрямованими на захист національних інтересів у кіберпросторі, визначеними Законом України «Про основні засади забезпечення кібербезпеки України» [7]. Цей закон ставить на меті захист важливих інтересів громадян, суспільства й держави в кіберпросторі. Він встановлює цілі, напрями і принципи державної політики у сфері кібербезпеки, а також визначає повноваження державних органів, підприємств, установ, організацій та громадян.

Останніми роками Україна дедалі більше стикається з масштабними кібератаками та їх негативними наслідками. Зокрема, кількість кримінальних правопорушень у сфері інформаційних технологій постійно зростає. За даними Генеральної прокуратури України, станом на 31 грудня 2022 року було зареєстровано 3415 кримінальних правопорушень у сфері інформаційних технологій, що на 105 випадків більше, порівняно з 2021 роком та на 917 випадків більше порівняно з 2020 роком. Це свідчить про суттєве зростання кількості зареєстрованих кримінальних правопорушень: на 3,1% порівняно з 2021 роком та на 26,8% порівняно з 2020 роком [8].

Також варто додати, що за даними урядової команди реагування на комп'ютерні надзвичайні події CERT-UA, у 2023 році було зафіксовано близько 900 кібератак (рис. 1).

Рис. 1 Кількість кібератак по різним сферам України за 2023 рік, од.
Джерело: складено авторами на основі [9]

Отже, як можна побачити, кількість кібератак і кіберзлочинів в Україні постійно зростає, вони охоплюють різні сфери діяльності і спричиняють збитки компаніям. Тому вкрай важливо захищати інформаційні системи якісними інструментами захисту.

Сьогодні однозначного визначення блокчейну не існує. Зазвичай його описують як вдосконалений механізм баз даних, який дає змогу прозоро обмінюватися інформацією в мережі [5]. База даних блокчейну буквально зберігає дані в блоках, які пов'язані між собою в ланцюжок, тобто дані є хронологічно послідовними, тож ніщо не може бути видалене або змінене в ланцюжку без консенсусу в мережі. Оскільки блоки пов'язані між собою, записи не можуть бути вилучені, змінені, або відредаговані, так як це призведе до порушення структури блокчейну [3].

Також необхідно додати, що блокчейн-технології забезпечують децентралізовану і розподілену структуру зберігання даних, що робить його стійким до атак і маніпуляцій. Завдяки криптографічним алгоритмам і механізмам консенсусу, блокчейн забезпечує високий рівень захисту даних,

які зберігаються в його ланцюгах, що дозволяє значно зменшити ризики несанкціонованого доступу та змін, а також підвищити прозорість і довіру до системи.

Загалом, технологія блокчейну базується на трьох ключових принципах, які відрізняють її від інших технологій (рис. 2), та охоплюють певні аспекти кібербезпеки.

Рис. 2 Основні принципи блокчейн технологій у кібербезпеці

Децентралізація є ефективним засобом проти фальсифікації баз даних. У централізованих мережах з головним центром, зловмисникам достатньо завдати шкоди цьому центру, оскільки він є єдиною точкою відмови. В децентралізованій мережі цей підхід не працює, оскільки дані зберігаються розподілено. Для модифікації даних необхідно змінити їх у кожного учасника мережі, а це вимагає, щоб більшість учасників підтвердили та внесли ці зміни до ланцюга, що є вкрай складним завданням [10].

Прозорість також є однією з основних характеристик блокчейн-технології, яка значно підвищує рівень довіри і безпеки. У публічних блокчейнах всі транзакції є видимими для кожного учасника мережі, що дає змогу здійснювати перевірку та аудит даних у будь-який момент. Така відкритість забезпечує можливість відстеження всіх операцій від початку до кінця, що ускладнює можливість здійснення шахрайських дій або приховування змін. Прозорість блокчейну створює середовище, де будь-яка спроба маніпуляції або несанкціонованого доступу до даних стає швидко виявленою.

Незмінність є однією з найважливіших властивостей блокчейну, яка забезпечує збереження цілісності й достовірності даних. Після того як дані записані в блокчейн, вони не можуть бути змінені або видалені без внесення змін до всіх наступних блоків у ланцюзі. Це досягається завдяки криптографічним методам, які пов'язують кожен блок з попереднім через унікальні хеші. Така структура гарантує, що будь-яка спроба зміни даних в одному блоці потребує переобчислення хешів і повторного погодження всіх наступних блоків, що є надзвичайно складним і ресурсомістким завданням. Незмінність блокчейну забезпечує високий рівень захисту від фальсифікації

та несанкціонованих змін, роблячи його надійним інструментом для зберігання важливих даних.

Отже, такі властивості блокчейн технологій забезпечують високий рівень захисту від фальсифікації, несанкціонованого доступу й інших кіберзагроз, роблячи блокчейн надійним рішенням для збереження важливої інформації в умовах сучасних кіберзагроз.

За даними Marketsand Markets, у 2022 році світовий ринок блокчейну становив близько $7,4 млрд, а до кінця 2027 року він має згенерувати понад $94 млрд із середньорічним темпом зростання (CAGR) 66,2% (рис.3.) . Північна Америка наразі є домінуючим регіоном на світовому ринку блокчейну.

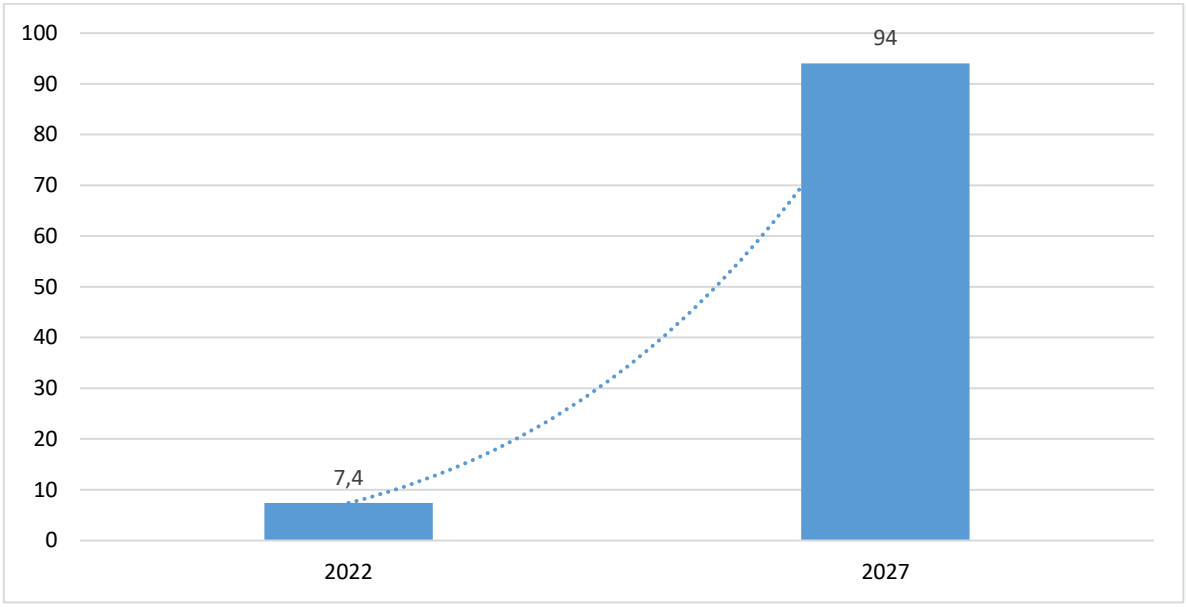

Рис. 3 Об'єм світового ринку блокчейн-технологій у 2022 і у прогнозному 2027 рр., млрд. долл.

Джерело: складено авторами на основі [11]

Отже, технологія блокчейн набуває великих обертів, що свідчить постійно зростаючі об'єми світового ринку блокчейн-технологій.

Спеціалісти компанії PwC стверджують, що 61% сучасних компаній зараз ставлять ініціативи з цифрової трансформації на перше місце в списку пріоритетів свого розвитку, а блокчейн дає змогу задовольнити зростаючий попит на кращу безпеку і прозорість у бізнесі.

Роль блокчейн-технологій у забезпеченні кібербезпеки проявляється через сукупність його можливостей і ризиків (табл. 1).

Таблиця 1.

Можливості і ризики застосування блокчейн-технологій у забезпеченні кібербезпеки

№	Можливості	Ризики
1	2	3
1	Децентралізація – блокчейн є розподіленою системою, що зберігає дані на багатьох вузлах, отже це усуває єдину точку відмови і робить систему стійкою до атак, які спрямовані на центральні сервери	Децентралізація управління – хоча децентралізація є однією з основних переваг блокчейну, вона також може створювати проблеми з управлінням і прийняттям рішень. Відсутність централізованого контролю може ускладнити процес впровадження змін та вирішення конфліктів.
2	Цілісність даних – кожен блок у блокчейні містить хеш попереднього блоку, що створює ланцюг записів, отже це забезпечує неможливість несанкціонованого змінення даних, оскільки будь-яка спроба змінити інформацію в одному блоці потребувала б змінити всі наступні блоки, що практично неможливо	Масштабованість – блокчейн-технології можуть мати проблеми з масштабуванням, особливо в мережах з високим обсягом транзакцій. Збільшення кількості учасників може призвести до уповільнення транзакцій та підвищення витрат на обробку даних.
3	Прозорість та відстежуваність – кожен блок у блокчейні містить хеш попереднього блоку, що створює ланцюг записів, отже це забезпечує неможливість несанкціонованого змінення даних, оскільки будь-яка спроба змінити інформацію в одному блоці потребувала б змінити всі наступні блоки, що практично неможливо	Енергоспоживання – деякі блокчейн-мережі, такі як Bitcoin, потребують значних обчислювальних ресурсів для підтримки процесу майнінгу й верифікації транзакцій, що призводить до високого енергоспоживання. Це може бути екологічно несприятливим і економічно затратним.
4	Криптографічний захист – блокчейн використовує складні криптографічні алгоритми для захисту даних, що забезпечує високий рівень безпеки. Це ускладнює кібератаки і робить дані в блокчейні дуже важкодоступними для хакерів.	Криптографічні ризики – хоча блокчейн використовує передові криптографічні методи для забезпечення безпеки, існує ризик того, що майбутні прориви в області квантових обчислень або інші технологічні досягнення можуть скомпрометувати поточні криптографічні стандарти.
5	Автоматизація і смарт-контракти – смарт-контракти дають змогу автоматизувати виконання угод та інших процесів, що мінімізує людський фактор та знижує ризики помилок і шахрайства. Вони виконуються автоматично, коли виконуються умови, закладені в коді контракту	Безпека смарт-контрактів – смарт-контракти є програмним кодом, який автоматично виконує певні дії при дотриманні встановлених умов. Однак помилки в коді або уразливості можуть бути використані для атак, що може призвести до фінансових втрат або інших негативних наслідків.

Продовження таблиці 1

1	2	3
6	Незмінність – записи в блокчейні є незмінними, що означає, що після додавання інформації до ланцюга її не можна змінити або видалити. Це забезпечує високу надійність та довіру до даних, що зберігаються в системі.	Відсутність зворотності – транзакції в блокчейні є незворотними, що означає, що помилкові або шахрайські транзакції не можуть бути відмінені, що створює ризики для користувачів, особливо у випадках людської помилки або соціальної інженерії.
7	Стійкість до DDoS-атак – Завдяки розподіленій природі блокчейну, атаки типу DDoS (розподілені атаки відмови в обслуговуванні) стають менш ефективними, оскільки атакувати одночасно всі вузли мережі практично неможливо	Регуляторні питання – блокчейн є новою технологією, і її правовий статус у багатьох країнах ще не визначений. Відсутність чітких регуляторних рамок може створювати правову невизначеність і ризики для компаній та користувачів.
8	Підвищена ефективність та зниження витрат - використання блокчейну зменшує витрати на управління й безпеку даних, оскільки багато процесів автоматизуються, а потреба в посередниках зменшується	Складність інтеграції - інтеграція блокчейн-технологій в існуючі системи є складною та дорогою, що потребує значних ресурсів та технічних знань, і може бути бар'єром для багатьох організацій.
9	Відсутність посередників – технологія блокчейн дає змогу усунути необхідність використання посередників, оскільки інформація зберігається та підтверджується всіма учасниками мережі, що зменшує ризики шахрайства.	
10	Контроль доступу та приватність – блокчейн дає змогу контролювати доступ до даних і забезпечує їхню приватність, що особливо важливо при роботі з конфіденційною інформацією або комерційною таємницею	.

Джерело: створено авторами [1;6;12]

Отже, вищеназвані переваги роблять блокчейн-технології перспективним інструментом для покращення кібербезпеки в різних галузях, включаючи фінансовий сектор, охорону здоров'я, урядові установи, енергетику та багато інших. Проте існуючи ризики підкреслюють важливість ретельного планування й аналізу перед впровадженням блокчейн-технологій у сферу кібербезпеки. Організації мають зважувати потенційні вигоди проти можливих викликів, щоб прийняти обґрунтоване рішення щодо використання блокчейну.

Однак останнім часом зростає занепокоєння щодо безпеки блокчейну, особливо через те, що ця технологія вважається більш вразливою до атаки «51%» (коли хакери намагаються здійснити контроль над більшістю

мережевої потужності, або хешрейту, мережі, що дає їм змогу змінювати транзакції і поділитися на дві різні гілки блокчейну, що призводить до подвійного витрачання та інших атак). Найбільшим відомим прикладом цього стала атака Pancake Bunny у травні 2021 року, яка призвела до втрати криптовалютних активів на суму понад 200 мільйонів доларів. Кіберзлочинці можуть викрадати ключі безпеки і переводити активи з гаманців, що належать системі, а також визнавати недійсними нові транзакції і модифікувати нові блоки [13]. Протягом 2022 року сума збитків внаслідок атак на блокчейни перевищила 9 млрд. долл. Протягом цього року було зареєстровано найвищу кількість атак з усіх часів існування блокчейну [14].

Отже, незважаючи на високий рівень захисту від традиційних атак хакерів, блокчейн має свої вразливості, які використовуються зловмисниками. Окрім поширеного фішингу, блокчейн стикається з унікальними загрозами, що притаманні саме цій технології: атаки 51%, спроби злому, викрадання закритих ключів, атаки Race та Фінні.

З огляду на це слід надати рекомендації, які допоможуть захистити блокчейн технології від атак, або пом’якшити їх наслідки.

По-перше, необхідно використовувати управління, специфічне для блокчейну. Блокчейн – це поєднання розподіленого реєстру та блокової структури даних, засноване на криптографічній зв’язаності, що дає змогу підтримувати цілісність і доступність інформації. Однак публічна блокчейн-мережа має проблему з конфіденційністю. Для її вирішення з’явилася модель приватного блокчейну, яка має іншу архітектуру. В даному випадку використовується модель доступу до мережі, в якій тільки певні учасники можуть вносити зміни до реєстру. У мережі є оператор, тому вона залишається розподіленою, але не може вважатися децентралізованою. За рахунок цього підвищується конфіденційність записів, адже доступ надається згідно з політиками безпеки.

По-друге, варто мінімізувати дані в ланцюжку, що є відомою практикою для зменшення ризику атак. Однак, додаткові заходи безпеки до інших об'єктів можуть допомогти подолати потенційні загрози. Застосування криптографічних алгоритмів для захисту даних від несанкціонованого доступу, ефективне керування й захист ключів, використання надійних алгоритмів консенсусу, захист смарт-контрактів та вузлів мережі - це основні заходи, спрямовані на забезпечення безпеки даних у блокчейні та попередження можливих атак або пом’якшення їх наслідків.

По-третє, для забезпечення безпеки мережі варто вживати заходи, які включають перевірку вузлів та протоколів, регулярний аудит безпеки та вибір надійних постачальників послуг.

В четвертих, необхідно проводити ретельну ідентифікацію користувачів і реалізацію різних рівнів доступу, які можуть допомогти у запобіганні

несанкціонованому доступу до програм. Наприклад, у приватних блокчейнах можуть бути встановлені «білі» списки користувачів, що дасть змогу обмежити доступ лише до авторизованих осіб.

По-п’яте, потрібно використовувати довірених аудиторів та третіх осіб, що виявляється ефективним методом забезпечення безпеки блокчейну та смарт-контрактів. Ретельний аудит дає змогу виявити потенційні вразливості у системі. Такі аудитори часто є компетентними організаціями з високим рівнем довіри від клієнтів. Наприклад, компанія H-X Technologies спеціалізується на аудиті систем на відповідність вимогам безпеки, а також перевірці смарт-контрактів та вихідного коду для виявлення можливих загроз.

Висновки. Таким чином, сучасний стан кіберзлочинів і кібератак в Україні потребує уваги, оскільки вони стають все більш поширеними та складними, вимагаючи посилення заходів з кібербезпеки. В цьому контексті блокчейн технології набувають великого значення, оскільки їхні особливості, такі як децентралізація, криптографічний захист і незмінність даних, можуть допомогти у забезпеченні надійності та цілісності інформації, а також попередженні та виявленні кіберзлочинів та кібератак. В статті було з'ясовано, що роль блокчейн технологій проявляється через сукупність їх можливостей, а саме: децентралізація, що усуває єдину точку відмови і забезпечує стійкість до атак; цілісність даних, що гарантує неможливість несанкціонованого змінення інформації; прозорість та відстежуваність, які забезпечують історію змін даних та можливість перевірки кожної транзакції; автоматизація та смарт-контракти, що дозволяють автоматизувати процеси та угоди з мінімізацією людського втручання тощо. Авторами було надано рекомендації щодо забезпечення безпеки блокчейн технологій, які включають використання управління, специфічного для блокчейну, мінімізацію даних у ланцюжку, ретельний аудит безпеки, а також використання довірених аудиторів та третіх осіб для виявлення потенційних вразливостей у системі. Практична значимість результатів дослідження полягає в тому, що вони надають конкретні рекомендації щодо захисту блокчейн технологій від потенційних атак або пом'якшення їх наслідків.

Література:

1. Яровенко Г., Ковач В. Перспективи застосування технології блокчейн у системах забезпечення кібербезпеки банків. *Підприємництво та інновації* 2020. (12), 206-214. https://doi.org/10.37320/2415-3583/12.36

2. Балацька В., Опірський І. Забезпечення конфіденційності персональних даних і підтримки кібербезпеки за допомогою блокчейну. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»,* 2023. 4(20), 6–19. https://doi.org/10.28925/2663-4023.2023.20.619

3. Mir,S., Capretz,M.A. M., Grolinger,K., ElYamany,H.F., ElGayyar,M.M. Blockchain-based federated identity and auditing.International Journal of Blockchains and Cryptocurrencies, 2020. 1(2), 179.https://doi.org/10.1504/ijbc.2020.10031109

4. Куліковський А. Технологія blockchain як складова інформаційної безпеки. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»,* 2019. 4(4), 85–89. https://doi.org/10.28925/2663-4023.2019.4.8589

5. Lee S., Kim S. Blockchain as a cyber defense: Opportunities, applications, and challenges. *IEEE Access,* PP(99), 2021. 1-1. https://doi.org/10.1109/ACCESS.2021.3136328

6. Шахматов І. О. Технологія blockchain як інструмент протидії неправомірному використанню доступу до вебсайтів. *Державний університет інформаційно-комунікаційних технологій,* 2024. (1) . https://doi.org/10.31673/2412-9070.2024.012025

7. Про основні засади забезпечення кібербезпеки України- Закон України № 2163-VIII від 05.10.2017, поточна редакція від 04.04.2024 https://zakon.rada.gov.ua/laws/show/2163-19#Text

8. Звіт про результати роботи Департаменту кіберполіції у 2022 році. 2023. https://cyberpolice.gov.ua/news/zvit-pro-rezultaty-roboty-departamentu-kiberpolicziyi-u--roczi-969/

9. Жарікова А. Кількість кібератак у 2023 році зросла на 16% - Держспецзв'язку. 2024. URL: https://www.epravda.com.ua/news/2024/01/31/709355/

10. Четверіков, І.О., & Петренко, А.І. (2024). Технологія Blockchain в системі захисту інформації. Blockchain Technology in the Information Security System. *Державний університет телекомунікацій*. UDK: 004.056. DOI: 10.33111/mise.99.14

11. Blockchain Statistics: Top Stats, Facts and Trends for 2024. https://connect.comptia.org/blog/blockchain-statistics

12. Павлюк А. В., Луценко М. М. Аналіз механізмів захисту технології блокчейн від кібератак. *Сучасний захист інформації*, 2022. 2. https://doi.org/10.31673/2409-7292.2022.025969

13. Behnke, R. (2021). Explained: The PancakeBunny protocol hack. Retrieved from https://www.halborn.com/blog/post/explained-the-pancakebunny-protocol-hack-may-2021

14. Мащенко С. 8 найкращих практик для забезпечення безпеки блокчейну. 2023. https://www.h-x.technology/ua/blog-ua/8-best-practices-for-blockchain-security-ua

References:

1. Yarovenko, H., & Kovach, V. (2020). Perspektyvy zastosuvannia tekhnolohii blokchein u systemakh zabezpechennia kiberbezpeky bankiv [Prospects for the use of blockchain technology in banking cybersecurity systems]. *Pidpryiemnytstvo ta innovatsii - Entrepreneurship and Innovation*, (12), 206-214. https://doi.org/10.37320/2415-3583/12.36 (in Ukrainian)

2. Balatska, V., & Opirskyi, I. (2023). Zabezpechennia konfidentsiinosti personalnykh danykh i pidtrymky kiberbezpeky za dopomohoiu blokcheinu [Ensuring the confidentiality of personal data and cybersecurity support using blockchain]. *Elektronne fakhove naukove vydannia "Kiberbezpeka: osvita, nauka, tekhnika" - Electronic Professional Scientific Edition "Cybersecurity: Education, Science, Technology",* 4(20), 6–19. https://doi.org/10.28925/2663-4023.2023.20.619 (in Ukrainian)

3. Mir, S., Capretz, M. A. M., Grolinger, K., ElYamany, H. F., & ElGayyar, M. M. (2020). Blockchain-based federated identity and auditing. *International Journal of Blockchains and Cryptocurrencies,* 1(2), 179. https://doi.org/10.1504/ijbc.2020.10031109 (in English)

4. Kulikovskyi, A. (2019). Tekhnolohiia blockchain yak skladova informatsiinoi bezpeky [Blockchain technology as a component of information security]. *Elektronne fakhove naukove vydannia "Kiberbezpeka: osvita, nauka, tekhnika" - Electronic Professional Scientific Edition "Cybersecurity: Education, Science, Technology"*, 4(4), 85–89. https://doi.org/10.28925/2663-4023.2019.4.8589 (in Ukrainian)

5. Lee S., Kim S. Blockchain as a cyber defense: Opportunities, applications, and challenges. IEEE Access, PP(99), 2021. 1-1. https://doi.org/10.1109/ACCESS.2021.3136328 (in English)

6. Shakhmatov, I. O. (2024). Tekhnolohiia blockchain yak instrument protydii nepravomirnomu vykorystanniu dostupu do vebsaitiv [Blockchain technology as a tool to combat unauthorized website access]. *Derzhavnyi universytet informatsiino-komunikatsiinykh tekhnolohii - State University of Telecommunications*, (1). https://doi.org/10.31673/2412-9070.2024.012025 (in Ukrainian)

7. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy- Zakon Ukrainy № 2163-VIII vid 05.10.2017, potochna redaktsiia vid 04.04.2024 [On the basic principles of ensuring cybersecurity of Ukraine - Law of Ukraine No. 2163-VIII dated 05.10.2017, current version dated 04.04.2024]. Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text (in Ukrainian)

8. Zvit pro rezultaty roboty Departamentu kiberpolitsii u 2022 rotsi [Report on the results of the Cyber Police Department's work in 2022]. (2023). Retrieved from https://cyberpolice.gov.ua/news/zvit-pro-rezultaty-roboty-departamentu-kiberpolicziyi-u--roczi-969 (in Ukrainian)

9. Zharikova, A. (2024). Kilkist kiberatak u 2023 rotsi zrosla na 16% - Derzhspetszviazku [The number of cyberattacks increased by 16% in 2023 - State Special Communications Service]. Retrieved from https://www.epravda.com.ua/news/2024/01/31/709355/ (in Ukrainian)

10. Chetverikov, I. O., & Petrenko, A. I. (2024). Tekhnolohiia Blockchain v systemi zakhystu informatsii [Blockchain technology in the information security system]. *Derzhavnyi universytet telekomunikatsii - State University of Telecommunications,* m. Kyiv. UDK: 004.056. https://doi.org/10.33111/mise.99.14 (in Ukrainian)

11. CompTIA. (2024). Blockchain statistics: Top stats, facts and trends for 2024. Retrieved from https://connect.comptia.org/blog/blockchain-statistics (in Ukrainian)

12. Pavliuk, A. V., & Lutsenko, M. M. (2022). Analiz mekhanizmiv zakhystu tekhnolohii blokchein vid kiberatak [Analysis of blockchain technology protection mechanisms against cyberattacks]. *Suchasnyi zakhyst informatsii - Modern Information Protection,* (2). https://doi.org/10.31673/2409-7292.2022.025969 (in Ukrainian)

13. Behnke, R. (2021). Explained: The PancakeBunny protocol hack. Retrieved from https://www.halborn.com/blog/post/explained-the-pancakebunny-protocol-hack-may-2021 (in English)

14. Mashchenko S. (2023). 8 naikrashchykh praktyk dlia zabezpechennia bezpeky blokcheĭnu [8 Best Practices for Blockchain Retrieved from https://www.h-x.technology/ua/blog-ua/8-best-practices-for-blockchain-security-ua (in Ukrainian)