УДК 004.8:65.05:681.5 DOI: 10.31673/2518-7678.2023.020909

**Вишнівський О.В.,** аспірант; **Зінченко О.В.,** д.т.н.,
**Катков Ю.І.,** д.т.н., **Березовська Ю.В.,** PhD,
**Колдун П.П.**

# АНАЛІЗ ФАКТОРІВ УРАЗЛИВОСТІ ТЕХНОЛОГІЇ WEB 3.0

**Vyshnivskyi O.V., Zinchenko O.V., Katkov Y.I., Berezovska Yu.V., Coldun P.P. Analysis of vulnerability factors of WEB 3.0 technology.** The article is devoted to critical aspects during the implementation of Web-3.0 technology. The task is set: based on the analysis of the implementation of Web-3.0 technology to solve a number of tasks, namely: blockchain-based decentralization; creation of general accessibility; increasing trust in sites; increasing the security of personal information from hackers; ensuring true ownership of authors' information; lack of censorship; improvement of social interaction; use of the Internet of Things is compatible with virtual or augmented reality; application of artificial intelligence – consider a zero-day exploit for Web-3.0. A zero-day exploit indicates that the vendor or developer has just become aware of the vulnerability and has "zero days" to fix it. A zero-day attack occurs as a result of attackers exploiting a vulnerability (critical points) before the developers managed to fix it. To solve this problem in the article: a description of the main differences between the Web-3.0 construction architecture and Web-2.0 is made; the analysis of the tasks of Oprah Winfrey Network of the Web-3.0 architecture was carried out; consider the possibilities of: external interface (design and interface of web applications), server part (based on decentralized technologies, primarily dApp, which uses the advantages of blockchain: transparency, reliability and immutability of data.), database (stores data about users, their messages , tags and comments); an analysis of possible threats and vulnerabilities due to the introduction of Web-3.0 technology before the start of the zero-day exploit was performed. Based on the performed analysis, the following conclusions are drawn: that the vulnerability is related to scalability, limited transaction throughput and computing power, security, complexity, compatibility; that Web-3.0 creates many conditions that can be useful to people, but the introduction of new Web-3.0 capabilities leads to the emergence of new threats or vulnerabilities that can be used by attackers to harm people. This requires considering the possible impact of threats, identifying possible vulnerabilities in Web-3.0 technology before the start of a zero-day exploit, that is, it requires the need to investigate the possibility of the appearance of new vulnerabilities.

**Keywords**: Web-3.0, vulnerability, zero-day exploit.

**Вишнівський О.В., Зінченко О.В., Катков, Ю.І., Березовська Ю.В., Колдун П.П. Аналіз факторів уразливості технології WEB 3.0.** Стаття присвячена критичним аспектам під час впровадження технології Web-3.0. Ставиться завдання: на основі аналізу впровадження технології Web-3.0 для вирішення множини завдань, а саме: децентралізації на основі блокчейну; створення загальної доступності; підвищення довіри сайтам; підвищення безпеки персональної інформації від хакерів; забезпечення справжній власності на інформацію авторів; відсутність цензури; поліпшення соціальної взаємодії; використання інтернет речей сумісно з віртуальною або доповненою реальністю; застосовування штучного інтелекту – розглянути експлойт нульового дня для Web-3.0. Експлойт нульового дня показує, що постачальник або розробник щойно дізналися про уразливість і вони мають «нуль днів» її виправлення. Атака нульового дня відбувається внаслідок використання зловмисниками уразливості (критичних місць) до того, як розробникам вдалося її виправити. Для вирішення цього завдання в статті: зроблено опис основних відмінностей архітектури побудови Web-3.0 від Web-2.0; виконаний аналіз завдань Oprah Winfrey Network архітектури Web-3.0; розглянуто можливості: зовнішнього інтерфейсу (дизайн та інтерфейс веб-програм), серверної частини (ґрунтується на децентралізованих технологіях, насамперед, dApp, яка використовує переваги блокчейна: прозорість, надійність та незмінність даних), бази даних (зберігає дані про користувачів, їх повідомлення, теги та коментарі); виконано аналіз можливих загроз та уразливості внаслідок впровадження технології Web-3.0 до початку експлойту нульового дня. На основі виконаного аналізу робляться висновки: що уразливість пов’язана з масштабованістю, обмеженою пропускною спроможністю транзакцій та обчислювальної потужності, безпекою, складністю, сумісністю; що Web-3.0 створює багато умов, які можуть бути корисні людям, але впровадження нових можливостей Web-3.0 призводить до появи нових загроз або уразливості, які можуть бути використані зловмисниками для нанесення шкоди людям. Це вимагає розглянути можливий вплив загроз, визначити можливі уразливості в технології Web-3.0 до початку експлойту нульового дня, тобто вимагає необхідність дослідження можливості появи нових уразливих місць.

**Ключові слова:** Web-3.0, уразливість, експлойт нульового дня

**Вступ**

З 1990-х років веб-технології набули широкого поширення та створили інформаційні послуги. Сьогодні існування інформаційного простору не можливе без всесвітньої павутини WWW (World Wide Web), яка є розподіленою системою, що надає доступ до пов'язаних між собою документів, розташованих на різних комп'ютерах, які підключені до Інтернету. На веб-серверах розгорнуті веб-технології у вигляді інтегрованих різноманітних платформ для створення послуг користувачам через додатки, пошукові технології, електронні ресурси, аудіовізуальні інструменти, блоги та соціальні мережі. Сукупність WWW та веб-технології є Інтернетом, що надає різноманітні Інтернет-послуги, а саме: послуги доступу до різних комунікаційних служб, які пропонують обмін інформацією з окремими особами чи групами; послуги інформаційно-пошукових служб; послуги доступу до веб-сервісів та їх додатків; послуги відео та аудіо конференцій у соціальних та спеціальних мережах. Звідси треба розуміти, що Інтернет утворюють сотні мільйонів веб-серверів, які з'єднані в мережу, що WWW не є Інтернетом, що WWW лише використовує мережу веб-серверів Інтернету як середовище передачі даних за допомогою протоколу HTTP передачі даних. Тоді стає зрозумілим, що за допомогою веб-серверів можна створювати різні версії WWW.

Відомо, що головною особливістю побудови WWW є те, що ресурси базуються на технології гіпертексту та принципах семантичної павутини.

*Технології гіпертексту* у найпростішому вигляді це така програма, що отримує по мережі HTTP-запит на певний ресурс, знаходить відповідний файл на локальному жорсткому диску і відправляє його по мережі комп'ютеру. Гіпертекстові документи, що розміщуються у WWW, називаються веб-сторінками. Декілька веб-сторінок, об'єднаних спільною темою або дизайном, а також пов'язаних між собою посиланнями і зазвичай знаходяться на тому самому веб-сервері, називаються веб-сайтом. Для завантаження та перегляду веб-сторінок використовуються спеціальні програми – браузери. Для покращення візуального сприйняття Інтернету широко використовується технологія Cascading Style Sheets (CSS), яка дозволяє задавати єдині стилі оформлення для багатьох веб-сторінок. Також застосовується система позначення ресурсів Uniform Resource Name (URN). CSS – це комп'ютерна мова для компонування та структурування веб-сторінок (HTML або XML). Ця мова містить елементи кодування і складається з цих "каскадних таблиць стилів", які однаково називаються файлами CSS (*.css). CSS призначений для поділу вмісту та подання, включаючи макет, кольори та шрифти. Такий поділ може: покращити доступність контенту; забезпечити більшу гнучкість та контроль у специфікації характеристик презентації; дозволити кільком веб-сторінкам спільне форматування; при увімкненні кешування файлу *.css, підвищується швидкість завантаження сторінки між сторінками, які спільно використовують файл та його форматування; робити можливим подання однієї й тієї ж сторінки розмітки в різних стилях для різних методів рендерингу, наприклад, на екрані, друку, голосом (через мовний браузер або програму читання з екрана). URN – це постійний ідентифікатор інтернет-ресурсів. По суті, це незалежний від розташування рядок символів, який ідентифікує кожен ресурс в Інтернеті, незалежно від його форми, як-от веб-сайт або електронна пошта.

*Семантична павутина* (*Semantic Web)* – це бачення розширення існуючої Всесвітньої павутини, яка надає програмам машинно-інтерпретовані метадані опублікованої інформації та даних. Тому слово «семантичний» вказує на можливість машинної обробки семантичних метаданих. Семантичні метадані є семантичними тегами, які додаються до звичайних веб-сторінок для кращого опису їх значення. Такі метадані значно полегшують пошук веб-сторінок на основі семантичних критеріїв. Створення семантичної павутини – це надбудова над існуючою Всесвітньою павутиною, яка покликана зробити інформацію, що розміщена в мережі, більш зрозумілою для комп'ютерів. Семантична павутина відкриває доступ до чітко структурованої інформації для будь-яких програм, незалежно від платформи та незалежно від мов програмування. Програми зможуть самі знаходити потрібні ресурси, обробляти інформацію, класифікувати дані, виявляти логічні зв'язки, робити висновки та навіть приймати рішення на основі цих висновків. Для створення зрозумілого комп'ютера опису ресурсу, в

семантичній павутині використовується формат RDF (Resource Description Framework), який заснований на синтаксисі XML і використовує ідентифікатори URI для позначення ресурсів. Новинки у цій галузі: RDFS (англ. RDF Schema) і SPARQL (англ. Protocol And RDF Query Language), нова мова запитів для швидкого доступу до даних RDF. Іншими словами, Semantic Web, пов'язане з трьома речами: автоматизацією пошуку інформації, Інтернетом речей, персональними помічниками. Щоб семантична павутина функціонувала, комп'ютери повинні мати доступ до структурованих наборів інформації та наборів правил виведення, які вони можуть використовувати для автоматизованих міркувань. Для цього ми додаємо додаткові дескриптори даних до існуючого контенту та даних в Інтернеті. У результаті комп'ютери здатні робити осмислені інтерпретації, подібно до того, як люди обробляють інформацію для досягнення своїх цілей. Кінцева мета семантичної мережі полягає в тому, щоб дозволити комп'ютерам краще маніпулювати інформацією від нашого імені. Прикладами є сайти: Best Buy, BBC World Cup, Google, Facebook та Flipboard.

Відомо, що за час існування та використання користувачами Інтернет було декілька ітерацій розвитку Web-технологій, а саме: Web-1.0 та Web-2.0, Web-3.0. Трансформація Web-технологій була викликана зміною потреб користувачів Інтернету [1].

Web-1.0 була першою ітерацією, коли Інтернет надавав послуги лише для читання, тому що більшість людей, які використовували Web-1.0, були лише споживачами. Розробники створювали контент через статичні HTML-сторінки та надавали його публіці на сайтах. Інтернет був схожий на бібліотеку, яку люди відвідували за інформацією, а автори були розробниками та технічними фахівцями. Основні тенденції Web-1.0 включали турботи про проблеми безпеки та приватності в односторонньому потоці інформації через веб-сайти, що містять матеріал тільки для читання. Web-1.0 не дозволяв людям робити багато речей, які ми можемо робити зараз, наприклад, спілкуватися з друзями або змінювати сайти. Люди могли лише дивитися та читати те, що було в Інтернеті. Але з часом користувачі набували навички роботи в Інтернет, тому у них виникли нові потреби – створювати контент за допомогою соціальних платформ. Web-1.0 проіснував приблизно з 1991 по 2004 рік.

Web-2.0 був другою ітерацією, яким ми користуємося зараз. Він створив інтерактивний Інтернет, тобто надавав послуги для читання та запису. Web-2.0 надавало споживачі право створювати контент за допомогою соціальних платформ, таких як Facebook, Twitter тощо. Він дозволяє людям створювати такі речі, як повідомлення, фотографії, відео та ділитися ними з іншими. Web-2.0 простий у використанні, і завдяки цій простоті, все більше людей у всьому світі стають творцями. Web-2.0 також полегшив людям використання Інтернету на мобільних телефонах. Web-2.0 існує і сьогодні але він має недоліки. У Web-2.0 є можливість інтернет-компаніям використовувати інформацію про людей, щоб показувати їм рекламу та нав'язувати їм використання своїх товарів та послуг. Виникли проблеми з тим, що ці компанії можуть контролювати та маніпулювати інформацією про людей та не завжди її захищають. Вони можуть використовувати дані для будь-яких цілей. Крім того, виток даних став повсюдним для будь-яких платформ. У міру поширення Інтернету "цифрова особистість" стала важливою соціальною та політичною темою. У даний час всі великі платформи, такі як Google, Facebook, Instagram та ін. повністю контролюють персональні дані. Існує щонайменше три аспекти, якими характеризується ваша цифрова особистість: ваша IP-адреса, особиста інформація та логіни, цифрові підписи та метадані. Загрози втрати цих даних поставить під загрозу вашу репутацію, фінансовий стан, права власності на житло та багато іншого – у разі їх зловмисної крадіжки та неправомірного використання. Фактично може порушити всі інші аспекти вашого життя, особливо зараз, коли більшість зв'язків, які ми встановлюємо, знаходяться в Інтернеті.

Web-3.0 – це ідея нової версії Всесвітньої павутини, що включає такі концепції, як децентралізація (прагне зробити інтернет менш контрольованим компаніями), загальна доступність (люди можуть користуватися інтернетом більш вільно та легко), система без довіри (люди повинні довіряти лише мережі, а не компаніям), технології блокчейну (буде використовуватися блокчейн та цифрові гроші для фінансової свободи, таких як децентралізовані фінанси (DeFi) або криптовалюти), підвищена безпека вашої інформації

(використовуватиме нові способи зберігання та захисту інформації від хакерів), справжня власність на вашу інформацію (люди матимуть більший контроль над своєю інформацією і навіть зможуть заробляти на ній гроші за допомогою економіки на основі токенів), відсутність цензури (не матиме центрального органу, який може несправедливо цензурувати людей), поліпшена соціальна взаємодія (буде використовувати нові технології, такі як віртуальна реальність та інтернет речей, доповнена реальність та штучний інтелект, щоб зробити онлайн-взаємодію кращою, можна використовувати аватари для спілкування з іншими людьми у 3D-світах, грати в ігри та навіть працювати віддалено). Необхідно підкреслити, що Web-3.0 поєднує в собі позитивні сторони Web-1.0 та Web-2.0. Він хоче дати людям більше контролю над своєю інформацією та над тим, як вони використовують Інтернет [1, 2]. Але впровадження вказаних концепцій створює умови для появи уразливості.

Таким чином, нова версія Всесвітньої павутини Web-3.0 створює багато умов, які можуть бути корисні людям. Але впровадження нових можливостей призводить до появи нових загроз або уразливості, які можуть бути використані зловмисниками для нанесення шкоди людям. Це вимагає розглянути можливий вплив загроз, визначити можливі уразливості в технології Web-3.0 до початку експлойту нульового дня, тобто вимагає необхідність дослідження можливості появи нових уразливих (критичних) місць. Експлойт нульового дня показує, що постачальник або розробник щойно дізналися про уразливість і вони мають «нуль днів» для її виправлення. Атака нульового дня відбувається внаслідок використання зловмисниками уразливості (критичних місць) до того, як розробникам вдалося її виправити. Це є актуальною та своєчасною задачею для дослідження.

**Постановка завдання**

Розглядається проблема виникнення можливих загроз та уразливості внаслідок впровадження технології Web-3.0 до початку експлойту нульового дня. Треба визначити, в якому вигляді необхідно застосовувати технологію Web-3.0 для вирішення безлічі завдань покращення всесвітньої павутини WWW та вказати загальний перелік критичних місць, де застосування технології Web-3.0 буде мати вразливості.

**Аналіз останніх наукових досліджень**

Впровадження технології Web-3.0 обговорюється починаючи з 2010 року. Інтегрований огляд літератури, що досліджує природу чуйних, семантичних та інтерактивних технологій Web-3.0, які застосовуються для академічних бібліотек був виконаний в [2]. Авторами проаналізовано вибірку досліджень, щоб охарактеризувати тенденції розвитку та впровадження Web-3.0. У цьому огляді показано, як технології Web-3.0 покращують послуги в їхній цілісній концептуалізації та переходять до більш надійної, інклюзивної та адаптованої фази своїх послуг та інновацій. З іншого боку технологія Web-3.0 розглянута в [3], де розглядаються питання застосування Web-3.0 на базі технологій хмарних обчислень. У [4] розглядаються застосування Web-3.0 в галузі когнітивної та освітньої психології. Всі ці роботи аналізували позитивні якості застосування технології Web-3.0. Але були також роботи, де аналізувалися негативні аспекти, наприклад, у [5] автори розглядали скептицизм до Web-3.0, в [6] вказуються негативні наслідки впровадження технології Web-3.0. Можна навести десятки прикладів прихильників та противників впровадження технології Web-3.0. Тобто, що для одних людей Web-3.0 звучить як ще одне модне слово, яке використовується для просування крипто-шахрайства або отримання ажіотажу, а для інших це децентралізовані веб-додатки, в яких мережа людей контролює свій власний шматок інтернету, де дані керуються за допомогою смарт-контрактів та криптографії, а не належать Google, Meta (Facebook) і Amazon. Тому зрозуміло, що технологія Web-3.0. має право на існування. І тепер важливо вирішити її центральну проблему, яка полягає в тому, щоб визначити, які уразливості може створити нова технологія для соціального, економічного та політичного життя суспільства, тому що досвід розвитку інформаційних технологій вказує, що будь-яка нова технологія традиційно має як

позитивні, так і негативні сторони. Тому пошук уразливості нової технології Web-3.0 є актуальним та своєчасним.

**Виклад основного матеріалу дослідження**

Розгляд проблеми виникнення можливих загроз та уразливості WWW внаслідок впровадження технології Web-3.0 до початку експлойту нульового дня необхідно розпочати з визначення понять загроза та уразливість.

*Загроза* в інформаційних технологіях – це будь-які обставини або події, що виникають у зовнішньому середовищі, які можуть бути причиною порушення політики безпеки інформації і (або) нанесення збитків інформаційній системі. Загроза проявляється відносно уразливих елементів, які існують у будь-якій системі.

*Уразливість* – це параметр, що характеризує можливість нанесення описуваній системі пошкоджень будь-якої природи тими чи іншими зовнішніми засобами чи факторами. Уразливість проявляється, як певна помилка або недолік, які дають змогу зловмиснику отримати несанкціонований позитивний для нього результат, наприклад, використання уразливості програмного забезпечення (в операційній системі або програмі) є загальний спосіб встановлення шкідливого коду на комп'ютер.

На даний момент багато зловмисників фокусують свої зусилля саме на виявленні невідомих уразливостей в різних елементах систем. У технології Web-3.0 може бути не тільки в програмному забезпеченні, а й у соціальних, економічних та політичних аспектах. Це обумовлено високою ефективністю використання уразливості, що, в свою чергу, пов'язано з двома фактами – високим поширенням уразливого програмного забезпечення (саме таке програмне забезпечення, як правило, атакують) і деяким часовим проміжком між виявленням уразливості компанією-розробником програмного забезпечення і випуском патчів. У зв’язку з цим виникає поняття уразливість нульового дня (загроза нульового дня), наприклад, недолік у безпеці програмного забезпечення, який невідомий тому, хто зацікавлений у його усуненні, приміром, розробнику. Звідси уразливість нульового дня (Zero-day / 0 day) – це уразливість будь-якого елементу системи, яка ще невідома користувачам чи розробникам та проти яких ще не розроблені механізми захисту. Для визначення уразливості нульового дня існує поняття експлойту нульового дня.

*Експлойт* (exploit, експлуатувати) нульового дня – це загальний термін, що описує нещодавно виявлені уразливості у системі безпеки, які можуть бути використані зловмисниками для атаки на систему. Термін «нульовий день» показує, що постачальник або розробник щойно дізналися про уразливість деякого елементу системи, але він має «нуль днів» для її виправлення. Такі уразливі елементи системи підлягають атаці.

*Атака нульового дня* – це коли зловмисники використовують свій експлойт нульового дня для атаки, що часто призводить до таких проблем, як крадіжка особистих даних або їх втрата. Атака нульового дня відбувається внаслідок використання зловмисниками уразливості до того, як розробникам вдалося її виправити.

Таким чином, вказані терміни показують, що у розробників є 0 днів на виправлення дефекту: уразливість або атака стає публічно відомою до моменту початку експлуатації системи виробником. З точки зору впровадження Web-3.0 сьогодні спостерігається момент експлойту нульового дня. Одним зі способів усунення експлойту є завчасний пошук таких критичних місць у системі. Звідси стає зрозумілим важливість попереднього пошуку уразливості Web-3.0 для виправлення помилок до початку її експлуатування.

Якщо розглядати експлойт нульового дня відносно Web-1.0, то у 1980-х роках WWW складався з двох категорій: невеликої групи людей, яка створювала контент для більш широкої аудиторі та великої кількості користувачів, головна мета яких була читання. У цей період виникли такі найпоширеніші загрози при роботі в Інтернеті: загроза зараження операційних систем шкідливим програмним забезпеченням; доступ до небажаного вмісту; контакти з незнайомими людьми-зловмисниками за допомогою чату або електронної пошти.

Якщо розглядати експлойт нульового дня відносно Web-2.0, він складається з мільйонів користувачів, що розробляють контент для широкої аудиторії або читають цей контент. Web-2.0 відрізняється від Web-1.0 тим, що ця інтернет-форма в першу чергу пов'язана з User-generated content (UGC) та додаванням можливостей веб-браузера фреймворками JavaScript.

*UGC* означає контент користувача. За визначенням, контент користувача – це будь-яка форма контенту – текст, публікації, зображення, відео, огляди та ін. – створена окремими людьми (не брендами) і опублікована в Інтернеті або соціальній мережі. UGC забезпечує ефективну розширену взаємодію з іншими пристроями та системами, тобто ця веб-форма відповідала за створення соціальних мереж, партнерських відносин та спільнот. Web-2.0 приділяє більше уваги взаємодії та читанню/запису, тому Web-2.0 називають "соціально-інтерактивною мережею".

*JavaScript-фреймворки* – це набір бібліотек, що містять код, написаний на JavaScript, що значно спрощує життя розробникам програмного забезпечення. Кожен фреймворк JavaScript пропонує готові коди для різних областей та різних цілей розробки програмного забезпечення, що заощаджує час розробника. Ось список деяких популярних фреймворків JavaScript, які потрібно вивчити, щоб йти в ногу із сучасними галузевими вимогами: React, Vue, Angular, Ember, Backbone, Node, jQuery.

Під час використання Web-2.0 виникли такі найпоширеніші загрози при роботі в Інтернеті: загроза зараження шкідливим програмним забезпеченням; доступ до небажаного вмісту; контакти з незнайомими людьми-зловмисниками за допомогою чату або електронної пошти; пошук розваг в Інтернеті; неконтрольовані покупки; розміщення небажаного контенту анонімних авторів; несанкціонований анонімний доступ; витоку інформації; втрата персональних даних; шахрайство; кібервійни; кібертероризм.

Web-3.0 – це нова і майбутня ітерація всесвітньої павутини, загальнодоступної мережі, побудованої на технології розподіленого реєстру, штучного інтелекту та семантичної архітектури, що забезпечує децентралізацію інтернет-середовища, імерсивність, персоналізацію та економіку, що базується на токенах.

*Децентралізація інтернет-середовища* передбачає незалежність від будь-якої центральної влади.

*Імерсивні технології* (immersive – занурювати) – це технології повного або часткового занурення у віртуальний світ або різні види змішання реальної і віртуальної реальності. Імерсивні технології також називають технологіями розширеної реальності. До їх списку входить віртуальна і доповнена реальність, а також панорамні 360° відео. Вони забезпечують ефект повної або часткової присутності в альтернативному просторі і тим самим змінюють призначений для користувача досвід в абсолютно різних сферах. Існують наступні види імерсивних технології:

RR (real reality) – «реальна реальність» або об'єктивна реальність, в якій ми перебуваємо і яку сприймаємо органами чуття;

VR (virtual reality) – віртуальна реальність – повністю змодельована дійсність із застосуванням сучасних технологій. Це не тільки 3D або панорамні 360º сцени, це також звук, тактильні відчуття і навіть запахи;

AR (augmented reality) – доповнена («додана») реальність, тобто ми додаємо в нашу реальну дійсність (RR) елементи віртуальної, змодельованої реальності;

MR (mixed reality) – змішана реальність. По суті, це VR з деякими доповненнями RR або AR із застосуванням окулярів змішаної реальності (Microsoft HoloLens та подібне);

XR (extended reality) – розширена реальність – це загальна назва для AR- і VR-технологій.

Панорамні 360º сцени, фото, відео – контент, що складається з одного 360° або декількох зшитих фото і відео. Поширені також 360°-трансляції.

*Персоналізація* – у Web-3.0 Інтернет знатиме кожного користувача, що дозволить знайти його за тисячами записів, які ми в даний час знаходимо при виконанні пошуку. Тепер він

підлаштовуватиметься під кожну людину, аналізуючи дані та персоналізуючи результати. Web-3.0 надає право власності на ваші цифрові активи. Персоналізація включає використання особистісно-орієнтованого підходу у всіх сферах практики охорони здоров'я та соціальної допомоги. Це означає роботу з цінностями, орієнтованими на людину, включаючи повагу, гідність, розширення прав та можливостей, незалежність, недоторканність приватного життя, вибір, контроль та індивідуальність.

*Економіка, що базується на токенах*. Використання технології блокчейн у Web 3.0 може змінити використання Інтернету. Він може дати Інтернет абсолютно новий вимір. Фізичні особи можуть купувати, володіти, продавати та отримувати прибуток від продажу своїх цифрових матеріалів у вигляді незамінних токенів (Non-Fungible Tokens, NFT).

NFT або невзаємозамінні токени – це свого роду крипто валюта, яка являє собою єдиний у своєму роді цифровий актив або унікальний витвір мистецтва. Фіат і крипто валюти в основному використовуються для транзакційних цілей та є взаємозамінними, що означає, кожну одиницю можна обміняти. Прикладом NFT є: предмети колекціонування: яхт-клуб Bored Ape, Crypto Punks та Pudgy Panda; доменні імена NFT, які надають право власності на доменні імена для вашого веб-сайту або веб-сайтів; музика, коли виконавці можуть токенізувати свою музику, надаючи покупцям права, які артист хоче, щоб вони мали. Сьогодні 1 NFT коштує у доларах: 1 NFT = 0,0194 USD. Можна назвати різні типи NFT:

1. Мистецтво. Мистецтво – найпопулярніша форма NFT. Через це мистецтво також є видом NFT, який продається найкраще. Концепція NFT була чудовою можливістю для художників продавати свої найкращі роботи в Інтернеті, начебто вони були фізичними. Зараз багато з найдорожчих NFT – це витвори мистецтва. За словами Луно, найцінніший з будь-коли проданих NFT називається «КОЖНИЙ ДЕНЬ: ПЕРШІ 5000 ДНІВ» відомого художника Біпла. Цей твір продали за колосальні 69 мільйонів доларів. Є й інші наддорогі NFT, які зламують банківські рахунки мільярдерів. Це стосується й творів відеоарту. Короткі відеоролики та навіть GIF-файли продавалися як гарячі пиріжки на мільйони доларів. Примітно, що зациклене 10-секундне відео під назвою «Перекресток», що зображує оголеного Дональда Трампа, що лежить на землі, було продано за 6,6 мільйона доларів. Це відео також було від Beeple;

2. Музика. Також високо у спектрі NFT знаходиться музика. Музика десятиліттями була взаємозамінним товаром, її записували та розповсюджували на платівках, касетах, компакт-дисках та у цифровому вигляді. Проте останнім часом музиканти та ді-джеї продають свої роботи як NFT, заробляючи деяким із них мільйони доларів за лічені години. Музиканти, як правило, привласнюють лише невелику частину грошей, які приносить їхня музика, за рахунок скорочень стрімінгових платформ та скорочень звукозаписних компаній. Коли справа доходить до NFT, музиканти можуть залишити приблизно 100% коштів, тому багато музикантів звертаються до цього методу;

3. Предмети для відеоігор. Ще одним місцем застосування у просторі NFT є відеоігри. Компанії не продають цілі ігри як NFT. Швидше, вони продаватимуть внутрішньо ігровий контент, такий як скіни, персонажі та інші предмети. Наразі гравцям продаються мільйони копій активів downloadable content (DLC), але актив NFT буде унікальним та ексклюзивним для одного покупця.

DLC, або завантажуваний контент, відноситься до додаткового контенту, що завантажується геймерами для відеоігор після їхнього початкового випуску. Завантажуваний контент – це додатковий контент, який можна придбати в Інтернеті та додати до відеогри для розширення її можливостей: якщо ви купите DLC, у вас буде доступ до нових наборів зброї. Тому розробники можуть продавати звичайний DLC, а потім продавати обмежену версію на ринку NFT;

4. Колекційні картки/колекційні предмети. NFT можна використовувати як цифрові торгові карти. Ми всі знаємо про бейсбольні картки обмеженого випуску, які продаються за тисячі доларів, і ринок NFT не дуже відрізняється. Люди можуть купувати та продавати

віртуальні версії колекційних карток на ринку та зберігати їх так само, як і справжні. І, як і справжні, деякі з них продаються за мільйон доларів. Компанії можуть продавати всі види колекційних предметів на ринку NFT, а не лише колекційні картки. Якщо це щось, що ви вважаєте колекційним, його можна виставити на продаж;

5. Великі спортивні моменти. NFT пропонують те, що насправді немає фізичного еквівалента: пам'ятні спортивні моменти. Це короткі ролики про важливі моменти в історії спорту, такі як новаторські слем-данки або революційні тачдауни. Ці кліпи можуть тривати лише 10 секунд, але продаються за ціною понад 200 000 доларів;

6. Меми. Якщо ви думали, що в Інтернеті немає нічого цікавішого, ви можете купувати та обмінювати мем на ринку NFT. Що приємно, то це те, що в деяких випадках людина в мемі є фактичним продавцем. Деякі з найбільш популярних мемів, такі як Nyan Cat, Bad Luck Brian, Disaster Girl та інші, перебувають у списку і коштують від 30 000 до 770 000 доларів. Найцінніший продаж мемів NFT на сьогоднішній день – це мем Doge, який був проданий за 4 мільйони доларів;

7. Доменні імена. Доменні імена не захищені від певних вимог NFT. Ви можете зареєструвати доменне ім'я та продавати його на ринку NFT, і це дає певні переваги. Зазвичай вам потрібно платити сторонній компанії за керування вашим доменним ім'ям. Якщо ви купите його на ринку NFT, ви зможете претендувати на виняткове право власності на ім'я, за винятком посередників;

8. Віртуальна мода. Звідси віртуальна мода купується і продається на ринку NFT. Ви можете витратити великі гроші на бомби бікіні, але насправді ви не зможете його носити. Люди, які купують модні NFT, натомість прикрашатимуть онлайн-аватари. Це може здатися смішним, але пам'ятайте, що хтось на цій планеті витратив 4 мільйони доларів на створення мема Doge. Володіння віртуальною сумочкою або намистом призначено для більш екстравагантних і модних людей. Зрозуміло, всі вони матимуть унікальний дизайн та обмежену кількість;

9. Різні онлайн-предмети. Інші елементи в цьому списку було легко визначити, але ринок NFT – це своєрідний дикий захід інтернет-торгівлі; це ілюструється крахом ринку NFT, який стався кілька місяців тому.

Звідси бачимо, що як тільки Web-3.0 буде широко використовуватися, популярність багатьох програм блокчейна, таких як смарт-контракти та децентралізовані програми (dApps), зростатиме. Відомо, що сучасні Web 3-додатки мають такі атрибути як: DAO (decentralized autonomous organization – децентралізована автономна організація), вони також називаються децентралізованими автономними корпораціями (Decentralized Autonomous Corporations – DAC); крипто валюти; блокчейн та децентралізовані системи зберігання даних; суверенна ідентичність (SSI) «інтернет речей»; метавсесвіт; NFT та інші явища та технології.

Ключовими принципами DAC/DAO були децентралізація компаній, токенізація їх акцій і відкритість операцій з кодом, що перевіряється публічно. DAC/DAO управляється за допомогою смарт-контрактів. Смарт-контракт (Smart contract – "розумний контракт") – комп'ютерний алгоритм, призначений для укладання та підтримки контрактів, що виконуються в блокчейн-середовищі. Такі контракти записуються у вигляді коду, який існує в розподіленому реєстрі – блокчейні, який підтримується та керується мережею комп'ютерів. Простими словами, Smart contract дозволяють обмінюватися активами, не вдаючись до послуг посередників. Тому архітектура Web-3.0 відрізняється від його попередника Web-2.0 тим, що вводить ще один елемент під назвою OWN – власний, особистий, Oprah Winfrey Network), тобто ви можете взаємодіяти та володіти своїми даними.

Архітектура Web-3.0 складається з наступних основних рівнів (рис. 1):

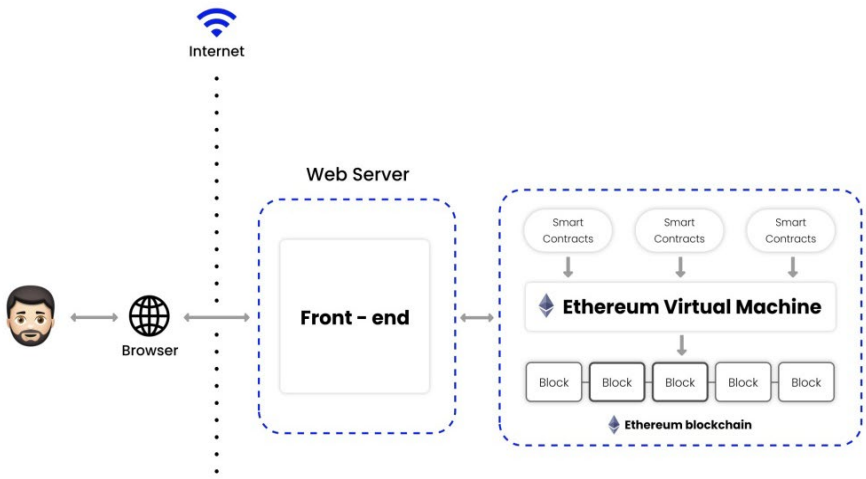


Рис. 1. Архітектура додатків Web-3.0

На рисунку 1 наведені елементи архітектури додатків Web-3.0, а саме:

*Blok* (блокчейн) – це кінцеві автомати, які доступні глобально. Вони підтримуються одноранговою мережею вузлів, в якій будь-яка людина у світі може написати і отримати до неї доступ. Однак, користувачі можуть додавати нові дані до блокчейну, але ніколи не можуть змінювати існуючі дані.

*Смарт-контракти* – це бізнес-логіка, що зберігається в блокчейні (кінцеві автомати). Без участі будь-якого посередника його буде виконано, коли буде погоджено заздалегідь визначені умови. В даний час найвідомішими смарт-контрактами є протоколи транзакцій, що працюють на блокчейні Ethereum. Смарт-контракти завжди виконуються на приватних однорангових вузлах, що належать певним членам мережі, з перевіреними даними, розміщеними на цих однорангових вузлах.

*Віртуальна машина Ethereum* (EVM). Ціль цих машин – виконувати логіку, визначену в смарт-контрактах. Вони обробляють зміни стану, які у кінцевому автоматі.

*Зовнішній процес.* Дозволяє користувачеві підключатися та надсилати запити на виклик функцій контракту через інтерфейс програми. Тобто він взаємодіє з логікою застосування, визначеної в смарт-контрактах. Звідси основна відмінність архітектури Web-3.0 від Web-2.0 полягає у застосуванні технології dApp замість Backend. Відомо, що технологія Backend визначає централізовано організовану бізнес-логіку, вхід/вихід, публікація та ін. Застосування технології dApp (блокчейна) робить всі процеси прозорими та неможливими для редагування або фальсифікації. Дані не можна редагувати або неможливо видалити, коли щось існує у блокчейні. Фактично контроль над децентралізованими сервісами буде передано користувачам, все буде прозорим та захищеним від несанкціонованого доступу в системі.

*Порівняння веб-інтерфейсу Web-2.0 та Web-3.0.* У Web-2.0 зовнішній інтерфейс програми дає користувачеві можливість запитувати і публікувати в базі даних, аналогічно це не змінюється в Web-3.0. Основні завдання фронтенд-розробника Web-3.0 є незмінними для Web-2.0, де вони реалізують усе, що бачать користувачі. Розробники веб-інтерфейсу зазвичай потребують однакового набору навичок, включаючи володіння HTML, CSS, JavaScript, React.js та ін. Однак основною відмінністю є Web3.js, що є набором бібліотек JavaScript, який дозволяє вам взаємодіяти з вузлом Ethereum. Загалом Web3.js надає API, тому можна спілкуватися з вузлом блокчейна за допомогою HTTP- або IPC-з'єднання.

*Взаємодія з віртуальною машиною Ethereum (EVM) та смарт-контрактами.* Програма Web3 (dApp) повинна розміщувати вузол Ethereum або використовувати стороннього постачальника, такого як Infura, Alchemy та Quicknode. Це необхідно, тому що будь-який вузол може вимагати дані або виконувати транзакцію на віртуальній машині Ethereum. Однак майте на увазі, що запуск повного вузла Ethereum може стати дорогим, що пов’язане з тим, що додаток має проблеми під час обслуговування. Тому використання стороннього сервісу може бути зручнішим. Провайдери Ethereum реалізують специфікації JSON-RPC для зв'язку із

мережами блокчейнів. JSON-RPC (JavaScript Object Notation (JSON)/Remote Procedure Call (RPC)) – це протокол віддаленого виклику процедур, закодований JSON. Є одним з декількох методів, що використовуються сьогодні та дозволяють програмному додатку викликати функції з іншого додатка. Загалом його можна порівняти з SOAP, gRPC та XML-RPC. JSON-RPC схожий на протокол XML-RPC, визначаючи лише кілька типів даних та команд.

Віддалений виклик процедур (RPC) – це протокол запиту-відповіді, який визначає правила, що дозволяють клієнту надсилати повідомлення на віддалений комп'ютер для виконання функції та отримання відповіді. При такому спілкуванні програма працює так, як вона розташована на машині клієнта, тобто клієнт не знає про віддалену машину. Все спілкування відбувається через HTTP чи веб-сокети.

Відомо, що під час застосування Web-2.0 доступ до програм надається через вхід до централізованої бази даних, у Web-3.0 доступ до dApp аутентифікується за допомогою провайдера. Провайдери, такі як Metamask, що надають доступ до крипто валютного гаманця, діють як особа, яка підписує транзакцію, та постачальник. Він зберігає зашифровані закриті ключі, використовуючи сховище даних браузера. Усі транзакції запитів на запис підписуються закритим ключем клієнта. Природно, що кожна транзакція буде коштувати користувачеві комісію в Ethereum, яка піде іншим вузлам (майнерам), які перевіряють транзакції. Тому коли користувач хоче створити нову транзакцію, dApp через провайдера Web-3.0 попросить користувача підписати транзакцію, використовуючи свій закритий ключ. Після того, як користувач підписався, dApp буде взаємодіяти зі смарт-контрактом від імені користувача та транслюватиме виведення в мережу Ethereum.

Важливо розуміти, як організовано сховище в блокчейні Ethereum. Логічно, що всі смарт-контракти та дані мають існувати у блокчейні Ethereum. Однак, коли дані фіксуються у блокчейні Ethereum, це коштує грошей (плата майнерам). Таким чином, зберігання всього в блокчейні може стати надзвичайно дорогим.

Оскільки користувачу не рекомендується платити великі транзакційні збори під час використання вашого dApp, використовується децентралізоване рішення для зберігання поза мережею. Ось деякі варіанти:

IPFS – міжпланетна файлова система (Inter Planetary File System) – це контентно-адресований, одноранговий гіпермедійний протокол зв'язку для обміну файлами. IPFS використовується для зберігання та доступу до файлів, веб-сайтів, програм та даних. IPFS використовує адресацію вмісту для ідентифікації кожного файлу у глобальному просторі імен, що з'єднує усі обчислювальні пристрої. IPFS також має шар відомий як Filecoin. Цей шар використовується для зберігання та пошуку даних. Такі провайдери, як Infura або Pintara, корисні для закріплення файлів IPFS і їх зберігання в блокчейні;

Swarm також є децентралізованою платформою для зберігання, обслуговування та зв'язку і захищеної від цензури інфраструктури для розгортання коду dApp;

хмарні сервери, наприклад, Azure або AWS. Однак, вони схожі на архітектуру Web-2.0, де маємо централізацію даних. Крім того, якщо Azure або AWS перестануть працювати, піддаючи вашу програму цензурі, у вас більше не буде доступу до даних.

З вищевказаних причин справжнє dApp зберігатиме всі свої дані поза мережею в децентралізованому сховищі.

Таким чином, технологія блокчейну продовжуватиме відігравати важливу роль в інтернет-інфраструктурі в міру розвитку Web-3.0. Web-3.0 – це зміна парадигми, коли користувачі отримують контроль над своєю конфіденційністю та даними. Також цікаво буде подивитися, як великі технологічні компанії відреагують на цю майбутню тенденцію. Але у технології блокчейн поряд з перевагами блокчейну виникають і серйозні проблеми, що створює багато умов і для загроз. Давайте поглянемо на деякі з найбільш нагальних проблем уразливості, які стоять перед блокчейном сьогодні.

*Масштабованість.* Мережі блокчейнів можуть бути повільними та неефективними через високі обчислювальні вимоги, необхідні для перевірки транзакцій. У міру збільшення кількості користувачів, транзакцій та додатків здатність мереж блокчейна своєчасно

обробляти та перевіряти їх стає напруженою. Це ускладнює використання блокчейн-мереж у додатках, що потребують високої швидкості обробки транзакцій. Було запропоновано різні рішення, щоб спробувати подолати проблеми масштабованості, у тому числі системи масштабування для створення каналів поза мережею, які дозволяють проводити швидші та економічні транзакції. І хоча експерти з блокчейну досягли певного прогресу, створення масштабованих, ефективних та децентралізованих мереж блокчейнів залишається постійною проблемою, яка потребує подальшого вивчення.

*Обмежена пропускна спроможність транзакцій та обчислювальної потужності.* Традиційні блокчейни, такі як Біткойн та Ефіріум, покладаються на алгоритми консенсусу, такі як доказ роботи та доказ частки, які можуть бути повільними та ресурсномісткими. В результаті ці мережі стикаються з обмеженнями пропускної спроможності транзакцій, що часто призводить до перевантаження та високих комісій за транзакції. Процес перевірки транзакцій у мережі блокчейн потребує велику обчислювальну потужність, що, своєю чергою, потребує багато енергії. Це викликало занепокоєння з приводу: по-перше, вирішення проблеми охолодження процесорів в обчислювальних засобах; по-друге, вплив технології блокчейн на навколишнє середовище, тому що вироблення енергії пов’язане з викидами вуглецю в навколишнє середовище. Деякі блокчейн-проекти використовують альтернативні механізми консенсусу, такі як PoS, які споживають значно менше енергії. Такі ініціативи, як Ethereum 2.0 також спрямовані на зниження енергоспоживання мережі Ethereum. Хоча ці зусилля є багатообіцяючими, для спільноти блокчейнів дуже важливо продовжувати вивчати способи мінімізації енергоспоживання та розробки екологічно стійких рішень.

*Безпека.* Заходи безпеки блокчейну часто рекламувалися як ключові сильні сторони технології, але безпека мереж блокчейну не обходиться без проблем. Були випадки порушень безпеки і атак хакерів на мережі блокчейн, і ці проблеми можуть призвести до грошових втрат і пошкодження цілісності мережі. Щоб знизити ризики, компанії працюють над підвищенням безпеки мереж та додатків блокчейну. Їхні зусилля з безпеки включають офіційну перевірку смарт-контрактів, що допомагає виявити потенційні вразливості, та використання гаманців з мультипідписом для зберігання та керування цифровими активами. Оскільки технологія блокчейна продовжує розвиватися, забезпечення безпеки користувачів, активів та транзакцій, як і раніше, викликає занепокоєння.

*Складність.* Блокчейн – це складна технологія, для впровадження та обслуговування якої потрібний високий рівень технічних знань. Технічні проблеми можуть завадити широкому впровадженню технології блокчейну та відбити у потенційних користувачів та розробників інтерес до неї. Складність блокчейна також може призвести до помилок та неефективності реалізації. Зусилля щодо вирішення цієї проблеми включають розробку зручних інтерфейсів, оптимізованих процесів адаптації та освітніх ресурсів, які спрощують складність блокчейну. Розширення співробітництва між галузевими експертами, академічними колами та державними органами також може сприяти обміну знаннями та створенню стандартизованих протоколів та структур, що знижують вхідні бар'єри.

*Сумісність.* Інтероперабельність (Interoperability), або здатність різних інформаційних систем, пристроїв, додатків або продуктів спілкуватися та розуміти інформацію, що передається одна одній, або з'єднуватися та обмінюватися даними скоординованим чином без зусиль з боку кінцевого користувача, тобто здатність різних мереж блокчейнів спілкуватися та взаємодіяти один з одним, є ще однією серйозною проблемою, що стоїть перед галуззю. В даний час існує безліч різних блокчейн-платформ, кожна зі своїми протоколами та стандартами, і часто вони погано працюють разом. Існує три основні типи сумісності: синтаксична, структурна та семантична. Також визначають чотири рівні сумісності: юридичний, організаційний, семантичний та технічний.

**Висновки**

Таким чином, нова версія Всесвітньої павутини Web-3.0 створює багато умов, які можуть бути корисні людям. Але впровадження нових можливостей призводить до появи нових загроз або уразливості, які можуть бути зловмисниками використані для нанесення шкоди людям. Це вимагає розглянути можливий вплив загроз, визначити можливі уразливості в технології Web-3.0 до початку експлойту нульового дня, тобто вимагає необхідність дослідження можливості появи нових вразливих (критичних) місць. Це є актуальною та своєчасною задачею для дослідження.

**Список використаної літератури**

1. Web 3.0 – Solution To Big Problems / [електронний ресурс] – режим доступу: https://rehansattar.dev/web-30-solution-to-big-problems/(Дата перегляду 20 квітня 2023)

2. Preedip Balaji, Vinay M S, Shalini B G, J S Mohan Raju An integrative review of Web 3.0 in academic libraries/ June 2018Library Hi Tech News 35(4) DOI:10.1108/LHTN-12-2017-0092// [електронний ресурс] – режим доступу: https://www.researchgate.net/publication/325980398_An_integrative_review_of_Web_30_in_academic_libraries/

3. Bolinder, J. (2008), "The return of Web 3.0 – cloud computing, browser extensions or the distributed Web", blog post, 4 August, available at: http://impl.emented.com/2008/08/04/the-return-of-Web-30-cloud-computingbrowser-xtensions-or-the-distributed-Web/(accessed 10 November 2017).

4. Isaias, P., Ifenthaler, D., Sampson, D.G. and Spector, J.M. (Eds) (2011), Towards Learning and Instruction in Web 3.0: Advances in Cognitive and Educational Psychology, Springer, New York, NY. New Library World, Vol. 113 Nos 3/4, pp. 202-217, doi: 10.1108/03074801211218561

5. Web3 and crypto skepticism is growing and people are finally starting to listen/ [електронний ресурс] – режим доступу:https://www.coywolf.news/webdev/web3-crypto-skepticism/#:~:text=Web3%2C%20which%20is%20supposed%20to,that%20Web3%20is%20fake%20decentralization/(Дата перегляду 20 квітня 2023).

6. 5 Reasons Why Web 3.0 will Fail? / [електронний ресурс] – режим доступу: https://itnext.io/top-5-reasons-why-web-3-will-fail-57237e4c3db/

***Автори статті***

**Вишнівський Олександр** – аспірант, Державний університет інформаційно-комунікаційних технологій, Київ, Україна

**Зінченко Ольга** – доктор технічних наук, доцент, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

**Катков Юрій** – доктор технічних наук, доцент, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

**Березовська Юлія** – PhD, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

**Колдун Павло** – студент, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

***Authors of the article***

**Vyshnivskyi Oleksandr** – postgraduate student, State University of Information and Communication Technologies, Kyiv, Ukraine.

**Zinchenko Olha** – Doctor of Science (technic), associate professor, State University of Information and Communication Technologies, Kyiv, Ukraine.

**Katkov Yurii** – Doctor of Science (technic), associate professor, State University of Information and Communication Technologies, Kyiv, Ukraine

**Berezovska Yuliia** – PhD, Senior Lecturer, State University of Information and Communication Technologies, Kyiv, Ukraine

**Coldun Pavlo** – student, State University of Information and Communication Technologies, Kyiv, Ukraine.