CYBERSECURITY AND CRITICAL INFRASTRUCTURE PROTECTION

DOI 10.20535/2411-1031.2023.11.2.293824
УДК 004.056

АНАСТАСІЯ ТОЛКАЧОВА,
АНДРІЯН ПІСКОЗУБ

АНАЛІЗ ЗАГРОЗ ТА РИЗИКІВ В ЕКОСИСТЕМІ WEB3 В КОНТЕКСТІ БЕЗПЕКИ

У даній науковій статті розглядається актуальна та перспективна проблематика в області кібербезпеки, зокрема - аналіз потенційних загроз та ризиків розвитку Web3. Web3 - нове покоління інтернету, яке базується на технології блокчейн, децентралізації, криптографії та розумних контрактах. Цей підхід спрямований на покращення безпеки, конфіденційності та забезпечення прав користувачів у віртуальному середовищі, однак без відповідного розуміння може нести зворотній ризик. Наведено аналіз останніх досліджень та проблематики. Автори розглядають потенційні загрози та ризики, в тому числі можливі напади на протоколи децентралізації, маніпуляцію цензурою, атаки на протокол блокчейн, спроби зламу системи та несправедливих угод розумних контрактів. У статті розглядаються ряд вразливостей та атак, які можуть нашкодити новій технології Web 3.0. Описано нові загрози приватності користувачів та їх цифрових активів, зокрема використання технологій збереження анонімності та механізми протидії з боку злочинних структур чи державних органів. Також стаття наголошує на значимості обговорення правових аспектів інтеграції Web3, пошуку оптимального балансу між регуляцією цифрового простору та правами користувачів на конфіденційність та автономію. Глобальні виклики вимагають міжнародної співпраці та стандартизації правил регулювання в цій сфері. Результати дослідження демонструють, що свідомий підхід до аналізу загроз Web3 є ключем до побудови безпечного майбутнього Інтернету. Ця стаття сприяє поширенню інформації та знань про можливі ризики, відкриває нові горизонти для наукових досліджень, практичної реалізації заходів щодо забезпечення кібербезпеки та політичного діалогу в епоху Web3.

Ключові слова: блокчейн, вразливості, децентралізація, інформаційна безпека, захист інформації, смарт контракти, web3, NFT.

Постановка проблеми. Основна ідея Web 3.0 полягає в тому, щоб забезпечити приватну та децентралізовану інтернет-екосистему, де користувачі матимуть більший і надійніший контроль над своїми даними у мережі. Web 3.0 є майбутнім Інтернету, який буде забезпечувати ефективнішу взаємодію між людьми і комп'ютерами, забезпечить безпеку і конфіденційність даних та дозволить створити нові можливості для розвитку різних інтернет сервісів і додатків. Так, технологія блокчейн може бути використана для створення безпечної та надійної системи електронних голосувань. Технології AI (artificial intelligence) можуть допомогти забезпечити точніший аналіз даних, що сприяє вирішенню складних проблем і покращенню ефективності бізнес-процесів. Web 3.0 дозволяє створювати децентралізовані додатки (distributed applications (DApps)), які можуть бути запущені на блокчейні і забезпечать більшу безпеку і приватність для користувачів. Такі додатки можна використовувати в різних галузях, зокрема в медицині для збереження медичних даних пацієнтів, у фінансовому секторі для забезпечення безпеки фінансових операцій тощо. Однак технологія Web 3.0 має свої виклики і проблеми, а саме: складність впровадження нових технологій, висока вартість, нестабільність

розподілених систем, потреба в нових знаннях і навичках для розробників і користувачів. Загалом ця технологія є важливим напрямом розвитку Інтернету, який дозволить забезпечити безпечнішу, приватну та децентралізовану інтернет-екосистему, що може стати основою для нових інновацій та розвитку різних галузей. У сучасному цифровому світі технології постійно розвиваються, а з ними і виклики та можливості, що ставляться перед спільнотою. Однак, перехід до екосистеми Web3 також ставить перед дослідниками та розробниками великий акцент на питання безпеки, які досі залишаються недостатньо досліджені.

Головною проблемою, яка стоїть перед спільнотою Web3 та сферою цифрової економіки, є забезпечення безпеки персональних даних, забезпечення конфіденційності транзакцій, стабільність розподільчих систем та захист цифрових прав власності [2]. Ці та інші виклики заслуговують на глибокий аналіз та проведення комплексних досліджень, щоб забезпечити стале й гармонійне зростання екосистеми Web3 у безпечних межах.

Отже, дана стаття ставить перед собою мету аналізувати виклики та можливості в екосистемі Web3 з точки зору безпеки, а також спробувати ідентифікувати області роботи, в яких потрібно зосередитись для реалізації потенціалу Web3 технологій на користь глобального цифрового суспільства.

Аналіз останніх досліджень і публікацій. Вивчаючи найновіші наукові дослідження щодо Web3 та аспектів безпеки, слід зупинитись на кількох ключових моментах, які були отримані в ряді важливих публікацій.

1. Блокчейн технологія та її вплив на безпеку Web3:

Дослідження Aviv Zohar та Yonatan Sompolinsky показали, що залучення блокчейн-технологій як базової архітектури для надання безпеки та захисту цифрових активів може суттєво знизити ризики атак, забезпечити прозорість транзакцій, а також зменшити залежність від централізованих систем [1].

2. Важливість конфіденційності:

Дослідження на платформі Binance наголошують на важливій ролі конфіденційності у блокчейні та пропонують практики, орієнтовані на конфіденційність в децентралізованих мережах [11].

3. Відкриті стандарти та принципи бізнесу для надання безпеки Web3:

Дослідження Berners-Lee зосереджується на тому, як використання відкритих стандартів та етичних принципів бізнесу можуть допомогти встановити безпеку та стабільність екосистеми Web3. Автор відзначає важливість співпраці розробників, установ та державних органів у побудові надійної екосистеми [12]-[13].

4. Регулювання та управління ризиками у Web3:

De Filippi у своєму дослідженні розглядає регулювання та управління ризиками в екосистемі Web3. Результати дослідження свідчать про необхідність існування механізму регулювання та контролю від комерційних організацій до державних установ для забезпечення глобальної безпеки [17].

Ці та інші результати досліджень допомагають розробити стратегії для побудови та обслуговування високої якості екосистеми Web3, що забезпечують безпеку на всіх рівнях - від комерційних підприємств до національних державних органів.

Метою статті дослідження є проведення комплексного аналізу викликів та можливостей, пов'язаних з розвитком та впровадженням екосистеми Web3. У контексті стрімкого розвитку цифрових технологій та переходу від централізованих до децентралізованих рішень, важливим є належне розуміння ризиків та надійного захисту користувачів й активів в межах нової парадигми Інтернету.

Для досягнення визначеної мети будуть досліджені ключові аспекти екосистеми Web3 та її технологічних компонентів, таких як блокчейн, децентралізовані додатки, криптовалюти та невзаємозамінні токени (NFT). Особлива увага буде приділена виявленню потенційних загроз, їх аналізу та розробці шляхів їх подолання.

Виклад основного матеріалу дослідження. Хоча дати чітке визначення того, що таке Web3, складно, створення цієї версії мережі регулюється кількома основними принципами.

– Мережа Web3 децентралізована: на відміну від інших версій інтернету, де великі ділянки мережі перебувають під контролем і у власності централізованих організацій, право власності у Web3 розподіляється між розробниками та користувачами.

– Мережа Web3 не потребує дозволів: кожен має однаковий доступ до участі у Web3, і нікого не буде виключено.

– Мережа Web3 має власну платіжну систему: у ній використовується криптовалюта для витрачання та надсилання грошей в інтернеті, замість того щоб покладатися на застарілу інфраструктуру банків та інструментів для обробки платежів.

– Мережа Web3 не вимагає довіри: вона працює на основі стимулів і економічних механізмів, а не покладається на надійні треті сторони.

Децентралізація – один із головних принципів технології Web 3.0. В цій системі відсутня централізована влада чи контроль, а замість цього вона базується на розподілених мережах і протоколах. Це дає багато переваг порівняно з централізованими системами. Однією з найбільших переваг таких систем є зменшення ризиків, пов'язаних з владою і контролем. У цій моделі немає одного центру контролю, який може бути скомпрометований або зламаний. Замість цього дані та інформація розподіляються по всій мережі, що робить систему стійкішою і захищенішою. Крім того, децентралізовані системи дають можливість кожному користувачеві мати більший контроль над своїми даними та інформацією, що зберігається в системі. Це важливо, оскільки користувачі можуть бути впевнені, що їх дані не будуть використані без їхньої згоди. Нарешті децентралізація дає можливість створювати нові додатки і сервіси, які були би неможливі у централізованих системах, наприклад: відкриті ринки та системи децентралізованих фінансів, які забезпечують доступ до фінансових послуг без посередників, що відкриває нові можливості для людей у країнах, де доступ до традиційних фінансових послуг обмежений. Таким чином, децентралізація як один із ключових принципів Web 3.0 дозволяє створювати стійкіші і захищеніші системи, забезпечуючи надійніший контроль над даними користувача і відкриваючи нові можливості для розвитку технологій та інновацій.

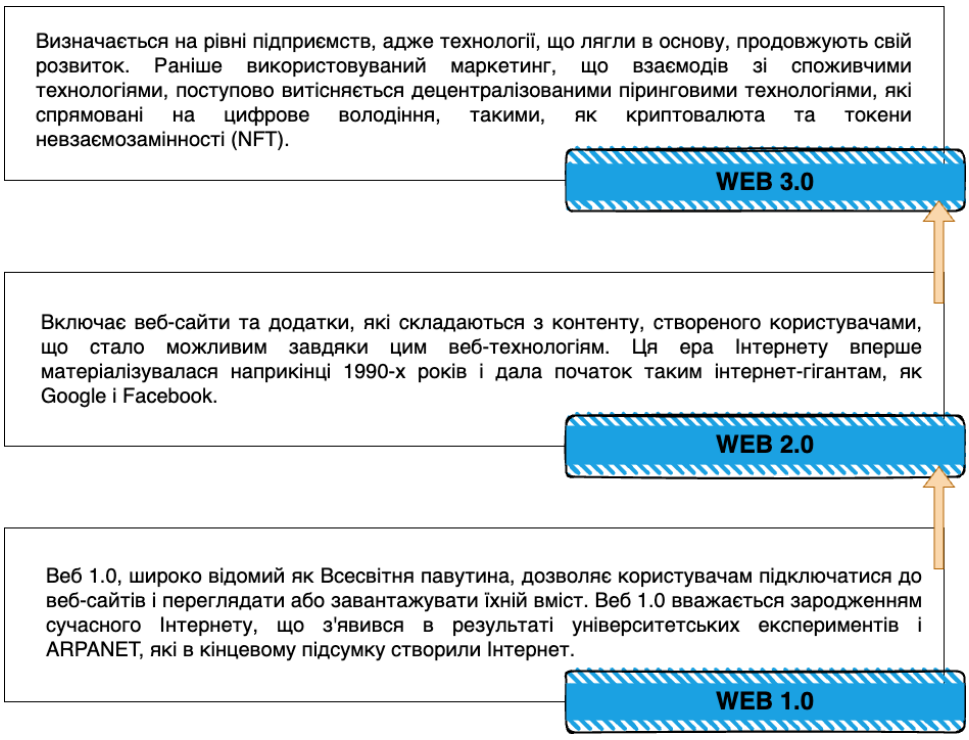

Рисунок 1 – Стислий опис поколінь WEB

Web3 базується на блокчейн-технології, що надає можливість зберігання інформації в захищеній, децентралізованій мережі, де кожна особа має рівні права та можливості [5], [8]-[9]. Це розподілена база даних, яка містить інформацію про транзакції та операції, що відбуваються в мережі. Інформація розподіляється по всіх вузлах мережі, що робить блокчейн стійкішим і захищенішим від атак ззовні. Використання блокчейну дає можливість створювати децентралізовані додатки і сервіси, які працюють на основі смарт-контрактів [4]. Блокчейн дозволяє забезпечити безпеку і прозорість транзакцій у децентралізованих системах, таких як криптовалютні біржі, системи голосування та ін. [5].

За допомогою смарт-контрактів користувачі мають змогу безпосередньо спілкуватися, робити це швидко та відкрито, а також розробляти новаторські програми та послуги [7]. У Web3 ви маєте можливість заробляти на криптовалюті, керувати своїми електронними ресурсами, обмінювати токени (NFT) та користуватися множиною децентралізованих послуг, включаючи фінанси, страхування, навчання та розваги [14]. Таким чином, Web 3.0 відкриває новий розділ в історії Інтернету, надаючи користувачам більше автономії, управління та шляхів для прогресу в цифровій добі.

Однак разом із розвитком Web 3.0 приходять і нові ризики. Вони стосуються як користувачів так і недоліків пов’язаних із системами:

Нульова довіра (zero trust). У сфері інформаційної безпеки концепція "нульової довіри" привернула багато уваги. З точки зору Web 3.0, децентралізація приводить Інтернет у відповідність до архітектури безпеки з нульовою довірою. В епоху Web 2.0 споживачі довіряли компаніям, які часто керували сайтами та послугами. Замість того, щоб передавати дані через посередників, яким споживачі довіряють, Web 3.0 не має довіри, оскільки потоки даних передаються від одного користувача до іншого через децентралізовані додатки.

Маніпуляції з даними. Одним із значних ризиків для кібербезпеки є навмисне маніпулювання даними, що використовуються для навчання ШІ. Штучний інтелект є наймасштабнішою системою дезінформації у світі, оскільки будь-хто може створити неправдиві дані для отримання бажаних результатів. Наприклад, чат-бот Microsoft “Tay” став расистом після того, як його запрограмували на шкідливі твіти. Тей був розроблений, щоб вчитися на основі стрічки Твіттера [19].

Удосконалений спам. В епоху Web 3.0, коли існує величезна бібліотека інтегрованої та взаємопов'язаної інформації, спам-атаки можуть легше поширюватися багатьма шляхами. Для розповсюдження спаму зловмисники можуть зосередитися на певних ресурсах, а потім експлуатувати, забруднювати та насичувати їх, щоб націлитися на конкретні Web-сайти, пошукові системи та додатки.

Шкідливе ПЗ. JavaScript-шкідливе програмне забезпечення або програми-вимагачі можуть бути приховані всередині програми і надсилатися кожному користувачеві через ці спам-кампанії. Також до загроз, пов'язаних зі спамом, можна віднести можливість зміни урядами країн даних на Web-сайтах для того, щоб годувати алгоритми штучного інтелекту дезінформацією, яка згодом поширюється серед мешканців країни.

Ризик ідентичності. Web 3.0 пропонує використовувати суверенну ідентичність для забезпечення глобально портативного набору облікових даних, вимог і дозволів при взаємодії з Web-сайтами, іншими користувачами та Web-додатками. Ця ідентичність на основі блокчейну дозволяє користувачам вирішувати, якими частинами своєї ідентичності ділитися з певними третіми сторонами. Деякі ризики для ідентичності пов'язані зі створенням справді суверенної інфраструктури ідентифікації. Припустимо, зловмисник помітив, що один і той самий ідентифікатор користувача використовується в усіх сесіях користувача в певному додатку або на певному Web-сайті. У такому випадку він зможе зібрати воєдино конфіденційну інформацію про цього користувача. Ризик крадіжки особистих даних викликає справжнє занепокоєння при використанні недостатньо безпечних методів автентифікації.

Безпека даних. Записи, що додаються до блоків, шифруються, що робить блокчейн однією з найбезпечніших технологій. Однак у неї є недоліки. Виявлено недоліки в цій нібито

неприступній технології, серед яких ‘атака 51%’, атака Сивілли, фішинг і крадіжка ключа користувача. Атака 51% – l це потенційна атака на блокчейн-мережу, де одна особа або організація може контролювати більшу частину хешрейту, що може призвести до порушення роботи мережі. У такому сценарії зловмисник матиме достатньо потужності для майнінгу, щоб навмисно виключити або змінити порядок транзакцій. Він також зможе скасувати транзакції, які він здійснював, маючи контроль, що призведе до проблеми подвійних витрат. Атака Сивілли – вид атаки, в якій репутаційна система підривається шляхом підробки ідентичності в одноранговій мережі. В результаті атаки жертва підключається тільки до вузлів, контрольованих зловмисником.

Клонування гаманців є поширеним ризиком безпеки в епоху Web 3.0. Хакер може продублювати гаманець користувача і використовувати його для купівлі товарів в Інтернеті, якщо у нього є приватний ключ користувача.

Оскільки блокчейн є основою Web 3.0, етичні хакери зобов'язані розробити засоби для запобігання витоку даних і злому. Якщо зловмисник викрав цифровий актив, його складно відновити. У децентралізованій мережі дійсно складно відстежити потоки транзакцій.

Соціальна інженерія. Фундаментальна технологія блокчейн, що лежить в основі Web 3.0, забезпечує незмінність даних, що зберігаються в блокчейні. Однак навіть ті дані, які здаються непорушними, можуть бути зламані. Фішингові атаки Web 3.0 включатимуть зловмисників, які видаватимуть себе за надійні організації, щоб отримати доступ до конфіденційних даних. Аутентифікаційні дані стануть мішенню для інших спроб соціальної інженерії.

Web 3.0 відкрив новий клас кіберзагроз, які є унікальними для мереж та інтерфейсів блокчейну. Нижче наведено кілька прикладів цих нових загроз:

Зламування логіки смарт-контрактів. Ця нова загроза націлена на логіку, закодовану в сервісах блокчейну. Злам використовуються для експлуатації широкого спектру функцій і послуг, таких як послуги криптопозик, управління проектами і функції криптовалютних гаманців. Зламування логіки смарт-контрактів також піднімає важливі юридичні питання, оскільки смарт-контракти часто не захищені законом.

Експлуатація NFT. Саме завдяки розвитку NFT криптовалюти набувають все більшого поширення, що віщує гнучкий наратив для інших сфер застосування криптовалют, таких як фінанси, що, в свою чергу, вплине на Web 3.0. Існує багато інших способів використовувати Web 3.0, щоб підштовхнути вашу цільову аудиторію до певного кроку, одним з яких є прийняття біткоїна для забезпечення конфіденційності та транскордонних платежів. Слід зазначити, що NFT є ключовим компонентом Web 3.0. NFT тільки починають розвиватися, тому важливо усвідомлювати ризики, пов'язані з ними, і вживати відповідних заходів обережності для отримання максимального прибутку. Першим кроком в атаці є надсилання жертві посилання на пошкоджений NFT. У зловмисних зломах NFT використовується код JavaScript для відправки жертві набору запитів. Ненавмисно відправляючи запит, жертва надає зловмиснику повний доступ до своїх NFT або біткоїнів.

Атаки на флеш-кредити (Flash loan). Ця загроза полягає в тому, що смарт-контракти, призначені для підтримки надання флеш-кредитів, бувають атаковані з метою викачування активів. Незабезпечені кредити експлуатуються шляхом маніпулювання різними вхідними даними смарт-контракту, як це сталося нещодавно під час атаки на xToken на суму 24 мільйони доларів [18].

Криптоджекінг. Відбувається, коли зловмисники непомітно встановлюють програмне забезпечення для криптомайнінгу на комп'ютери та мережі жертв. Щоб здійснити криптоджекінг, злочинець викрадає обчислювальну потужність жертви і використовує її для генерації біткоїнів для власної вигоди. Коли жертва мимоволі завантажує шкідливе програмне забезпечення зі скриптами, наприклад, за посиланням в електронному листі або на шкідливому Web-сайті, кіберзлочинець отримує доступ до її комп'ютера або інших пристроїв, підключених до Інтернету. Використовуючи “майнери монет”, злочинець створює криптовалюту за допомогою сторонніх програм. Оскільки криптовалюта є цифровими

грошима, її можна створити лише за допомогою комп'ютерних програм та обчислювальних потужностей. На відміну від інших криптовалют, Monero видобувається переважно вдома за допомогою персонального комп'ютера [3].

Перетягування ковдри (Rug pulls). У цих атаках беруть участь інсайдери - розробники криптовалют, злочинні угруповання, проплачені впливові особи тощо, які створюють ажіотаж навколо проекту, щоб потім втекти з коштами інвесторів. Часто шахраї створюють криптовалюту, реєструють її на децентралізованих біржах (DEX), а потім прив'язують до основної криптовалюти, наприклад, Ethereum [10]. Видаляючи гроші з пулу ліквідності, зловмисники призводять до того, що ціна монети падає до нуля. Щоб завоювати довіру інвесторів, вони можуть навіть наповнити свій пул ліквідністю в Telegram, Twitter та інших соціальних мережах. DEX дозволяють користувачам публікувати свої токени безкоштовно і без аудиту, на відміну від централізованих криптовалютних бірж. Блокчейни з відкритим вихідним кодом, такі як Ethereum, наприклад, роблять створення токенів простим і безкоштовним. Цими двома факторами користуються злочинці.

Крижаний фішинг (Ice phishing). Відносно новий термін, який з'явився лише кілька років тому. При крижаному фішингу зловмисники переконують користувачів підписати транзакцію, яка дозволяє зловмиснику використовувати та схвалювати токени – так звана “обманна операція”. Для смарт-контрактів DeFi характерно делегувати дозвіл на використання токенів як транзакцію смарт-контракту. Для здійснення льодового фішингу вам не потрібні ваші приватні ключі. В якості альтернативи, зловмисник може обманом змусити жертву підписати транзакцію, яка дає йому або їй контроль над токенами.

Ці нові методи існують поряд із традиційними загрозами соціальної інженерії, такими як фішингові атаки. Ризики посилюються тим, що користувачі повинні брати на себе відповідальність за безпеку своїх даних, а не покладатися на централізованих контролерів. Насправді, складність інтерфейсів Web 3.0, які часто включають в себе кілька особистих гаманців і паролів, які неможливо відновити, створює вразливість до атак соціальної інженерії.

Багато нещодавніх атак на блокчейн були зосереджені не стільки на технології, скільки на базових людських вразливостях. Наприклад, викрадені криптографічні ключі (приватні цифрові підписи) були ймовірною причиною злому криптовалютної біржі Bitfinex на суму 73 мільйони доларів. Вразливості кінцевих точок, наприклад, на рівні пристроїв, додатків, гаманців або сторонніх постачальників, також є точками входу для зловмисників. Співробітники або персонал постачальників також є мішенями, як у випадку з Bithumb, криптовалютною біржею, яку, як стверджують слідчі, було зламано шляхом компрометації комп'ютера співробітника [6].

Наївних користувачів переконують підписати транзакції, надаючи зловмисникам доступ до їхніх криптографічних токенів. Людей часто вводять в оману, переконуючи, що гроші надсилаються від члена сім'ї або друга за допомогою банківських переказів. Одним з найефективніших методів льодового фішингу є використання добре продуманої графіки. Ці зображення використовують різноманітні стратегії, щоб змусити глядачів натискати на кнопки та здійснювати фінансові операції.

Безпека та надійність даних. Ширша топологія мережі, яка охоплює учасників, сховища даних та інтерфейси, по суті, розширює діапазон ризиків для безпеки. Хоча транзакції в блокчейні зашифровані, а децентралізація даних і сервісів зменшує кількість точок атаки і ризики цензури, вони також мають потенціал піддавати дані ширшому набору ризиків, включаючи наступні:

– *Доступність даних*. Враховуючи, що набагато більший контроль лежить на вузлах кінцевих користувачів, виникають питання про те, як залежність доступності даних від вузлів може вплинути на процеси або додатки, якщо дані стануть недоступними.

– *Автентичність даних*. Варто також відзначити зворотний виклик доступності: Як люди переконаються в тому, що доступні дані є автентичними, точними, оригінальними чи достовірними? Децентралізація ускладнює цензуру, але увічнює питання якості та точності

інформації, що вже призвело до величезної кількості дезінформації, дезінформації та проблем з безпекою. Залишається незрозумілим, як порушення нульової довіри, ідентичності та контролю впливають на якість даних, не кажучи вже про моделі штучного інтелекту, які поглинають ці дані.

– *Маніпулювання даними.* Ризики маніпулювання даними, що лежать в основі декількох частин екосистеми Web 3.0, включають, але не обмежуються наступним:

- вбудовування шкідливих скриптів у широкий спектр мов програмування, задіяних у Web 3.0, для виконання команд додатків;
- підслуховування або перехоплення незашифрованих даних, що передаються мережею;
- клонування гаманців, яке зловмисники можуть здійснити, отримавши доступ до парольної фрази користувача, фактично заволодівши його вмістом;
- несанкціонований доступ до даних, що відкриває зловмисникам доступ до всього перерахованого вище, на додаток до видавання себе за кінцевого користувача вузла.

Менш централізований нагляд. Інші проблеми безпеки Web 3.0 включають атаки на кінцеві точки, перевантаження трафіку та інші експлойти доступності сервісів – над якими, ймовірно, буде менше, а не більше нагляду з боку IT-спеціалістів. Питання безпеки охоплюють і ширшу мережу Web 3.0.

Ідентифікація та анонімність. Можливості Web 3.0, такі як контрольовані користувачем гаманці, перенесення ідентифікаторів та мінімізація даних, зменшують деякі ризики конфіденційності та приватності даних Web 2.0, пропонуючи людям більшу свободу дій та контроль над своїми даними. Однак ідентичність (SSI – sensitive security information) та анонімність мають і зворотній бік. Прозорий характер публічних блокчейнів, які роблять записи про транзакції доступними для всіх, зміцнює довіру без посередників, але водночас вимагає компромісів у сфері безпеки та конфіденційності. Ось кілька прикладів ризиків, пов'язаних з ідентичністю, які несе в собі Web 3.0:

1. Зручність для користувача. Більшість SSI та криптогаманців вимагають громіздких процесів реєстрації, навчання щодо приватних ключів і мають багато версій з низькою функціональною сумісністю.

2. *Конфіденційність (Приватність).* Web 3.0 викликав багато запитань про конфіденційність. Яка інформація зберігається в ланцюжку, а яка поза ним? Хто повинен знати, коли і як аутентифікувати транзакції? Хто приймає рішення і на основі яких параметрів?

3. Дотримання законодавства. Web 3.0 створює прогалини в даних для регуляторів і відкриває двері для відмивання грошей та фінансування тероризму. Децентралізовані ідентифікатори також ускладнюють існуючі правила, такі як GDPR, ускладнюючи розмежування контролерів даних персональних даних (суб'єктів, відповідальних за забезпечення конфіденційності та безпеки) від процесорів даних персональних даних (суб'єктів, які обробляють дані персональних даних відповідно до інструкцій контролера) [15], [16].

4. Анонімність. Таємниця може спричинити плутанину соціальних норм, як це продемонстрували боти Web 2.0. Анонімність піднімає питання підзвітності, відповідальності, правового захисту та захисту прав споживачів. У міру розвитку додатків Web 3.0 в наступному десятилітті організації повинні враховувати наступні ризики з боку суміжних технологічних, політичних і соціальних сил:

Як використання біометрії вплине на ідентифікацію у Web 3.0, чи то для автентифікації користувачів або співробітників, чи то в охороні здоров'я, чи то в інших сферах?

Як будуть взаємодіяти функції ідентифікації пристроїв Інтернету речей у середовищі Web 3.0, коли інфраструктура, така як автомобілі або сонячні панелі, стануть економічними суб'єктами?

Як інституційна реакція, політичні зловживання та національні централізовані блокчейни можуть вплинути на значення незмінних ідентифікаційних даних та права власності?

Як і у випадку з Web 2.0, організації повинні ретельно продумати питання, пов'язані з дизайном, політикою, правами людини та монетизацією Web 3.0.

Економічні стимули та соціальні ризики. Мікроекономіки, валюти та інші фінансові активи вбудовані в більшість ранніх додатків Web 3.0 і цифрових спільнот. Вони породжують нові стимули і стримуючі фактори, які змінюють розрахунок ризиків. Вбудовані економічні архітектури Web 3.0 створюють чіткі стимули для зловмисників у порівнянні з традиційними хмарними або IT-розгортаннями. У традиційних середовищах послуги і дані часто використовуються без чіткої або негайної грошової вигоди. У блокчейн-додатках, навпаки, значна цінність часто вже закодована безпосередньо в блокчейні.

Бізнес також повинен оцінювати Web 3.0 з точки зору споживчих і пов'язаних з ними правових, екологічних і суспільних ризиків. Оскільки поняття індивідуальної власності, фінансованої участі вбудовані в Інтернет, бізнес-лідери, а також ті, хто розробляє та захищає екосистему Web 3.0, стикаються з кількома питаннями, які впливають на безпеку організації та окремих осіб:

– як бізнес може підтримати доступність і уникнути поглиблення цифрової та фінансової дискримінації?

– як організації можуть підтримувати соціальне та екологічне покращення, коли користувацький інтерфейс капіталізований, а взаємодія визначається токенізацією, штучним дефіцитом або іншими сигналами репутації, які можна купити?

– як традиційний бізнес буде взаємодіяти з децентралізованими автономними організаціями, заснованими на Web 3.0, і які юридичні "обгортки" забезпечать захист?

І найголовніше, як організації будуть зміцнювати довіру окремих учасників і бізнесу в середовищі Web 3.0?

Обговорення результатів дослідження. У ході дослідження авторами розглянуто основні пріоритетні напрямки в області кібербезпеки з огляду на динамічний прогрес технологій Web 3.0. По-перше, ми ідентифікували основні потенційні загрози та ризики у сфері кібербезпеки для Web 3.0, які включають безпеку протоколів децентралізації, консенсусу, захисту розумних контрактів та користувачів, а також проблеми конфіденційності та анонімності. Серед результатів дослідження співвідношення між технологіями Web 3.0 та кібербезпекою слід виділити ріст взаємозалежності та поступове створення нових ресурсних осередків. Це дозволяє забезпечити рівень конфіденційності і безпеки, проте водночас ставить нові глобальні ризики та дає можливість для атак або маніпуляцій. Далі, важливим напрямком було впровадження правових механізмів, політики та регулятивних засад, які підтримують нормальний розвиток екосистеми, гарантують права користувачів, а також прийняття стандартів доступу та контролю блокчейн технологій. У подальшому, у висновках даного дослідження акцент робиться на відповідальному підході до аналізу майбутнього Інтернету та переходу до Web 3.0. Системне вирішення проблем кібербезпеки під час впровадження нових технологічних підходів дозволить досягнути глобальних цілей забезпечення прозорості, відкритості та стабільності віртуального простору в цифрову епоху Web 3.0.

Висновки та перспективи подальших досліджень. Отже, авторами було виявлено та проаналізовано основні аспекти, які потребують уваги, стратегічного планування та реалізації в плані покращення кібербезпеки в екосистемі Web 3.0. Технологія є новою та досі розвивається, що наголошує на потребі вивчення та аналізу. Також для подальших досліджень можна зосередити увагу на штучному інтелекті.

ШІ відіграє важливу роль у розвитку Web 3.0, оскільки ця технологія дозволяє створювати більш розумні та ефективні децентралізовані системи. За його допомогою можна підвищити точність і швидкість обробки даних, забезпечити автоматизацію процесів і підвищити рівень безпеки в децентралізованих системах. Наприклад, ШІ може використовуватися для розпізнавання образів і тексту, що дозволяє розуміти й аналізувати

великі обсяги даних, для прогнозування поведінки користувачів і виявлення потенційних загроз безпеці. Однак з розвитком ШІ появляються нові проблеми та виклики, пов'язані з етикою та безпекою. Так, можуть виникати питання щодо приватності і захисту даних, які збираються та обробляються системами ШІ, може бути важко зрозуміти, як приймаються рішення та контролюється поведінка систем ШІ. Тому важливо забезпечити розробку та використання AI з дотриманням етичних принципів і найкращих практик у сфері кібербезпеки. Наприклад, можна застосовувати методи шифрування даних і забезпечення приватності, щоб захистити особисту інформацію користувачів, а також використовувати технології блокчейну і розумних контрактів для забезпечення безпеки та довіри до систем ШІ. Таким чином, ШІ є важливою складовою Web 3.0, проте його розвиток пов'язаний з новими викликами та проблемами, які потребують використання етичних принципів і заходів забезпечення кібербезпеки. Для досягнення цих цілей необхідно поєднувати різні технології і методи: машинне навчання, глибинне навчання, нейронні мережі, обробку природньої мови, аналіз даних, блокчейн та ін. Однією з найважливіших проблем, пов'язаних з розвитком ШІ в Web 3.0, є питання безпеки. Так, ШІ може стати предметом атаки з боку зловмисників, які можуть намагатися зламати системи та отримати доступ до конфіденційної інформації. Для запобігання таким атакам необхідно застосовувати заходи кібербезпеки, передусім шифрування даних, аутентифікацію користувачів, контроль доступу до ресурсів. Однак тоді виникають етичні питання щодо розробки і використання ШІ в Web 3.0. Так, можуть виникати проблеми з автоматизацією процесів і заміною людей роботами, зі збереженням приватності і захистом прав користувачів.

Поєднання Web 3.0 і ШІ може стати потужним рушієм інновацій у цифровому світі. Використання децентралізованих технологій разом із ШІ може допомогти вирішити ключові проблеми, пов'язані з безпекою і приватністю в Інтернеті.

У результаті, співпраця Web3 та ШІ відкриває нові горизонти для розвитку технологій, які можуть революціонізувати Інтернет. Завдяки цьому симбіозу користувачі можуть отримати кращий контроль над своїми даними та забезпечити більш сталий та справедливий розвиток Інтернет-технологій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Y. Sompolinsky, and A. Zohar, "Secure high-rate transaction processing in bitcoin", in *Proc. International Conference on Financial Cryptography and Data Security (FC)*, San Juan, Puerto Rico, 2015, pp. 507-527. doi: https://doi.org/10.1007/978-3-662-47854-7_32.

[2] О. Ящик, І. Твердохліб Ю. Франко, та М. Ожга, "Використання технології блокчейн для забезпечення автоматизації управління освітніми документами", *Наукові записки Тернопільського національного педагогічного університету. Серія: педагогіка*, т. 1, № 2, с. 113-120, 2023. https://doi.org/10.25128/2415-3605.22.2.14.

[3] І. Гевко, О. Ящик, Т. Савчин, та Л. Гільтай, "Кібербезпека в децентралізованій інтернет-екосистемі Web 3.0", *Наукові записки Тернопільського національного педагогічного університету. Серія: педагогіка*, т. 1, № 1, с. 61-68, 2023. doi: https://doi.org/10.25128/2415-3605.23.1.8.

[4] К. Некіт, "Переваги та недоліки смарт-контрактів як підстав виникнення права власності", *Вісник НТУУ "КПІ" Політологія. Соціологія. Право*, № 3 (47), с. 101-105, 2020, doi: https://doi.org/10.20535/2308-5053.2020.3(47).229494.

[5] M. Ragnedda, and G. Destefanis, *Blockchain and Web 3. 0: Social, Economic, and Technological Challenges*. Abingdon, UK: Taylor & Francis Group, 2019.

[6] "Cybersecurity in web 3.0: A new way of protecting systems", *Strike: Continuous Security & Pentesting*. [Online]. Available: https://strike.sh/blog/web3.0-cybersecurity. Accessed on: Aug. 19, 2023.

[7] "Smart contract security challenges", Web3 University – Your Guide to Blockchain Development. [Online]. Available: https://www.web3.university/tracks/create-a-smart-contract/smart-contract-security-challenges. Accessed on: Sep. 19, 2023.

[8] J. Groopman, “Web 3.0 security risks: What you need to know”, *TechTarget*. [Online]. Available: https://www.techtarget.com/searchsecurity/tip/Top-3-Web3-security-and-business-risks. Accessed on: Sep. 19, 2023.
[9] K. Huang, and W. Ma, *Blockchain and Web3: Building the Cryptocurrency, Privacy, and Security Foundations of the Metaverse*. Hoboken, NJ, USA: Wiley & Sons, 2022.
[10] Ethereum. [Online]. Available: https://ethereum.org/uk. Accessed on: Sep. 19, 2023.
[11] “Безпека у Web3: Найкращі практики для майбутнього, орієнтованого на конфіденційність”, *Binance Blog*. [Електронний ресурс]. Доступно: https://www.binance.com/uk-UA/blog/ecosystem/безпека-у-web3-найкращі-практики-для-майбутнього-орієнтованого-на-конфіденційність-3731431418476279097. Дата звернення: Сер. 19, 2023.
[12] R. Browne, “Web inventor Tim Berners-Lee wants us to 'ignore' Web3: 'Web3 is not the web at all’”, *CNBC*. [Online]. Available: https://www.cnbc.com/2022/11/04/web-inventor-tim-berners-lee-wants-us-to-ignore-web3.html. Accessed on: Sep. 19, 2023.
[13] N. Ivanenko, “Tim berners-lee calls cryptocurrency “dangerous” and compares it to gambling”, *Mezha.Media*. [Online]. Available: https://mezha.media/en/2023/02/20/tim-berners-lee-calls-cryptocurrency-dangerous-and-compares-it-to-gambling. Accessed on: Sep. 19, 2023.
[14] J. J. DeLuccia, *The NFT & Crypto Currency Security Guide: Must Have Knowledge to Navigate, Purchase, Own, and Trade in the World of Cryptocurrency*. Independently published, 2022.
[15] Г.І. Радельчук, та М.Л. Хорошун, “Концепції проектування децентралізованої платіжної системи з власною цифровою валютою на базі блокчейн-платформи ethereum”, *Вісник ХНУ. Техн. науки*, том. 1, № 4, с. 89-93, 2020. doi: https://doi.org/10.31891/2307-5732-2020-287-4-89-93.
[16] П. Кравченко, Б. Скрябін, та О. Дубініна, *Блокчейн і децентралізовані системи*. Харків, Україна: ПРОМАРТ, 2020.
[17] P. de Filippi, and A. Wright, “Blockchain and the law: The rule of code”, Cambridge, Mass, USA: Harvard University Press, 2018, doi: https://doi.org/10.1111/1468-2230.12459.
[18] R. Taş, “Smart contract security vulnerabilities”, *Erzincan University Journal of Science and Technology*, vol. 16, iss. 1, pp. 196-211, 2023. doi: https://doi.org/10.18185/erzifbed.1105551.
[19] “Соцмережі зробили зі штучного інтелекту хама і расиста”, *Корреспондент.net*. [Електронний ресурс]. Доступно: https://ua.korrespondent.net/lifestyle/3656008-sotsmerezhi-zrobyly-zi-shtuchnoho-intelektu-khama-i-rasysta. Дата звернення: Сер. 23, 2023.

Стаття надійшла до редакції 30.08.2023.

REFERENCE

[1] Y. Sompolinsky, and A. Zohar, “Secure high-rate transaction processing in bitcoin”, in *Proc. International Conference on Financial Cryptography and Data Security (FC)*, San Juan, Puerto Rico, 2015, pp. 507-527. doi: https://doi.org/10.1007/978-3-662-47854-7_32.
[2] O. Yashchyk, I. Tverdokhlib, Y. Franko, and M. Ozhha, “Using blockchain technology for security automation of management of educational documents”, *Scientific Issues Ternopil Nat. Pedagogical University. Series: Pedagogy*, vol. 1, iss. 2, pp. 113-120, 2023. doi: https://doi.org/10.25128/2415-3605.22.2.14.
[3] H. Hevko, O. Yashchyk, T. Savchyn, and L. Hiltai, “Cyber security in decentralized web 3.0 internet ecosystem”, *Scientific Issues Ternopil Nat. Pedagogical University. Series: Pedagogy*, vol. 1, iss. 1, pp. 61-68, 2023. doi: https://doi.org/10.25128/2415-3605.23.1.8.
[4] K. Nekit, “Advantages and disadvantages of smart-contracts as the basis for the emergence of ownership”, *Nat. Tech. Univ. Ukraine Journal. Political Science. Sociology. Law*, vol. 3, iss. 47, pp. 101-105, 2020, doi: https://doi.org/10.20535/2308-5053.2020.3(47).229494.

[5] M. Ragnedda, and G. Destefanis, *Blockchain and Web 3. 0: Social, Economic, and Technological Challenges*. Abingdon, UK: Taylor & Francis Group, 2019.
[6] "Cybersecurity in web 3.0: A new way of protecting systems", *Strike: Continuous Security & Pentesting*. [Online]. Available: https://strike.sh/blog/web3.0-cybersecurity. Accessed on: Aug. 19, 2023.
[7] "Smart contract security challenges", Web3 University – Your Guide to Blockchain Development. [Online]. Available: https://www.web3.university/tracks/create-a-smart-contract/smart-contract-security-challenges. Accessed on: Sep. 19, 2023.
[8] J. Groopman, "Web 3.0 security risks: What you need to know", *TechTarget*. [Online]. Available: https://www.techtarget.com/searchsecurity/tip/Top-3-Web3-security-and-business-risks. Accessed on: Sep. 19, 2023.
[9] K. Huang, and W. Ma, *Blockchain and Web3: Building the Cryptocurrency, Privacy, and Security Foundations of the Metaverse*. Hoboken, NJ, USA: Wiley & Sons, 2022.
[10] Ethereum. [Online]. Available: https://ethereum.org/uk. Accessed on: Sep. 19, 2023.
[11] "Security on the Web3: Best Practices for a Privacy-Driven Future", *Binance Blog*. [Online]. Available: https://www.binance.com/uk-UA/blog/ecosystem/безпека-у-web3-найкращі-практики-для-майбутнього-орієнтованого-на-конфіденційність-3731431418476279097. Accessed on: Sep. 19, 2023.
[12] R. Browne, "Web inventor Tim Berners-Lee wants us to 'ignore' Web3: 'Web3 is not the web at all'", *CNBC*. [Online]. Available: https://www.cnbc.com/2022/11/04/web-inventor-tim-berners-lee-wants-us-to-ignore-web3.html. Accessed on: Sep. 19, 2023.
[13] N. Ivanenko, "Tim berners-lee calls cryptocurrency "dangerous" and compares it to gambling", *Mezha.Media*. [Online]. Available: https://mezha.media/en/2023/02/20/tim-berners-lee-calls-cryptocurrency-dangerous-and-compares-it-to-gambling. Accessed on: Sep. 19, 2023.
[14] J. J. DeLuccia, *The NFT & Crypto Currency Security Guide: Must Have Knowledge to Navigate, Purchase, Own, and Trade in the World of Cryptocurrency*. Independently published, 2022.
[15] G. Radelchuk, and M. Khoroshun, "Concepts of designing a decentralized payment system with its own digital currency based on the ethereum blockchain platform", *Bulletin of KhNU. Technical of science*, vol. 1, iss. 4, pp. 89-93, 2020. doi: https://doi.org/10.31891/2307-5732-2020-287-4-89-93.
[16] P. Kravchenko, B. Skryabin, and O. Dubinina. *Blockchain and decentralized systems*, Kharkiv, Ukraine: PROMART, 2020.
[17] P. de Filippi, and A. Wright, "Blockchain and the law: The rule of code", Cambridge, Mass, USA: Harvard University Press, 2018, doi: https://doi.org/10.1111/1468-2230.12459.
[18] R. Taş, "Smart contract security vulnerabilities", *Erzincan University Journal of Science and Technology*, vol. 16, iss. 1, pp. 196-211, 2023. doi: https://doi.org/10.18185/erzifbed.1105551.
[19] "Social networks have turned artificial intelligence into a brat and a racist", *Correspondent.net*. [Online]. Available: https://ua.korrespondent.net/lifestyle/3656008-sotsmerezhi-zrobyly-zi-shtuchnoho-intelektu-khama-i-rasysta. Accessed on: Sep. 23, 2023.

ANASTASIIA TOLKACHOVA
ANDRIAN PISKOZUB

ANALYSIS OF THREATS AND RISKS IN THE WEB3 ECOSYSTEM IN THE SECURITY CONTEXT

This research article discusses current and promising issues in the field of cybersecurity, in particular, the analysis of potential threats and risks of Web3 development. Web3 is a new generation of the Internet based on blockchain technology, decentralization, cryptography, and smart contracts. This approach aims to improve security, privacy, and user rights in the virtual environment, but

without proper understanding, it can carry the opposite risk. The article begins with an analysis of recent research and issues. The authors discuss potential threats and risks, including possible attacks on decentralization protocols, censorship manipulation, attacks on blockchain protocols, attempts to break the consensus system, and unfair smart contract transactions. The article discusses a number of vulnerabilities and attacks that can harm the new Web 3.0 technology. The article describes new threats to the privacy of users and their digital assets, including the use of anonymization technologies and countermeasures by criminal organizations or government agencies. The article also emphasizes the importance of discussing the legal aspects of Web3 integration, finding an optimal balance between the regulation of the digital space and users' rights to privacy and autonomy. Global challenges require international cooperation and standardization of regulatory rules in this area. The results of the study demonstrate that a conscious approach to analyzing Web3 threats is the key to building a secure future for the Internet. This article contributes to the dissemination of information and knowledge about possible risks, opens up new horizons for scientific research, practical implementation of cybersecurity measures, and political dialogue in the Web3 era.

Keywords: blockchain, vulnerabilities, decentralization, information security, information protection, smart contracts, Web3, NFT.

Толкачова Анастасія Юріївна, студентка, кафедра захисту інформації Національного університету “Львівська політехніка”, Львів, Україна, ORCID 0000-0002-8196-7963, tolkachova.nastia@gmail.com.

Піскозуб Андріян Збігнєвич, кандидат технічних наук, доцент кафедри захисту інформації Національного університету “Львівська політехніка”, Львів, Україна, ORCID 0000-0002-3582-2835, azpiskozub@gmail.com.

Tolkachova Anastasiia, student, department of information security, Lviv Polytechnic National University, Lviv, Ukraine.

Piskozub Andrian, PhD. in engineering, associate professor, department of information security, Lviv Polytechnic National University, Lviv, Ukraine.