УДК 342.951(004.896)+351.327.355
DOI https://doi.org/10.32782/2524-0374/2024-4/107

РЕНЕСАНС ЦИФРОВИХ ТЕХНОЛОГІЙ ТА НАЦІОНАЛЬНА БЕЗПЕКА: ОЦІНКА ВПЛИВУ IOT, AI, ВІРТУАЛЬНОЇ РЕАЛЬНОСТІ

DIGITAL RENAISSANCE AND NATIONAL SECURITY: ASSESSING THE IMPACT OF IOT, AI, AND VIRTUAL REALITY

Прокопович-Ткаченко Д.І., к.т.н.,
доцент кафедри кібербезпеки та інформаційних технологій
Університет митної справи та фінансів

Саричев В.І., д.е.н.,
професор кафедри економіки та економічної безпеки
Університет митної справи та фінансів

Пархоменко А.І., старший викладач кафедри військової підготовки
Університет митної справи та фінансів

Поплавський О.О., к.і.н.,
доцент кафедри військової підготовки
Університет митної справи та фінансів

У роботі оцінюється вплив нових технологій на національну безпеку та суспільство в цілому. Дослідження констатує ренесанс цифрових технологій як трансформаційну силу, що впливає на всі сфери людської діяльності. Зазначається, що такі технології, як Metaverse, IoT, AI, AR/VR, машинне навчання та блокчейн, стимулюють соціальні зміни та сприяють новому технологічному стрибку цивілізації. Зосереджено увагу на розвитку віртуальних середовищ, таких як Metaverse, підкреслено прискорення до більш інтегрованого цифрового суспільства та соціальних відносин. Обговорюються різні застосування цих технологій, від медичної до військової сфери, наголошуючи на їхніх потенційних перевагах і ризиках для безпеки.

У дослідженні вказано на існування різновидів Metaverse, компонентів та їх потенціал як суб'єктів (осіб) та об'єктів. Також зосереджено увагу на концепції DarkMetaverse, як антагоністичного елемента, що може створювати значні виклики національній та кібербезпеці.

Вирішальною для дослідження є роль AI та IoT як невід'ємних частин Metaverse та їх наслідків для національної безпеки. Наголошується на необхідності всебічного аналізу впливу AI на аспекти національної безпеки, пропонується ідентифікація областей, чутливих до впливу AI, і методів використання AI для посилення національної безпеки в Metaverse, що швидко розвивається.

Пропонується багатовекторний підхід до вирішення проблем безпеки, пов'язаних з інтеграцією зазначених технологій у повсякденне життя та критичну інфраструктуру. Це включає аналіз технологічної основи AI, IoT та Metaverse, вивчення питань безпеки та конфіденційності, моделювання поточних і майбутніх загроз безпеці та вивчення ландшафту безпеки Metaverse. Наголошується на необхідності постійних досліджень і розробок, щоб зменшити ризики, пов'язані з Metaverse, AI та IoT, на тлі розвитку технологій і зростання складності цифрової екосистеми.

Дослідження представляє детальне дослідження складного ландшафту безпеки Metaverse, підкреслюючи необхідність постійних інновацій, адаптації законодавства та розробки нових методологій для забезпечення безпечного та інклюзивного цифрового простору. Комплексний аналіз дає актуальну інформацію про виклики та можливості, які відкриває цифрова трансформація, підкреслюючи критичну потребу в прогресивному підході до розвитку сучасних інформаційно-комунікаційних технологій.

Ключові слова: Metaverse, штучний інтелект (AI), Інтернет речей (IoT), національна безпека, критична інфраструктура, цифрова трансформація, доповнена реальність (AR), віртуальна реальність (VR).

The paper assesses the impact of new technologies on national security and society. The study defines the digital renaissance as a transformative force that affects all spheres of human activity. It is stated that technologies such as Metaverse, IoT, AI, AR/VR, machine learning and blockchain stimulate social change and contribute to a new technological leap of civilization. The focus is on the development of virtual environments such as the Metaverse, emphasizing the acceleration towards a more integrated digital society and social relations. Various applications of these technologies, from medical to military, are discussed, emphasizing their potential benefits and security risks.

The study points to the existence of different types of Metaverse, components and their potential as subjects (individuals) and objects (legal entities, avatars, digital assets) in these virtual spaces. The author also emphasizes the existence of the Dark Metaverse concept as an antagonistic element that poses significant challenges to national and cybersecurity in this emerging technological field.

The role of AI and IoT as integral parts of the Metaverse and their implications for national security is crucial for the study. The author emphasizes the need for a comprehensive analysis of the impact of AI on national security aspects, proposes the identification of areas sensitive to the impact of AI, and methods of using AI to enhance national security in the rapidly evolving Metaverse.

A multidimensional approach to solving security problems associated with the integration of these technologies into everyday life and critical infrastructure is proposed. This includes analyzing the technological basis of AI, IoT, and Metaverse, studying security and privacy issues, modeling current and future security threats, and studying the Metaverse security landscape. It emphasizes the need for ongoing research and development to mitigate the risks associated with the Metaverse, AI, and IoT as technology evolves and the digital ecosystem becomes more complex.

The study presents a detailed exploration of the complex Metaverse security landscape, emphasizing the need for continuous innovation, adaptation of legislation, and development of new methodologies to ensure a safe and inclusive digital space. The comprehensive analysis provides up-to-date information on the challenges and opportunities presented by digital transformation, emphasizing the critical need for a progressive approach to the development of modern information and communication technologies.

Key words: Metaverse, artificial intelligence (AI), Internet of Things (IoT), national security, critical infrastructure, digital transformation, augmented reality (AR), virtual reality (VR).

Метою статті є оцінка впливу Metaverse, IoT, штучного інтелекту (AI), технологій доповненої реальності (AR) і віртуальної реальності (VR) у зв'язку з їх впливом на сферу національної безпеки та на суспільство.

Виклад основних положень. Ренесанс цифрових технологій Metaverse, IoT, AI, AR/VR, машинного навчання, блокчейну формують нові соціальні зміни, що впливають на всі сфери життєдіяльності людини. Ці технології дали

поштовх ребрендингу Facebook на Meta та розвитку віртуальних середовищ Metaverse, що, в свою чергу, наблизило цивілізацію до нового технологічного стрибка. Metaverse та інші віртуальні простори містять потенціал для різноманітних застосувань. Однак це широке впровадження новітніх віртуальних технологій висуває на перший план критичні проблеми щодо національної та безпеки в цій технологічній сфері, що зароджується [1].

На сьогодні в світі функціонують кілька різновидів Metaverse, суб'єктами Metaverse вважаються фізичні особи, а до категорії об'єктів певний час будуть віднесені юридичні особи, аватари, електронні особи, віртуальні цифрові роботи класу AAI та ASI, цифрові гуманоїди, немайнові електронні активи всіх форм та видів тощо. Metaverse стає більш структурованою і складатиметься з таких провідних елементів: Personal metaverse (PM), Collective metaverse (CM), Corporate metaverse (CorpM), Confederate metaverse (CfM), State metaworld (SM) та Megametaverse or Whitemetaverse (MMV or WM). Megametaverse or Whitemetaverse (MMV or WM) – загальний децентралізований електронний простір, в якому існують безліч персональних, колективних, корпоративних, конфедеративних та державних Metaverse, які взаємодіють між собою на підставі законодавства WM [2].

Також будуть функціонувати Darkmetaverse (DarkMet), як обов'язковий антагоністичний елемент, в якому можуть сконцентруватися суб'єкти, об'єкти та Metaverse із системою самоуправління відмінною від прийнятої у WM. Крім того, DarkMet може бути елементом військового, політичного, економічного втручання в діяльність інших держав з боку певних країн [3].

Ця нова цифрова реальність створить нові виклики кібербезпеці та національній безпеці і посилить уже існуючі цифрові проблеми. На жаль, нові технології часто розробляються та виводяться на ринок задовго до вирішення питань їх юридичного, технологічного та безпекового регулювання, що генерує багато деструктивних соціальних патологій, які можуть мати значно серйозніші наслідки, ніж ті, що спостерігаємо сьогодні.

Як відомо штучний інтелект (AI) є невід'ємним елементом Metaverse. Нині AI став платформою, що може впливати на різноманітні аспекти життя суспільства. Проте, однією з сфер, на яку розвиток AI має особливо потужний вплив, є національна безпека. Важливість штучного інтелекту для підвищення національної безпеки стала предметом значного інтересу та занепокоєння урядів усього світу.

Розвиток штучного інтелекту (AI) ініціює формування нової дослідницької галузі, зосередженої на фундаментальному, комплексному аналізі та оцінці його впливу на аспекти національної безпеки. Вплив AI на національну безпеку має широкий спектр проявів, де застосування технологій AI дозволяє державам розширити свої можливості у сферах акумуляції, зберігання інформації та моніторингу ключових глобальних процесів, а також виявлення загроз і розробки відповідних реакцій для мінімізації потенційних ризиків. Основні напрями дослідження впливу AI на національну безпеку включають:

1. Аналіз технологічної основи AI та Metaverse: детальне дослідження ключових технологій, що лежать в основі AI та Metaverse, включно з блокчейном, технологією штучного інтелекту, інтерактивними технологіями, хмарними сервісами, Інтернетом речей (IoT) та цифровими двійниками.

2. Вивчення проблем безпеки та конфіденційності: аналіз потенційних викликів безпеки та конфіденційності, які можуть виникнути внаслідок інтеграції зазначених технологій для забезпечення балансу між технологічним прогресом та захистом основних прав і свобод громадян.

3. Моделювання поточних та майбутніх загроз безпеки: виявлення та розробка стратегій реагування на безпекові виклики, що виникають від основних технологій, що підтримують AI та Metaverse, з метою ефективної мінімізації можливих ризиків та загроз.

4. Аналіз безпекового ландшафту Metaverse, що вимагає інтегрованого, мультидисциплінарного підходу для ефективного забезпечення безпеки, а також адаптації існуючих стратегій безпеки та розробки нових методологій, які б враховували унікальні аспекти та виклики, притаманні Metaverse.

5. Формування безперервних досліджень та розробок, встановлення критичних потреб в безперервних дослідженнях та розробках, адаптивного підходу до розробки безпекових рішень, що враховують динамічну природу загроз та експлуатаційного середовища, з метою мінімізації ризиків, асоційованих з Metaverse та AI, на фоні постійної еволюції технологій та зростаючої складності цифрових екосистем.

6. Формування етичних кордонів та обов'язковості проведення етичного аналізу та оцінок при розробці політик та механізмів безпеки та конфіденційності з застосуванням AI та Metaverse, розробку високих етичних стандартів забезпечення захисту прав та свобод користувачів, а також сприяння створенню справедливого та інклюзивного цифрового простору.

Дослідження безпеки та конфіденційності Metaverse свідчить, що інновації та адаптація законодавства є важливими для ефективного управління ризиками, пов'язаними з Metaverse, особливо у таких сферах:

– визначення прав і відповідальності користувачів Metaverse для підтримки порядку та безпеки глобального кіберпростору;

– відповідальність щодо захисту даних та забезпечення виконання обов'язків щодо захисту даних;

– посилення стандартів автентифікації у Metaverse;

– перегляд та оновлення чинних законів і нормативних актів, які не були розроблені з урахуванням такого складного цифрового середовища, як Metaverse;

– підтримання порядку в децентралізованому світі Metaverse.

З метою забезпечення фундаментально безпечного віртуального світу, майбутні закони та нормативні акти повинні розвиватися разом із Metaverse, гарантуючи, що вони придатні для цілей управління новою цифровою сферою. При цьому, ландшафт безпеки Metaverse є складним через інтеграцію безлічі існуючих технологій, що створює численні ризики та виклики для безпеки.

Metaverse також глибоко впливає на різні потреби людей, змінюючи спосіб життя, спілкування та ведення бізнесу, що водночас створює нові проблеми безпеки, такі як загрози захисту даних, крадіжка особистих даних і шахрайство з використання інформації, отриманої нелегальним шляхом. Наприклад, хмарні сервіси та Інтернет речей (IoT), які обробляють великомасштабні дані та часто є децентралізованими, стикаються з проблемами керування, якими можуть скористатися зловмисники, що підкреслює необхідність покращення безпеки інфраструктури та даних. Окрім цього, безпека інтерактивних технологій, таких як доповнена реальність (AR) і віртуальна реальність (VR), представляє проблеми з точки зору величезної кількості інформації, яку можна вкрасти, і труднощів під час автентифікації особи. Для підвищення безпеки в цих середовищах використовуються біометричні методи автентифікації, такі як розпізнавання ходи. Однак їх також потрібно захистити від більш витончених атак, таких як технологія синтезу голосу та схеми плечового серфінгу.

Поряд з цим, безпека штучного інтелекту є ще однією проблемою, оскільки багато алгоритмів AI, які виконують завдання класифікації та розпізнавання, мають характеристики «чорного ящика», що ускладнює виявлення кібератаки.

Достатньо ефективною з позиції захисту даних є технологія цифрових близнюків, яка може створювати без-

печні симуляції реального світу. Вона була запропонована як метод посилення безпеки Metaverse шляхом надання посилань на безпечний дизайн, виявлення вторгнень і тестування безпеки.

Тому, вкрай важливо знайти баланс між регуляторними заходами та досвідом користувачів. Надмірне регулювання може погіршити взаємодію з користувачем, тоді як недостатнє регулювання може не підтримувати стандарти безпеки та конфіденційності. Ці приклади ілюструють багатогранний підхід, необхідний для вирішення проблем безпеки Metaverse, які включають технологічні, управлінські та нормотворчі аспекти для забезпечення безпечного та надійного цифрового середовища.

Етичні наслідки є також важливим аспектом, який слід враховувати під час розробки рішень щодо безпеки та конфіденційності Metaverse. Найбільш важливими серед них, на наш погляд, є такі:

− Конфіденційність та контроль даних. Metaverse створює гострі проблеми для особистої конфіденційності через те, що розробники можуть контролювати всі аспекти своїх платформ Metaverse, збираючи величезну кількість даних користувачів. Це викликає етичні питання щодо згоди користувача, монетизації даних і можливості зловживання цими даними через децентралізований характер Metaverse, який важко піддається регулюванню.

− Анонімність, псевдонімізаця і зловживання. Анонімність у Metaverse може призвести до різних форм зловживання, зокрема до поширення тероризму, порушення інтелектуальної власності та інших зловмисних дій, використання користувачів для шкідливих цілей.

− Соціальна інженерія – це тактика маніпулювання, за допомогою якої можливо обманом змусити користувачів порушити їх безпеку або розкрити конфіденційну інформацію. У Metaverse, де маскування злочинців може бути переконливішим і їх важче виявити, існує підвищений ризик маніпуляцій, що викликає етичні занепокоєння щодо використання довіри та необхідності навчання користувачів проти застосування такої тактики.

− Штучний інтелект і робототехніка. З розвитком AI та робототехніки в Metaverse значно звужуються вплив принципів етики, підзвітності і законів, які регулюють взаємодію з цими суб'єктами. Етичні проблеми тут, з одного боку, полягають у формуванні потреби щодо відповідальності за дії штучного інтелекту, який має поважати конфіденційність користувачів. З іншого – нагальною потребою стає потенційний суспільний вплив щодо якості рішень та взаємодії штучного інтелекту.

− Шкідливий інформаційний вміст. Metaverse також може зіткнутися з проблемами, пов'язаними зі шкідливим вмістом, таким як фейкові новини, розпалювання ворожнечі, релігійний екстремізм, расизм, публічне залякування та переслідування. Етичні наслідки передбачають створення середовища, яке б сприяло безпеці та інклюзивності, поважаючи свободу слова.

Вирішення цих етичних проблем вимагає багатогранного підходу, який включає технологічні рішення, освіту користувачів і чітку правову та нормативну базу для регулювання поведінки в Metaverse.

Аналіз та узагальнення поглядів науковців дозволяє сформулювати такі основні напрями досліджень щодо безпеки Metaverse: децентралізована ідентифікація та автентифікація; захист даних; моделі загроз і атак; управління та законодавче регулювання; застосування криптографії для підвищення конфіденційності. Запропоновані напрями є перспективними, підкреслюють важливість як інновацій, так і етичних наслідків впровадження нових технологій.

Для проведення ретельного вивчення нових технологій, таких як Metaverse, особливо в контексті авторитарних режимів, доцільно забезпечити:

1) мультидисциплінарні дослідження та залучення експертів з технологій, соціальних наук, політології та етики, щоб зрозуміти багатогранний вплив Metaverse;

2) аналіз конфіденційності та спостереження, шляхом дослідження можливості Metaverse щодо збору даних і спостереження, а також їхні наслідки для конфіденційності та прав людини;

3) оцінку впливу Metaverse на громадську думку, поширення пропаганди чи контролю над психологією великих груп;

4) порівняльні дослідження, шляхом аналізу різних моделей управління Metaverse та їх впливу на суспільство в різних політичних контекстах та дискурсах;

5) розробку політики та керівних принципів захисту прав користувачів і запобігання зловживанню технологією державними суб'єктами.

Розвиток Metaverse, як інноваційної технології, породжує значні потенційні проблеми, пов'язані з глобальною конфіденційністю та безпекою. Технології доповненої (AR) та віртуальної реальності (VR), які є фундаментальними для функціонування Metaverse, мають інтегровані специфічні вразливості, такі як:

− ризики безпеки доповненої реальності: AR, будучи ключовим компонентом Metaverse, несе в собі значні безпекові виклики, особливо у контексті захисту конфіденційності користувачів;

− ризики безпеки віртуальної реальності: VR разом з AR, також має невирішені проблеми пов'язані із несанкціонованим збором конфіденційних даних, таких як сканування сітківки ока, біометрична інформація та голосові відбитки, крадіжка особистих даних, розрив зав'язків між користувачами/виробниками та програмним забезпеченням, а також загроза шкідливих програм;

− ризики, пов'язані з нелегальним доступом до пристроїв AR/ VR, які можуть вплинути на конфіденційність користувачів;

− способи управління та захисту даних, зібраних за допомогою технологій AR/ VR, компаніями-розробниками; механізми зберігання та шифрування даних, зібраних у контексті доповненої реальності;

− потенційні наслідки передачі даних AR третім сторонам;

− загальні ризики безпеки Metaverse, попри заяви про безпрецедентну інтеграцію та конвергенцію, Metaverse в суті своїй включає ризики, пов'язані з конфіденційністю, фізичною безпекою, радикалізацією та поляризацією. Інтеграція різноманітних груп користувачів в один віртуальний домен може призвести до серйозних безпекових викликів. Враховуючи динамічний розвиток Metaverse, ключовим завданням є розробка ефективних стратегій і політик для адресації цих комплексних проблем безпеки з метою створення безпечного, інклюзивного та стійкого цифрового середовища для сучасних та майбутніх поколінь.

Наступний базововий елемент Metaverse – IoT та його сучасні різновиди. Інтернет речей (IoT) є поняттям, що описує мережу фізичних об'єктів («речей»), оснащених вбудованими сенсорами, програмним забезпеченням та іншими технологіями для з'єднання та обміну даними з іншими пристроями та системами через Інтернет. Ця концепція розширює можливості Інтернет-з'єднання за межі стандартних пристроїв, таких як комп'ютери та смартфони, до широкого спектру невеликих фізичних гаджетів [3].

Промисловий Інтернет речей (IIoT) представляє собою застосування концепції IoT у промисловому секторі, включаючи виробництво, логістику, нафто- та газопровідний транспорт, агрокультуру та інші галузі. IIoT спрямований на покращення операційної ефективності, безпеки та надійності через автоматизацію процесів та оптимізацію управління активами, шляхом впровадження сенсор-

них технологій та мережевої інтеграції для моніторингу, збору, обміну та аналізу даних в реальному часі.

Інтернет бойових речей (IoBT) [4] являє собою адаптацію IoT для військових цілей, об'єднання та з'єднання військових засобів, військ та інших активів (ресурсів сили) для підвищення ситуаційної обізнаності, точності цілевказівок та ефективності бойових операцій, шляхом поєднання передових технологій, таких як штучний інтелект, машинне навчання, робототехніка та сенсорні мережі, для створення взаємопов'язаної, інтегрованої оборонної системи [5, 6].

Інтернет медичних речей (IoMT) відноситься до інтеграції IoT в галузі охорони здоров'я і включає використання під'єднаних медичних пристроїв та інших технологій для збору даних, які використовуються для моніторингу, інформування та попередження пацієнтів та медичних працівників [7].

Існують і інші специфічні різновиди IoT, кожен з яких адаптований до конкретних потреб та вимог різних галузей та доменів, наприклад, Інтернет речей у сфері смарт-дому (smart home IoT) або агротехнологічний IoT.

У контексті зростаючої інтеграції технологій IoT, IIoT, IoBT та IoMT в повсякденне життя та критичну інфраструктуру, важливо оцінити потенційні ризики, які ці технології можуть представляти для національної безпеки. Визнання та адекватне реагування на наступні важливі ризики для захисту суверенітету та забезпечення стабільності в державі.

Ризики для національної безпеки, пов'язані з IoT:

– кібербезпека: збільшення кількості підключених до Інтернету пристроїв створює більше точок входу для кібератак, що може призвести до несанкціонованого доступу до важливих даних та критичних систем;

– витік даних: bigdata, що збираються IoT-пристроями, може включати чутливу інформацію, яка при витоку може становити загрозу для національної безпеки;

– маніпуляція даними: втручання в bigdata, що збираються або передаються IoT-пристроями, може призвести до помилкових рішень, базованих на деструктивній інформації;

– порушення функціонування критичної інфраструктури: втручання в роботу промислових IoT-систем може призвести до зупинки виробництва, пошкодження обладнання або навіть екологічних катастроф;

– шпигунство: IIoT пристрої можуть бути використані для незаконного збору інформації про промислові процеси, виробничі таємниці та іншу важливу інформацію;

– військова парадигма, дилема національної оборони: кібератаки на військові системи через втручання в IoBT може призвести до збоїв у роботі оборонних систем, що може мати катастрофічні наслідки, а викрадення військових технологій шляхом несанкціонованого доступу до IoBT може дозволити противникам оволодіти військовими технологіями або інформацію;

– загроза здоров'ю населення: кібератаки на медичні IoT-пристрої, такі як імплантовані медичні пристрої або системи моніторингу пацієнтів, можуть призвести до загрози життю або здоров'ю людей;

– витік медичної інформації: несанкціонований доступ до IoMT може призвести до витоку чутливої медичної інформації, що ставить під загрозу конфіденційність та здоров'я пацієнтів.

Поява та інтеграція технологій Metaverse, Інтернету речей (IoT), штучного інтелекту (AI), доповненої реальності (AR) і віртуальної реальності (VR) створює як безпрецедентні можливості, так і значні виклики для національної безпеки та суспільного добробуту, враховуючи багатогранний характер цих технологій, ілюструючи їхній потенціал революціонізувати різні сектори, включаючи охорону здоров'я, військові та промислові застосування [8]. В той же час очевидним є факт наявності низки критичних вразливостей системи безпеки.

Поширення екосистем Metaverse та інших технологій розширює спектр атак та кіберзагроз, створюючи ризики для конфіденційності, цілісності та доступності даних. Здатність цих технологій збирати й обробляти величезні обсяги особистих і конфіденційних даних викликає серйозні занепокоєння щодо конфіденційності, захисту даних і можливого зловживання. Водночас, децентралізований і глобальний характер застосування IoT та AI ускладнює регулятивні та управлінські зусилля, кидаючи виклик існуючій правовій базі та вимагаючи міжнародної співпраці для встановлення норм і стандартів, які гарантують безпеку та основні права.

Висновки. Вирішення вказаних у дослідженні проблем вимагає цілісного та проактивного підходу, який охоплює технологічні, нормативні та етичні міркування. Вкрай важливо розробити надійні заходи кібербезпеки, політику захисту даних і механізми автентифікації для захисту від несанкціонованого доступу та витоків даних. Крім того, сприяння прозорості, підзвітності та розширення можливостей користувачів матиме вирішальне значення для забезпечення того, щоб ці технології використовувалися етично та відповідально, узгоджуючи суспільні цінності та права людини.

Поряд з цим, безперервні дослідження та співпраця між урядами, галузевими зацікавленими сторонами та академічною спільнотою є важливими для передбачення нових загроз, розробки інноваційних рішень безпеки та адаптації нормативно-правової бази до цифрового середовища, що розвивається. Використовуючи мультидисциплінарну та спільну стратегію, можливо використовувати трансформаційний потенціал технологій Metaverse, IoT, AI, AR та VR, одночасно зменшуючи їхні ризики, забезпечуючи безпечне, інклюзивне та стійке цифрове майбутнє для всіх.

Важливість перспективного та адаптивного підходу до навігації в складному ландшафті безпеки Metaverse та пов'язаних технологій може покласти основу для вирішення багатогранних викликів до національної безпеки, стимулювання економічного зростання та покращення якості життя, одночасно забезпечуючи захист конфіденційності, безпеки та основних свобод у цифрову епоху.

ЛІТЕРАТУРА

1. R. Di Pietro and S. Cresci. (2021). Metaverse: Security and Privacy Issues. *2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, pp. 281–288. DOI: https://doi.org/10.1109/TPSISA52974.2021.00032
2. Kostenko, O., Furashev, V., Zhuravlov, D., & Dniprov, O. (2022). Genesis of Legal Regulation Web and the Model of the Electronic Jurisdiction of the Metaverse. *Bratislava Law Review*, 6(2), 21–36. DOI: https://doi.org/10.46282/blr.2022.6.2.316
3. Kostenko, O. V. (2022). Electronic Jurisdiction, Metaverse, Artificial Intelligence, Digital Personality, Digital Avatar, Neural Networks: Theory, Practice, Perspective. *World Science*. 1(73), 1–13. DOI: https://doi.org/10.31435/rsglobal_ws/30012022/7751
4. Z. Chen, J. Wu, W. Gan and Z. Qi. (2022). Metaverse Security and Privacy: An Overview. *2022 IEEE International Conference on Big Data (Big Data)*, pp. 2950–2959. DOI: 10.1109/BigData55660.2022.10021112
5. Md I. Hossain and R. Hasan (2023). Threat Model-based Security Analysis and Mitigation Strategies for a Trustworthy Metaverse. *2023 IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom)*, pp. 33–40. DOI: 10.1109/MetaCom57706.2023.00021
6. Zhang Zhao, Guo Yujie, Zhao Xiaoning, et al. Military Metaverse: Key Technologies, Potential Applications and Future Directions. J*ournal of System Simulation*, 2023, 35(7):1421–1437. DOI: 10.16182/j.issn1004731x.joss.23-0104
7. Kott, Alexander, Ananthram Swami, and Bruce J. West. The Internet of Battle Things. *Computer* 49.12 (2016): 70–75. URL: https://people.computing.clemson.edu/~jmarty/projects/lowLatencyNetworking/papers/TheInternetOfBattleThings.pdf
8. Гріффін М. Що таке IoMT (Інтернет медичних речей)? 2022. URL: https://fiberroad.com/uk/resources/articles/what-is-iomt-internet-of-medical-things/