11. van Wyk M. M. Blog Phenomenology: Student Teachers' Views of Learning to Teach Economics. International Journal of Web-Based Learning and Teaching Technologies. 2018. Vol. 13. Is. 2. P. 62–77.
12. Ziraba A., Mariana A., Chenyuei G., Shiynsa N. The Adoption and Use of Moodle Learning Management System in Higher Institutions of Learning. A Systematic Literature Review. American Journal of Online and Distance Learning. 2020. Vol. 2 (1). P. 1–21.

УДК 004.056:004.7
DOI 10.25128/2415-3605.23.1.8

ІГОР ГЕВКО

https://orcid.org/0000-0003-1108-2753
gevko.i@gmail.com
доктор педагогічних наук, професор
Тернопільський національний педагогічний університет
імені Володимира Гнатюка
вул. Максима Кривоноса, 2, м. Тернопіль

ОЛЕКСАНДР ЯЩИК

https://orcid.org/0000-0002-8420-3336
sanytnpu@gmail.com
кандидат педагогічних наук, доцент
Тернопільський національний педагогічний університет
імені Володимира Гнатюка
вул. Максима Кривоноса, 2, м. Тернопіль

ТЕТЯНА САВЧИН

https://0000-0000-0003-3007-8960
savchyn.tanya@gmail.com
кандидат філологічних наук, доцент
Тернопільський національний технічний університет
імені Івана Пулюя
вул.Руська, 56, м.Тернопіль

ЛЕСЯ ГІЛЬТАЙ

https://orcid.org/0000-0001-6658-8175
lesyagiltay@gmail.com
аспірантка кафедри комп'ютерних технологій
Тернопільський національний педагогічний університет
імені Володимира Гнатюка
вул. Максима Кривоноса, 2, м. Тернопіль

КІБЕРБЕЗПЕКА В ДЕЦЕНТРАЛІЗОВАНІЙ ІНТЕРНЕТ-ЕКОСИСТЕМІ WEB 3.0

Досліджено проблему кібербезпеки в мережі Інтернет; з'ясовано основні принципи вдосконалення глобальної культури безпечної мережевої взаємодії. Розглянуто питання, пов'язані із забезпеченням інформаційної безпеки особистості під час користування інтернет-системами. Обґрунтовано, що кібербезпека є важливим питанням у сучасному світі і її захист вимагає уваги на належному рівні. Зазначено важливість знань про технології і методи захисту від кіберзагроз для всіх, хто використовує комп'ютерні системи й Інтернет. Оскільки кібератаки можуть стати серйозною загрозою для безпеки та конфіденційності особистої інформації, то важливо, щоб студенти мали знання про основні технології і методи захисту від кіберзагроз, а це актуалізує вивчення кібербезпеки майбутніми фахівцями. Також багато студентів вивчають цифрові технології і комп'ютерні науки, що робить знання про кібербезпеку ще більш важливим. Незважаючи на те, що студенти можуть вивчати різноманітні аспекти кібербезпеки в рамках своєї програми навчання, важливо сформувати в них загальне розуміння про те, як захистити себе та свої комп'ютерні системи від кіберзагроз. Описано, як вивчення соціальної інженерії допоможе студентам розібратись у тактиках, техніках і підходах, які

використовують зловмисники для отримання конфіденційної інформації. Важливо щоб вони розуміли, якими шляхами можуть бути здійснені атаки на системи кібербезпеки, та які методи можуть бути застосовані для запобігання таким атакам. Детально розглянуто технологію Web 3.0 як нове покоління Інтернету, що передбачає децентралізованішу та інтелектуальнішу мережу, з більш структурованими даними і здатністю до автоматизованої обробки. Описано основні складові Web 3.0: блокчейн, семантичний веб, штучний інтелект, децентралізація. Вказано на необхідність захисту особистої інформації і безпеку від зловживань інформацією в новітніх інтернет-екосистемах для забезпечення позитивного впливу цих технологій у суспільстві.

***Ключові слова**: інформаційні технології, кібербезпека, технологія Web 3.0, соціальна інженерія, блокчейн, семантичний веб, штучний інтелект, децентралізація,*

IHOR HEVKO

Doctor of Pedagogical Sciences, Professor
Ternopil Volodymyr Hnatiuk National Pedagogical University
2 Maksym Kryvonis Str., Ternopil

OLEKSANDR YASHCHYK

Candidate of Pedagogical Sciences, Associate Professor
Ternopil Volodymyr Hnatiuk National Pedagogical University
2 Maksym Kryvonis Str., Ternopil

TETIANA SAVCHYN

Candidate of Philological Sciences, Associate Professor
Ternopil Ivan Puliui National Technical University
56 Ruska Str., Ternopil

LESIA HILTAI

graduate student of the Department of Computer Technologies
Ternopil Volodymyr Hnatiuk National Pedagogical University
2 Maksym Kryvonis Str., Ternopil

CYBER SECURITY IN DECENTRALIZED WEB 3.0 INTERNET ECOSYSTEM

The article examines the problem of cyber security on the Internet; the main principles of improving the global culture of safe network interaction are clarified. Issues related to ensuring personal information security while using Internet systems are considered. Cyber security is an important issue in today's world, and its protection requires an appropriate level of attention. The importance of knowledge about technologies and methods of protection against cyber threats for everyone who uses computer systems and the Internet is noted. The relevance of studying cyber security by students is considered. Because cyber threats can pose a serious threat to the security and privacy of personal information, it is important that students have knowledge of the basic technologies and techniques to protect themselves against cyber threats. Also, many students study digital technology and computer science, which makes knowledge about cyber security even more important. While students may study various aspects of cyber security as part of their degree program, it is important for them to develop general understanding of how to protect themselves and their computer systems from cyber threats.

The article describes how the study of social engineering will help students understand the tactics, techniques, and approaches used by attackers to obtain sensitive information. It is important that they understand the ways in which cyber security systems can be attacked and the methods that can be used to prevent such attacks. Web 3.0, technology is considered in detail as a new generation of the Internet, which involves a more decentralized and intelligent network, with more structured data and the ability for automated processing. The main components of Web 3.0 are described: blockchain, semantic web, artificial intelligence and decentralization. The importance of protecting personal information and security against misuse of information in the latest Internet ecosystems is indicated. With the development of Web 3.0, there are more and more questions about privacy and security on the Internet. The article examines the importance of developing effective protection methods and regulating the use of these technologies to ensure a safe and reliable Internet for users. Web 3.0 technology has great potential for the development of the Internet ecosystem, and will become the basis for new innovations and opportunities in various fields. However, it is necessary to ensure the

protection of personal information and security against abuse in order to ensure the positive impact of these technologies on society.

***Keywords**: information technology, cyber security, Web 3.0, technology, social engineering, blockchain, semantic web, artificial intelligence, decentralization.*

Процеси глобалізації, євроінтеграції та цифровізації суспільства змінюють зміст та роль знань, трансформують освітні системи, які мають власну структуру та утворюються окремими елементами, що взаємозв'язані між собою. Провідними елементами електронної частини світового інформаційного простору є професійні бази, ділові ресурси мережі Інтернет, електронні бібліотеки. Зростання ролі інформаційного продукту визначає потребу в обробленні дедалі більших обсягів інформації, актуалізується потреба в різних формах сприйняття інформації, а також у її актуальності, точності й безпечне зберігання. При цьому інформаційні технології, засновані на використанні сучасних комп'ютерних і мережевих засобів, утворюють поняття «сучасні інформаційні технології». Під засобами сучасних інформаційних і комунікаційних технологій розуміються програмні, програмно-апаратні та технічні засоби, а також сучасні засоби й системи транслювання інформації, інформаційного обміну, які забезпечують операції зі збору, продукування, накопичення, зберігання, обробки, передачі інформації та можливість безпечного доступу до інформаційних ресурсів комп'ютерних мереж [1, с. 46–47].

Проблема кібербезпеки в мережі Інтернет є дуже серйозною та актуальною. Кібербезпека відноситься до заходів, які необхідно застосовувати, щоб захистити комп'ютерні системи і дані від несанкціонованого доступу, викрадення та пошкодження. Одна з головних проблем кібербезпеки − це хакерські атаки, під час яких зловмисники можуть намагатися проникнути в комп'ютерні системи, використовуючи різноманітні методи, такі як фішинг, віруси, троянські програми та ін.

Іншою проблемою кібербезпеки є зловживання персональними даними. Кожен раз, коли користувачі реєструються на сайтах і додатках, вони надають свої персональні дані: прізвище та ім'я, адреса електронної пошти, телефонний номер тощо. Якщо ці дані потраплять у руки зловмисників, вони можуть використовувати їх для шахрайства, викрадення грошей, ідентичності. Крім того, існує проблема кібертероризму, коли зловмисники намагаються завдати шкоди країні, компанії чи іншим організаціям, зламуючи їхні комп'ютерні системи і викрадаючи конфіденційну інформацію.

Метою статті є дослідження формування умов кібербезпеки в децентралізованій інтернет-екосистемі.

Щоб захистити себе від загроз, користувачі повинні бути обережними в Інтернеті і приймати необхідні заходи забезпечення кібербезпеки: встановлення антивірусного програмного забезпечення, регулярне оновлення програмного забезпечення, використання надійних паролів. Крім того, важливо слідкувати за своїми персональними даними і не надавати їх зловмисникам. Не варто також відкривати посилання з невідомих джерел, надсилати свої паролі чи іншу конфіденційну інформацію через електронну пошту, використовувати публічні Wi-Fi мережі без додаткового захисту.

Загалом кібербезпека є важливим питанням в сучасному світі і її захист має бути на належному рівні. Знання про технології і методи захисту від кіберзагроз корисні для всіх, хто використовує комп'ютерні системи й Інтернет.

Вивчення кібербезпеки важливе для студентів з двох причин. По-перше, нині майбутні фахівці використовують повсякденно комп'ютерні системи та Інтернет як для освітніх цілей, так і для особистих потреб. Оскільки кіберзагрози можуть стати серйозною загрозою для безпеки і конфіденційності особистої інформації, важливо, щоб студенти набули знання про основні технології і методи захисту від кіберзагроз. По-друге, багато здобувачів вищої освіти вивчають інформаційні технології та комп'ютерні науки, що робить отриманні знання про кібербезпеку ще більш важливим. Незважаючи на те, що студенти можуть вивчати різні аспекти кібербезпеки в рамках своєї програми навчання, важливо мати загальне розуміння про те, як захистити себе і свої комп'ютерні системи від кіберзагроз. Тож вивчення кібербезпеки є важливим як для їх особистої безпеки, так і для успішної професійної кар'єри.

Одним із поширених зловмисних методів є соціальна інженерія: техніка впливу на людей з метою отримання від них конфіденційної інформації чи здійснення шахрайства. Це може включати використання психологічних методів – маніпуляції, обману, увійти в довіру. Наприклад, зловмисник може вигадати історію про те, що він є представником компанії, яка займається

технічною підтримкою, і попросити відправити йому пароль для тестування. Інший приклад – може бути відправлення електронного листа, в якому зловмисник вигадує історію про те, що він є нібито колегою чи довіреною особою та просить отримати конфіденційну інформацію.

Оскільки соціальна інженерія зазвичай використовується для отримання конфіденційної інформації, вона є серйозною загрозою для кібербезпеки як індивідів, так і організацій. Вони можуть захистити себе від соціальної інженерії шляхом підвищення свідомості про неї та навчання співробітників виявляти і запобігати підступним методам збору інформації. Тому рекомендується встановлювати міцні паролі, не передавати їх третім особам й уважно перевіряти електронні повідомлення та веб-сайти, перш ніж надавати будь-яку конфіденційну інформацію.

Крім заходів безпеки на рівні індивідів та організацій, вивчення соціальної інженерії є важливим аспектом в загальному контексті кібербезпеки. Оскільки соціальна інженерія – один з найпоширеніших методів атак на системи кібербезпеки, особливо коли йдеться про атаки на малі організації та індивідуальних користувачів, які можуть бути менш захищеними порівняно з великими компаніями [10, с. 77].

Вивчення соціальної інженерії допоможе студентам розібратись у тактиках, техніках і підходах, що використовують зловмисники для отримання конфіденційної інформації. Вони будуть розуміти і знати, як здійснюються атаки на системи кібербезпеки і які методи можуть бути застосовані для запобігання таким атакам. У студентів, які вивчають кібербезпеку та соціальну інженерію, формується здатність виявляти і запобігати атакам на комп'ютерні системи. Вони також можуть бути експертами для розробки і вдосконалення заходів безпеки, які можуть бути застосовані в різних організаціях [8, с. 139].

Одним із нововведень ІКТ є технологія Web 3.0. Це поняття, що описує наступне покоління Інтернету, яке буде базуватися на розподілених системах, блокчейні і штучному інтелекті (англ. artificial intelligence – AI). Основною метою Web 3.0 є забезпечити користувачам більш безпечну, приватну і децентралізовану інтернет-екосистему.

Основні принципи Web 3.0 включають:

Децентралізацію − Web 3.0 має стати більш децентралізованою платформою, де користувачі матимуть більший контроль над своїми даними та взаємодією з іншими користувачами.

Блокчейн − Web 3.0 буде використовувати цю технологію для забезпечення безпеки, автентифікації та підтвердження транзакцій в мережі.

Штучний інтелект (AI) − Web 3.0 використовуватиме його для розумного аналізу даних, що дозволить зробити розумні прогнози та підвищити якість взаємодії користувачів з мережею.

Семантичний веб (Semantic Web) − Web 3.0 використовуватиме його для кращого розуміння змісту і контексту даних, що дозволить створити ефективнішу систему пошуку та інтерпретації даних.

Основна ідея Web 3.0 полягає в тому, щоб забезпечити більш безпечну, приватну та децентралізовану інтернет-екосистему, де користувачі матимуть більший і надійний контроль над своїми даними та взаємодією з мережею. 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 можуть допомогти забезпечити більш точний аналіз даних, що сприяє у вирішенні складних проблем і покращенні ефективності бізнес-процесів.

Web 3.0 дозволяє створювати децентралізовані додатки (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 більш безпечну, приватну та децентралізовану інтернет-екосистему, що може стати основою для нових інновацій та розвитку різних галузей.

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 більш стійкою і захищеною. 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 більш стійкі і захищені системи, забезпечуючи надійніший контроль над даними користувача і відкриваючи нові можливості для розвитку технологій та інновацій.

Однією з найбільш відомих децентралізованих систем є технологія блокчейн. Це розподілена база даних, яка містить інформацію про транзакції та операції, що відбуваються в мережі. Ця інформація розподіляється по всіх вузлах мережі, що робить блокчейн більш стійким і захищеним від атак ззовні. Використання блокчейну дає можливість створювати децентралізовані додатки і сервіси, які працюють на основі смарт-контрактів. Блокчейн дозволяє забезпечити безпеку і прозорість транзакцій у децентралізованих системах, таких як криптовалютні біржі, системи голосування та ін. [13, с. 117].

Як один із прикладів децентралізованої системи є криптовалюта Bitcoin. Вона дозволяє користувачам відправляти й отримувати гроші без посередників, що їм дає змогу зберігати більший контроль над своїми фінансами. Крім того, блокчейн дозволяє створювати інші децентралізовані фінансові сервіси, такі як децентралізовані обмінні платформи та кредитні системи. Іншим прикладом децентралізованих систем є децентралізовані соціальні мережі, де користувачі мають повний контроль над своїми даними та інформацією, що вони діляться в мережі. Такі мережі, як Mastodon та Diaspora, дозволяють користувачам спілкуватися і ділитися інформацією, не потрапляючи під контроль корпорацій та інших централізованих структур. Децентралізація також може бути використана для створення більш безпечних і стійких систем, зокрема систем голосування та управління, де кожен учасник має можливість контролювати процеси та рішення.

Крім блокчейну, існують інші децентралізовані технології, які можуть бути використані для реалізації інноваційних проєктів у різних сферах: наука, фінанси, транспорт, медицина тощо. Наприклад, технологія IPFS (Inter Planetary File System) дає можливість зберігати файли у розподіленій мережі вузлів, що забезпечує більшу стійкість і доступність файлів, зменшує витрати на зберігання даних.

Децентралізація як важлива складова Web 3.0 дозволяє забезпечити більшу свободу і контроль користувачів над своїми даними та інформацією, а також створює нові можливості для розвитку інноваційних проєктів у різних сферах. Однак разом з цим виникають проблеми і виклики, пов'язані з безпекою, ефективністю та надійністю децентралізованих систем. Щоби забезпечити безпеку в децентралізованих системах, використовуються різноманітні механізми захисту: шифрування, підписи, аутентифікація, авторизація. Також важливо враховувати можливі загрози та ризики, пов'язані з використанням децентралізованих технологій, такі як атаки на блокчейн, злами алгоритмів шифрування та ін.

Окрім того, важливо вирішувати проблеми щодо ефективності і надійності децентралізованих систем. Наприклад, виникає проблема масштабування децентралізованих систем, оскільки кожен вузол мережі повинен мати повну копію бази даних, що може призвести до затримок і перевантажень. Для розв'язання цієї проблеми використовуються різні технології, наприклад, розділення блокчейну на шари (англ. sharding).

Як вагома складова Web 3.0 децентралізація може принести багато переваг у різних сферах. Щоби забезпечити успішний розвиток Web 3.0, необхідно розв'язувати проблеми і

виклики, пов'язані з безпекою та ефективністю децентралізованих систем, використовуючи найкращі практики у сфері кібербезпеки і технологій децентралізації.

Важливо забезпечити підтримку та розвиток відкритих стандартів і протоколів, які використовуються в децентралізованих системах. Це дозволить забезпечити сумісність та інтероперабельність різних децентралізованих систем, що сприятиме подальшому розвитку Web 3.0. Нині актуально забезпечити підтримку і сприяння розвитку децентралізованих проєктів та ініціатив. Для цього можна створювати спеціальні програми підтримки: гранти, акселератори та інкубатори, які допоможуть розвивати і прискорити розвиток децентралізованих проєктів.

AI 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, AI 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 AI 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 AI, може бути важко зрозуміти, як приймаються рішення та контролюється поведінка систем AI. 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 AI [7, с. 65].

Таким чином, AI 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, обробка природньої мови, аналіз даних, блокчейн та ін.

Однією з найважливіших проблем, пов'язаних з розвитком AI в Web 3.0, є питання безпеки. Так, AI 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, аутентифікація користувачів, контроль доступу до ресурсів. Однак тоді виникають етичні питання щодо розробки і використання AI в Web 3.0. Так, можуть виникати проблеми з автоматизацією процесів і заміною людей роботами, зі збереженням приватності і захистом прав користувачів.

Семантичний веб є ще однією складовою Web 3.0. Основна його ідея полягає у тому, щоб додати до веб-сторінок додаткову інформацію, яка описує їх зміст і зв'язки між ними. Це дозволяє комп'ютерам краще розуміти контент веб-сторінок і робити висновки про зв'язки між різними об'єктами в Інтернеті. Семантичний веб базується на стандартах Resource Description Framework (RDF), Web Ontology Language (OWL) і SPARQL Protocol and RDF Query Language (SPARQL). Їх використання дозволяє створювати структуровану інформацію, яка може бути легко інтерпретована та оброблена комп'ютерами. Одним з прикладів використання семантичного вебу є Knowledge Graph від Google. Це система, що забезпечує користувачам швидкий і точний доступ до інформації шляхом аналізу зв'язків між об'єктами в Інтернеті.

Важливими перевагами семантичного вебу є збільшення ефективності та точності пошуку в Інтернеті, поліпшення співпраці між комп'ютерами і зручність розуміння змісту веб-сторінок для людей. Розвиток семантичного вебу зумовлює потребу в розробці нових технологій і методів забезпечення безпеки і приватності. Зокрема, виникають проблеми з обробкою конфіденційної інформації та захистом від атак зловмисників. Загалом семантичний веб як важлива складова Web 3.0 дозволяє створювати більш структуровану та зв'язану інформацію в Інтернеті. З розвитком технологій семантичного вебу виникає дедалі більше питань щодо приватності і безпеки в Інтернеті. Збільшення кількості даних та їх структурованість може зробити мережу більш вразливою до атак хакерів і кіберзлочинців, які можуть використовувати ці дані для зловживання або шахрайства.

Дуже ймовірною проблемою є те, що зібрана за допомогою семантичного вебу інформація може бути використана для створення профілю користувача. Це може призвести до порушення приватності і конфіденційності, до того, що користувачі втрачають контроль над своїми особистими даними. Крім того, зі структурованістю даних збільшується ймовірність створення ботів та автоматичних систем, які можуть виконувати певні дії на веб-сторінках без згоди користувача. Це може спричинити поширення спаму, фейкових новин, а також інші форми кіберзлочинності.

На нашу думку, з розвитком семантичного вебу необхідно знайти ефективні методи захисту приватності та безпеки в Інтернеті, щоб забезпечити безпечне і надійне використання цієї технології. Однією з можливих проблем в її використанні є те, що створення структурованої та зв'язаної інформації може бути дуже трудомістким процесом. Розробка стандартів та інструментів для семантичного вебу може займати дуже багато часу і коштів. З іншого боку, застосування цієї технології може мати значний вплив на різні сфери діяльності: науку, бізнес, освіту й ін. Наприклад, засоби семантичного вебу можуть допомогти у вирішенні таких складних проблем, як пошук великих обсягів даних або підвищення рівня автоматизації процесів в бізнесі. Також його використання може забезпечити більш точне і швидке розуміння змісту веб-сторінок і поліпшити взаємодію між користувачами та комп'ютерами.

Отже, технологія Web 3.0 − це нове покоління Інтернету, яке передбачає більш децентралізовану та інтелектуальну мережу, з більш структурованими даними і здатністю до автоматизованої обробки інформації.

Головні складові Web 3.0 – це блокчейн, семантичний веб, штучний інтелект і децентралізація. Кожен з цих елементів має великий потенціал для розвитку Інтернету й покращення життя людей. Проте з розвитком Web 3 з'являється дедалі більше питань стосовно приватності і безпеки в цій мережі. Важливо розробляти ефективні методи захисту і регулювання використання цих технологій, щоб забезпечити безпечний і надійний Інтернет для користувачів.

Технологія Web 3.0 має великий потенціал для розвитку інтернет-екосистеми й стане основою для нових інновацій і можливостей в різних галузях. Однак необхідно забезпечувати захист особистої інформації та безпеку від зловживань, щоб зберегти позитивний вплив цих технологій у суспільстві.

ЛІТЕРАТУРА

1. Гевко І. В. Використання сучасних інформаційних технологій у навчанні студентів Вищого навчального закладу. Науковий часопис Національного педагогічного університету імені М. П. Драгоманова. Серія 5. Педагогічні науки: реалії та перспективи; збірник наукових праць Випуск 62: / М-во освіти і науки України, Нац. пед. ун-т ім. М. П. Драгоманова. – Київ: Вид-во НПУ імені М. П. Драгоманова, 2018. – С. 46–50.
2. Ящик О. Б. Застосування SMART-технологій в суспільстві для побудови розумних міст. Сучасні проблеми графічної підготовки студентів у ЗФПО: теорія і практика. Електронний збірник матеріалів науково-практичної онлайн-конференції (м. Тернопіль, 16 березня 2023 р.). Тернопіль: ВСП «ТФК ТНТУ», 2023. С. 59–69.
3. Ящик О. Б. Зміцнення глобальної культури кібербезпеки в мережі Інтернет. Комп'ютерно-орієнтовані системи навчання: збірник наук. праць / відп. ред. М. І. Жалдак. Ю. С. Рамський. Київ: НПУ ім. М. П. Драгоманова, 2017. № 19 (26). С. 136–140.
4. Ящик О. Б., Марцинюк Р. Д. Профілактика інтернет-залежності в учнів старших класів. Матеріали VI Всеукраїнської науково-практичної інтернет-конференції «Актуальні проблеми та перспективи технологічної і професійної освіти». Тернопіль: ТНПУ ім. В. Гнатюка, 2021. С. 77–78.
5. Ящик О., Твердохліб І., Франко Ю., Ожга М. Використання технології блокчейн для забезпечення автоматизації управління освітніми документами. Наукові записки Тернопільського національного педагогічного університету імені Володимира Гнатюка. Серія: педагогіка. 2022. Ч. 1. С. 113–120. DOI: https://doi.org/10.25128/2415-3605.22.2.14

REFERENCES

1. Hevko I. V. The use of modern information technologies in the education of students of a higher educational institution. [Vykorystannia suchasnykh informatsiinykh tekhnolohii u navchanni studentiv Vyshchoho navchalnoho zakladu]. Scientific journal of the National Pedagogical University named after M. P. Drahomanov. Series 5. Pedagogical sciences: realities and prospects; collection of scientific works Issue 62: / Ministry of Education and Science of Ukraine, Nat. ped. University named after M. P.

Drahomanov. Kyiv: Publishing House of M. P. Drahomanov NPU [Naukovyi chasopys Natsionalnoho pedahohichnoho universytetu imeni M. P. Drahomanova. Seriia 5. Pedahohichni nauky: realii ta perspektyvy; zbirnyk naukovykh prats Vypusk 62: / M-vo osvity i nauky Ukrainy, Nats. ped. un-t im. M. P. Drahomanova. Kyiv: Vyd-vo NPU imeni M. P. Drahomanova], 2018. S. 46–50.

2. Yashchyk O. B. Application of SMART technologies in society for the construction of smart cities. [Zastosuvannia SMART-tekhnolohii v suspilstvi dlia pobudovy rozumnykh mist]. Modern problems of graphic training of students in ZFPO: theory and practice. Electronic collection of materials of the scientific and practical online conference [Suchasni problemy hrafichnoi pidhotovky studentiv u ZFPO: teoriia i praktyka. Elektronnyi zbirnyk materialiv naukovo-praktychnoi onlain-konferentsii]. (Ternopil, March 16, 2023). Ternopil: VSP "TFC TNTU", 2023. P. 59–69.
3. Yashchyk O. B. Strengthening of the global culture of cyber security on the Internet. [Zmitsnennia hlobalnoi kultury kiberbezpeky v merezhi Internet.]. Computer-oriented learning systems: coll. of science works / resp. ed. M. I. Zhaldak. Yu. S. Ramskyi. Kyiv: National Pedagogical Dragomanov University, [Kompiuterno-oriientovani systemy navchannia: zbirnyk nauk. prats / vidp. red. M. I. Zhaldak. Yu. S. Ramskyi. Kyiv: NPU im. M. P. Drahomanova] 2017. No. 19 (26). P. 136–140.
4. Yashchyk O. B., Martsyniuk R. D. Prevention of Internet addiction in high school students. Materials of the VI All-Ukrainian Scientific and Practical Internet Conference "Actual Problems and Prospects of Technological and Vocational Education". [Profilaktyka internet-zalezhnosti v uchniv starshykh klasiv. Materialy VI Vseukrainskoi naukovo-praktychnoi internet-konferentsii «Aktualni problemy ta perspektyvy tekhnolohichnoi i profesiinoi osvity»]. Ternopil: Ternopil Volodymyr Hnatiuk National Pedagogical University, 2021. P. 77–78.
5. Yashchyk O., Tverdokhlib I., Franko Y., Ozhha M. Use of blockchain technology to ensure automation of educational documents management. Scientific Notes of Ternopil Volodymyr Hnatiuk National Pedagogical University. Series: pedagogy. [Vykorystannia tekhnolohii blokchein dlia zabezpechennia avtomatyzatsii upravlinnia osvitnimy dokumentamy. Naukovi zapysky Ternopilskoho natsionalnoho pedahohichnoho universytetu imeni Volodymyra Hnatiuka. Seriia: pedahohika]. 2022. 1. P. 113–120. DOI: https://doi.org/10.25128/2415-3605.22.2.14.