УДК: 004.056 DOI 10.33111/mise.99.14

Четверіков І.О., кандидат технічних наук,
доцент кафедри комп'ютерної математики та інформаційної безпеки,
Петренко А.І.,
студентка IV курсу спеціальності «Кібербезпека»,
ДВНЗ «КНЕУ імені Вадима Гетьмана»

Chetverikov I.O., Candidate of Technical Sciences (Ph. D.),
Associate Professor at the
Department of Computer Mathematics and Information Security,
Petrenko A.I.,
4th year student majoring in Cybersecurity,
SHEI KNEU named after V. Hetman

ТЕХНОЛОГІЯ BLOCKCHAIN В СИСТЕМІ ЗАХИСТУ ІНФОРМАЦІЇ

BLOCKCHAIN TECHNOLOGY IN THE INFORMATION SECURITY SYSTEM

Анотація. *Незважаючи на постійне удосконалення технологій захисту даних і створення нових засобів, їх вразливість у сучасних умовах не тільки не зменшується, а й постійно зростає. Це пов'язано з тим, що зловмисники завжди знаходяться на крок попереду від фахівців із захисту, а превентивні заходи не можуть покрити всі можливі вектори атак. Тому актуальність проблем, пов'язаних із захистом інформації, усе більше посилюється.*

Проблема захисту інформації є багатоплановою, комплексною і охоплює ряд важливих завдань. Наприклад, конфіденційність даних, яка забезпечується застосуванням різних методів і засобів (криптогрфічні методи закривають дані від сторонніх осіб, а також вирішують забезпечення їх цілісності); ідентифікація користувачів на основі аналізу кодів, використовуваних ними для підтвердження своїх прав доступу до системи (мережі), на роботу з даними і на їх забезпечення (забезпечується введенням відповідних паролів, використання біометричних даних).

Очевидно, що з часом кількість пристроїв буде тільки зростати, а з ним і питання захисту інформації. Сьогодні найнадійнішими системами контролю доступу до інформації, в яких не використовуються картки, ключі, жетони, паролі і які не можна викрасти або втратити, є біометричні системи контролю доступу до інформації. Однак навіть і біометричні дані можна підробити — наприклад зробити копію відбитка пальця з поверхні і спокійно обійти систему захисту.

Усі сучасні технології захисту інформації є вразливими — більшою чи меншою мірою. Блокчейн є тією технологією, яка за рахунок використання в блоках ланцюжка криптографії, геш-функцій вирішує більшість на сьогоднішній день проблем безпеки. Технологія блокчейн дозволяє вирішити проблему, пов'язану з відсутністю гарантій з боку посередників, які виступають в якості третіх осіб при здійсненні тих чи інших дій.

Технологія блокчейн потенційно здатна забезпечити абсолютну цілісність і конфіденційність, надаючи при цьому особисту інформацію, якщо та необхідна для справи. Таким чином зростає захищеність ресурсу.

Стаття містить огляд основних принципів архітектури технології блокчейн в аспекті використання цієї технології у системі захисту інформації.
Ключові слова: *блокчейн; захист інформації; цілісність; кібератака; цифрова валюта; критерії захищенності.*

Abstract. *Despite the constant improvement of data protection technologies and the creation of new tools, their vulnerability in modern conditions not only does not decrease, but also constantly increases. This is due to the fact that attackers are always one step ahead of cybersecurity specialists, and preventive measures cannot cover all possible vectors of attacks. Therefore, the urgency of issues related to information security is growing.*

The problem of information security is multifaceted, complex and covers a number of important tasks. For example, data confidentiality, which is ensured by the use of various methods and tools (encryption closes data from third parties, as well as solves the problem of their integrity); identification of the user on the basis of the analysis of the codes used by them for confirmation of the rights to access to system (network), to work with data and on their maintenance (it is provided by entering of the corresponding passwords, use of biometric data).

Obviously, over time, the number of devices will only grow, and with it the issue of information security. Today, the most reliable systems for controlling access to information, which do not use cards, keys, tokens, passwords and which cannot be stolen or lost, are biometric systems for controlling access to information. However, even biometric data can be forged — for example, make a copy of a fingerprint from the surface and safely bypass the protection system.

All modern information security technologies are vulnerable — to a greater or lesser extent. Blockchain is a technology that, through the use of cryptography chains and hash functions in blocks, solves most security problems to date. Blockchain technology solves the problem associated with the lack of guarantees from intermediaries who act as third parties in the implementation of certain actions.

Blockchain technology has the potential to provide absolute integrity and confidentiality, while providing personal information if necessary. This increases the security of the resource.

The article provides an overview of the basic principles of the architecture of blockchain technology in terms of the use of this technology in information security.
Keywords: *blockchain; information security; integrity; cyberattack; digital currency; security criteria.*

Вступ: В інформаційну епоху питання безпеки даних стає одним з найважливіших. Здається, що все наше життя відслідковується через бази даних, а наша конфіденційна інформація стала вразливою як ніколи.

З появою кіберпростору організації безупинно виявляють вразливості у своїх мережах і впроваджують нові засоби захисту. Ці заходи мають бути ефективними проти кібератак на основні властивості інформації, що захищається — конфіденційності, цілісності та доступності, а не просто «для галочки».

Постановка проблеми: Сучасні засоби захисту не можуть забезпечити достатній рівень захищенності інформації від компле-

ксу цілеспрямованих атак, які несуть найбільшу загрозу. Найкращим засобом захисту є робота на випередження, тобто зробити так, щоб у злочинця навіть не було змоги скомпрометувати систему. З точки зору цілісності, чудовим рішенням є технологія блокчейн (Blockchain). Саме вона дозволяє забезпечити 100 % захист певних властивостей інформації апріорі, або це вже буде не блокчейн. Саме це твердження і зумовлює **актуальність** обраної теми. Блокчейн може бути застосований для перевірки оновлень, боротьби з DDoS, захисту периметру пристроїв, відмови від паролів, захисту ланцюжків поставок, контролю цілісності політик і конфігурацій, а також для управління ідентифікаційними даними. І це тільки початок, оскільки блокчейн напрямлений на захист цілісності інформації, що є одною із основних властивостей інформації. Атаки на конфіденційність, цілісність і доступність є основним набором зловмисників, за допомогою яких вони шукають слабке місце, щоб потрапити у систему та скомпрометувати її. Блокчейн пропонує абсолютну цілісність, яку неможливо підробити.

Концепцію ланцюжків блоків запропонував у 2008 р. Сатоші Накамото (Satoshi Nakamoto). Вперше реалізована вона була в 2009 році як складова цифрової валюти — Bitcoin, де блокчейн грає роль головного загального реєстру для всіх операцій. Технологія дозволяє організаціям спростити спільні робочі потоки (наприклад, ланцюжки поставок), обмінюючи і відстежуючи ресурси і транзакції в загальному реєстрі (часто називається технологією розподіленого реєстру або DLT).

Аналіз останніх досліджень і публікацій, у яких започатковано розв'язання проблеми створення стійких і надійних розподілених мереж, показав, що науковці Д. Тапскотт, А. Тапскотт, Р. Воттенхофер, Марк Андерсен, Девід Чаум, Адам Бак, Вей Дай, Хел Фінні, Елвуд Шеннон, Фрідріх Касіски, Мартін Хелман, Філіп Цимерман та інші, присвятили різним аспектам технології блокчейну багато уваги та часу [0].

Вперше про блокчейн заговорили з появою цифрових валют. Не дивно, що саме в фінансовій сфері зафіксували різке збільшення наукових досліджень щодо впровадження блокчейну для захисту цифрових активів.

Центральні банки світу за кілька останніх років пройшли шлях від неприйняття самої ідеї до пілотних проектів національної цифрової валюти (central bank digital currency, CBDC).

У [0] Центральний банк цифрових валют виклав свої напрацювання стосовно розвитку потенціалу цифрових валют. На по-

чатку 2020 року в роботу над CBDC — від вивчення питання до реалізації пілотного проекту — були залучені 80 %, або чотири з кожних п'яти центральних банків у країнах, на сукупну частку яких припадає три чверті світового населення і 90 % глобальної економіки.

У вересні — жовтні 2020 року можливість випуску цифрової валюти активно обговорюють центробанки: ФРС США, Європейський ЦБ, Банк Англії, Банк Росії. Йдуть активні обговорення в Національному Банку України.

Сьогодні дослідженнями блокчейну займаються найбільші компанії в усьому світі, зокрема Міжнародний валютний фонд. Крістін Лагард, глава ЄЦБ, у [0] наголошує, що якщо основна частина платежів буде проводитися за допомогою цифрових гаманців, а не банківських рахунків, і буде номінована в приватній цифровий валюті, грошовий суверенітет може бути ослаблений.

Ерін Інгліш, головний стратег з питань безпеки в Microsoft, у [0] запропонувала реальні можливості зменшення ризику кібербезпеки для системи інформаційних технологій завдяки технології блокчейн. Практики розглянули питання розміщення блокчейну на хмарній платформі, наприклад Microsoft Azure, що дозволило підвищити кіберзахист завдяки контролю доступу на платформі.

Таким чином **метою статті** є огляд доцільності використання технології блокчейну для інформаційної безпеки та для вдосконалення системи захисту інформації з огляду на функціональні критерії захищенності.

Блокчейн за своєю природою може забезпечити абсолютну цілісність інформації, що значно підвищить захищеність системи захисту від таких атак, як модифікації, імітація відправника, повторна передача повідомлення чи відмова від повідомлення.

Згідно з НД ТЗІ 1.1-003-99 критеріями оцінки захищеності є сукупність вимог, що використовується для оцінки ефективності функціональних послуг безпеки і коректності їх реалізації [0]. Система із блокчейном відповідає критерію «ЦД-4. Абсолютна довірча цілісність» та ЦЗ-3. «Повна цілісність при обміні» [0].

Виклад основного матеріалу: Блокчейн-мережі розподілені між усіма комп'ютерами партнерів (мережа консорціуму). Кожен партнер може відстежувати кожну транзакцію в мережі в режимі реального часу. Крім того, партнер може відхилити неправильні транзакції, перш ніж вони будуть застосовані до реєстру. Це спрощує аудит і значно знижує ризик шахрайства. До того ж до розробки додатків ланцюжка поставок і загальних робочих пото-

ків розробники відкривають нові канали надходження доходу, створюючи нові продукти і служби на основі блокчейну.

Учасники децентралізованої мережі разом зберігають інформацію, що оброблюється в ній, у вигляді захищених криптографією блоків з даними. За допомогою алгоритмів консенсусу учасники вирішують, яким чином вони будуть довіряти один одному. Для мережі важливо, щоб транзакція була схвалена більшою частиною учасників мережі (поріг 51 %), тільки після цього буде додано новий блок до ланцюга, який ніяк не можна потім змінити.

Оскільки мережа — децентралізована, не існує якогось центрального хаба, де зберігається вся інформація, або посередника, який узгоджує роботу мережі між 2 сторонами. Ця мережа абсолютно відрізняється від звичних нам централізованих мереж, де обов'язково є головний нод, який координує роботу всієї структури.

Блоки в ланцюжку блокчейну не можуть бути змінені або видалені, тому що кожен наступний ланцюжок містить геш попереднього блоку. Таким чином, ніякі маніпуляції з інформацією в блокчейні не пройдуть непоміченими [0].

Загалом технологія блокчейну будується на 3 величезних китах, що відокремлюють її від інших технологій (рис. 1).

Ці принципи відображають деякі аспекти кібербезпеки. Розглянемо кожну з характеристик детальніше з точки зору ІБ.

Децентралізація є ефективним засобом проти фальсифікації баз даних. В середньостатистичних мережах, де є головний центр, зловмисникам достатньо завдати непоправної шкоди цьому центру, що є єдиною точкою відмови. В децентралізованій мережі такий підхід не може бути реалізований, оскільки дані зберігаються розподілено. Єдиний вихід — модифікувати ці дані у кожного учасника. Але тепер постає питання як змусити більшість підтвердити цю зміну та внести в ланцюжок.

Рис. 1. Основні характеристики блокчейну

Якщо мережа працює за алгоритмом консенсусу Proof Of Work, знадобляться величезні обсяги комп'ютерних потужностей, щоб реалізувати таку ідею. Звичайно це рішення є неефективним, тому шукають гнучкіші способи. Мова йде саме про блокчейн у Bitcoin, оскільки форки (fork — внесення змін в попередньо визначеному протоколі мережі блокчейну) першої цифрової валюти, як менш глобально розподілені, мають певні вразливості.

Блокчейн має очевидні переваги над іншими системами, але будь-яка система, якою б ідеальною вона не була, не може вважатися повністю безпечною. В історії уже є випадки інцидентів порушення конфіденційності, цілісності чи доступності. Яскравим прикладом є Mt Gox [0]. На початку 2014 року Mt Gox, біткойн-біржа, що базується в Японії, була найбільшою у світі, обробляючи понад 70 % усіх біткойн-транзакцій. До кінця лютого того ж року вона збанкрутіла.

Варто зазначити, що враховуючи попередній досвід, блокчейн стає непідйомною ношею для крадіїв інформації завдяки експоненційному ускладненню операцій підробки блоків ланцюга. Тому безумовно будуть спроби зловживання і маніпулювання цією технологією, проводяться розрахунки на стійкість блокчейну в постквантову еру, але для цього буде потрібно значно більше часу, ресурсів і зусиль, ніж у випадку з традиційними технологіями.

Сьогодні найслабшим місцем у системі практичного застосування блокчейну є централізовані біржі. Саме вони є жертвами численних атак через свою централізованість. Головний принцип у такій архітектурі є найвразливішим місцем, який ніяк не може бути усунутий. Завдяки цьому зросте попит на децентралізовані системи.

Усвідомлюючи переваги технології блокчейн, багато організацій починають впроваджувати її в свою діяльність [0]. Наприклад, в Естонії розробили блокчейн-платформу для департаменту охорони здоров'я. На ній зберігається інформація, що стосується візитів до лікарів, рецепти, аналізи, історія хвороб тощо.

У кінці 2018 року IBM запустила платформу Food Trust, щоб допомогти компаніям боротися з контрафактом і вчасно реалізовувати товар, у якого закінчується термін придатності. До платформи підключилися такі компанії, як Nestle, Unilever, мережі супермаркетів Walmart і Carrefour. Це обходиться їм у десятки тисяч доларів, але допомагає заощадити в сотні разів більше. Блокчейн явно зарекомендував себе новим рівнем розвитку індустрії, навіть за межами сектора інформаційної безпеки.

Технологія блокчейну нерозривно пов'язана із цифровими валютами, тому і в цій сфері спостерігаються певні зрушення, особливо в аспекті прийняття криптовалют. Україна за результатами дослідження глобального індексу прийняття криптовалют очолює список країн, де спостерігається бурхливе поширення користування критовалютами. Дані були опублікованні у звіті «Chainalysis 2020 Geography of Cryptocurrency « 2020 року [0]. Рейтинг країн за індексом прийняття показано в табл. 1.

Таблиця 1

РЕЙТИНГ ІНДЕКСУ ПРИЙНЯТТЯ КРИПТОВАЛЮТИ У СВІТІ

Країна	Оцінка	Ранг	Рейтинг показників			
			Отримана цінність в ланцюзі	Отримана роздрібна вартість	Кількість онлайн-депозитів	Вартість обміну P2P
Україна	1	1	4	4	7	11
Росія	0,931	2	7	8	5	9
Венесуела	0,799	3	19	14	15	2
Китай	0,672	4	1	1	95	53
Кенія	0,645	5	37	11	57	1
США	0,627	6	5	6	39	16
Південна Африка	0,526	7	12	9	41	10
Нігерія	0,459	8	14	7	112	3
Колумбія	0,444	9	25	18	61	4
В'єтнам	0,443	10	2	2	44	81

Жодна з країн не збирається зупинятися на досягнутому та створює сприятливі умови для розвитку ринку цифрових валют.

Як показав досвід використання цифрових валют, криптографія та продумані економічні стимули можуть створити безпечний спосіб зберігання і управління фінансовими активами та інформацією, включаючи особисту інформацію.

Висновки: Незалежно від того, де і як використовується блокчейн, ключовим фактором його використання як технології захисту інформації є децентралізація.

Коли контроль доступу, мережевий трафік і навіть самі дані більше не зберігаються в одному місці, кіберзлочинцям стає набагато складніше атакувати інформаційні ресурси.

Підготовка до випуску CBDC займає роки, вимагаючи вивчення альтернативних моделей, раундів громадських консультацій, міжнародного обміну досвідом і багатоетапних експериментів. Швидкої появи цифрових національних валют очікувати навряд чи варто. Але вивчати і будувати моделі необхідно.

Це може означати більший рівень безпеки та меншу вразливість. Популярність використання технології блокчейну тільки зростатиме, що означає можливість продовжити дослідження питання використання блокчейну в системі захисту інформації для діяльностей різного напрямку.

Бібліографічні посилання

1. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-003-99 від 28 квітня 1999 р. №22. *ДСТСЗІ СБУ, 1999*. URL: https://tzi.com.ua/downloads/1.1-003-99.pdf
2. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.5-004-99 від 28 квітня 1999 р. №22. *ДСТСЗІ СБУ, 1999*. URL: https://tzi.com.ua/downloads/2.5-004-99.pdf
3. Башир И. Блокчейн: архитектура, криптовалюты, инструменты разработки, смарт-контракты» / Имран Башир; пер. с англ. под науч. ред.: М. А. Райтмана. — Москва : ДМК-пресс, 2019. — 538 с.
4. Кравченко П. Блокчейн і децентралізовані системи : навч. посібник для студ. закладів вищ. освіти : в 3 частинах. Ч. 1 / П. Кравченко, Б. Скрябін, О. Дубініна. — Харків : ПРОМАРТ, 2019. — 452 с.
5. Соловйов О. Блокчейн і технології розподіленого реєстру // Nplus1: інт. вид. 2020. URL: https://nplus1.ru/material/2020/02/21/course-blockchain-chapter-1
6. Chainanalysis: The 2020 Geography of Cryptocurrency Report. 132 p. URL: https://go.chainalysis.com/rs/503-FAP-074/images/2020-Geography-of-Crypto.pdf
7. Deloitte: Blockchain & Cyber Security. Let's Discuss. 16 p. URL: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-blockchain-and-cyber-security-lets-discuss.pdf
8. E. English, A. Davine Kim, M. Nonaka. Advancing Blockchain Cybersecurity: Technical and Policy Considerations for the Financial Services Industry. — 2018
9. R. Auer, G. Cornelli, J. Frost. Rise of the central bank digital currencies: drivers, approaches and technologies. BIS Working Papers . — 24 August 2020
10. Speech by Christine Lagarde, President of the ECB, at the Deutsche Bundesbank online conference on banking and payments in the digital world. Frankfurt am Main. — 10 September 2020

Статтю подано до редакції 15.10.2020