відбувається формування глобального інформаційного простору, активно розвиваються програмно-технічні засоби нанесення шкоди комп'ютерним та телекомунікаційним системам тощо. Врахування інформаційного простору в геостратегіях стає визначальнім напрямком держави для досягнення своїх цілей у внутрішній, регіональній та міжнародній політиці, а також у досягненні геополітичної переваги на світовій арені.

Інформаційні джерела:

1. Вегеш М., Палінчак М., Петрінко В. Геополітика в постатях і термінах : підручник для студентів і аспірантів спеціальності «Політологія». Ужгород : Видавничий дім «Гельветика». 2020. 786 с.
2. Луман Н. Поняття ризика. *Thesis*. 1994. № 5. URL: www.ecsocman.edu.ru/data/429/174/1217/5_2_2luhm.pdf (дата звернення 10.05.2023).
3. D. Bell. The Social Framework of the Information society. Oxford, 1980. P. 500-549.
4. Efferink L. van The Definition of Geopolitics – Classical, French and Critical Traditions. URL: https://exploringgeopolitics.org/%20Publication_Efferink_van_Leonhardt_The_Definition_of_Geopolitics_%20Classicial_French_Critical.html (дата звернення 7.05.2023).
5. Момот А. С. Інформаційні чинники впливу на сталий розвиток світосистеми. *Нова парадигма*. 2011. Вип. 104. С. 67–77.

УДК 004.031.43: 004.056

О.О. Рудь, канд. екон. наук *(ДБТУ, Харків)*
В.М. Сирий, ст. викл. *(ДБТУ, Харків)*

ТЕХНОЛОГІЯ БЛОКЧЕЙН ТА ЇЇ РОЛЬ У КІБЕРБЕЗПЕЦІ

Сучасний світ швидко цифровізується, тому кібербезпека стає однією з найактуальніших проблем підприємств, організацій та індивідуальних користувачів. Загрози у сфері кібербезпеки стають настільки складними й вишуканими, що традиційних підходів до захисту інформації вже недостатньо. Нові рішення для забезпечення кібербезпеки запроваджуються зокрема в технології блокчейн [1 - 3].

Блокчейн є розподіленою системою, де копії бази даних зберігаються на багатьох вузлах мережі. Це робить систему стійкою до єдиної точки відмови та знижує ризики крадіжки або втрати даних.

Крім того, розподілений характер блокчейна дозволяє користувачам мережі перевіряти й підтверджувати транзакції незалежно один від одного, що підвищує довіру та безпеку системи.

Технологія блокчейн зберігає інформацію у вигляді ланцюжка блоків. Кожен блок містить інформацію про транзакції або події та посилання на попередній блок, утворюючи безперервну послідовність. Це забезпечує прозорість та надійність зберігання даних, оскільки кожен блок містить хеш попереднього блоку і будь-яка зміна в одному з них призводить до зміни всіх наступних.

Основними принципами роботи блокчейна є децентралізація, консенсус та шифрування даних.

Децентралізація означає відсутність єдиного контролюючого центру, що робить систему стійкою до атак і маніпуляцій.

Консенсус досягається шляхом узгодження всіх учасників мережі щодо правильності транзакцій та блоків.

Шифрування забезпечує безпеку даних за допомогою криптографічних алгоритмів.

Основними напрямками застосування технологій блокчейн в кібербезпеці є підвищення безпеки даних, удосконалення ідентифікації й автентифікації, захист від DDoS-атак і покращення цифрових платежів та угод [4].

Підвищення безпеки здійснюється за рахунок незмінності, непідробності та шифрування даних. Однією з ключових переваг технології блокчейн є здатність забезпечувати незмінність та непідробність даних за рахунок ланцюгової структури блоків та хешування. Завдяки цьому маніпулювання даними стає вкрай складним і легко виявляється.

Криптографічне шифрування даних усуває ризики їх витоку або несанкціонованого використання. Дані шифруються за допомогою складних алгоритмів перед збереженням у блоці. Для їх розшифровування залучені в технології вузли мережі повинні мати відповідні ключі.

Вдосконалення ідентифікації й автентифікації досягається за рахунок розробки децентралізованих ідентифікаційних систем. Наприклад, традиційні централізовані системи ідентифікації піддаються постійному ризику крадіжки та підробки облікових даних. У блокчейні кожен користувач може мати унікальний ідентифікатор, пов'язаний з його цифровим гаманцем або публічним ключем. Ідентифікаційні дані зберігаються у блокчейні та кожного разу, коли потрібна автентифікація користувача, відбувається перевірка та порівняння даних, що забезпечує високий рівень безпеки та запобігає підробці.

Децентралізація даних полягає в тому, що у блокчейні відсутній єдиний центр управління і дані зберігаються на множині вузлів, що робить систему стійкою до відмов. Якщо один вузол виходить з ладу або піддається атаці, інші вузли продовжують працювати та підтримувати доступ до інформації. Це забезпечує безперервність роботи системи та запобігає єдиній точці відмови.

Внаслідок децентралізації даних блокчейн сприяє також захисту від DDoS-атак. У традиційних централізованих мережах зловмисники можуть спрямувати перевантаження запитами до однієї точки, що призводить до відмови системи в цілому. Завдяки децентралізації дані та обчислювальні ресурси зберігаються й обробляються на множині вузлів і це ускладнює виведення з ладу системи спрямуванням DDoS-атаки на окремі її елементи.

Запобігання DDoS-атакам і підвищення ефективності фільтрації трафіку у технології блокчейн можуть бути реалізовані за допомогою використання смарт-контрактів – різновиду угод у формі закодованих алгоритмів. Укладення, зміна, виконання й розірвання таких угод відбувається у середовищі комп'ютерних програм, зокрема на блокчейн-платформах. Наприклад, можна створювати смарт-контракти, які автоматично перевіряють ідентифікаційні дані відправника та приймають рішення щодо його допуску чи блокування. Це дозволяє фільтрувати потенційно шкідливий трафік ще до досягнення цільової мережі, що суттєво знижує ризик DDoS-атак.

Розвиток технології блокчейн виводить цифрові платежі на новий рівень як за рахунок підвищення безпечності транзакцій так і виключення з процесу посередників.

Згідно з технологією блокчейн кожна транзакція записується та підтверджується в ланцюжку блоків, що забезпечує непідробність та незмінність даних. Кожна транзакція повинна пройти перевірку та узгодження учасниками мережі, що запобігає можливості шахрайства та підробки.

Завдяки криптографічному шифруванню та використанню публічних і приватних ключів блокчейн забезпечує конфіденційність та цілісність даних під час здійснення платежів та угод.

У традиційних фінансових і платіжних системах потрібна участь банків, платіжних шлюзів та інших посередників, що супроводжується комісіями та ризиками. Блокчейн дозволяє користувачам здійснювати прямі транзакції без посередників, що виключає зайві комісії й ризики та суттєво спрощує й прискорює вказані процеси.

Таким чином технологія блокчейн пропонує інноваційні підходи у забезпеченні кібербезпеки. Розглянуті особливості застосування блокчейна в аспекті підвищення безпеки даних, децентралізації системи ідентифікації, захисту від DDoS-атак, а також покращення здійснення цифрових платежів та угод мають суттєвий потенціал для створення безпечного та надійного кіберсередовища.

Однак, з урахуванням обмежень та викликів, пов'язаних з масштабованістю, продуктивністю та конфіденційністю даних, а також задля більш повного розкриття потенціалу технології блокчейн у забезпеченні кібербезпеки є потреба в подальших дослідженнях.

Інформаційні джерела:

1. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. URL: https://bitcoin. org/bitcoin.pdf

2. Swan M. Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc. 2015, 152 p.

3. Лапко О.О., Солосіч О.С. Технологія блокчейн: поняття, сфери застосування та вплив на підприємницький сектор. БІЗНЕСІНФОРМ, №6, 2019. С. 77-82.

4. Спасітелева С.О., Бурячок В.Л. Перспективи розвитку додатків блокчейн в Україні // Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». Т.1 №1, 2018. С. 35-48. URL: https://www.csecurity.kubg.edu.ua/index.php/journal/article/view/18/59.

УДК 378.004.9

В.М. Сирий, ст. викл. *(ДБТУ, Харків)*
Т.А. Бутенко, канд. екон. наук, доц. *(ДБТУ, Харків)*

МЕТОДИЧНІ АСПЕКТИ ВИКЛАДАННЯ ДИСЦИПЛІН З ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ПРОГРАМУВАННЯ

Згідно з висновками звіту The Future of Jobs 2023 р. на ринку праці у сфері комп’ютерних технологій найбільш затребуваними зостаються компетентності зі штучного інтелекту та машинного навчання, аналітики великих даних, стратегії та цифрової трансформації бізнесу, фінансових технологій, автоматизації виробничих процесів, інформаційної безпеки тощо [1].

Сучасна ІТ-команда повинна складатися з фахівців різних напрямів: Front-end (клієнтська частина, зовнішній інтерфейс), Back-end