Бєлкін Леонід, *кандидат технічних наук, старший науковий співробітник, адвокат, адвокат індивідуальної практики, Київ, Україна*

https://orcid.org/0000-0001-8672-8147

Криволап Євгеній, PhD, спеціаліст з IT, *Київ, Україна*

https://orcid.org/0000-0003-2599-2520

Юринець Юлія, *доктор юридичних наук, професор, професор кафедри права та публічного управління Київського національного університету будівництва та архітектури, Київ, Україна,*

https://orcid.org/0000-0003-0281-3251

Belkin Leonid, *Candidate of Technical Sciences, Senior Researcher, Attorney, Individual Practice Attorney, Kyiv, Ukraine*

https://orcid.org/0000-0001-8672-8147

Kryvolap Evgeny, *PhD, IT specialist, Kyiv, Ukraine*

https://orcid.org/0000-0003-2599-2520

Iurynets Juliya, *Professor of the Department of Law and Public Administration, Kyiv National University of Civil Engineering and Architecture, Kyiv, Ukraine*

https://orcid.org/0000-0003-0281-3251

КІБЕРБЕЗПЕКА ВІРТУАЛЬНИХ АКТИВІВ: ПРАВОВИЙ АСПЕКТ

CYBERSECURITY OF VIRTUAL ASSETS: LEGAL ASPECT

Анотація

У статті досліджено доктринальні та законодавчі проблеми

забезпечення надійності віртуальних активів у контексті кібербезпеки та кіберзахисту. Обґрунтовано актуальність удосконалення правового регулювання сфери віртуальних активів з огляду на поширення цифрових технологій, зростання кількості кіберзагроз, шахрайських дій, хакерських атак та ризиків втрати цифрових активів. Проаналізовано положення Цивільного кодексу України, відповідно до яких віртуальні активи віднесено до цифрових речей, а також норми законодавства у сфері кібербезпеки та правового регулювання обігу віртуальних активів. Визначено взаємозв'язок між правовим статусом віртуальних активів та необхідністю забезпечення їх цілісності, конфіденційності, доступності й надійності.

Досліджено положення Закону України «Про віртуальні активи», які передбачають повноваження Національної комісії з цінних паперів та фондового ринку і Національного банку України щодо встановлення вимог до інформаційної безпеки та кібербезпеки постачальників послуг, пов'язаних з оборотом віртуальних активів. Наголошено, що чинне регулювання має фрагментарний характер.

Розглянуто основні види загроз інформаційній безпеці, зокрема копіювання, знищення, модифікацію та блокування інформації, а також обман. Визначено основні технологічні й організаційні заходи підвищення рівня інформаційної безпеки, серед яких використання надійних паролів, оновлення програмного забезпечення, антивірусний захист, двофакторна автентифікація та резервне копіювання.

Запропоновано основні напрями вдосконалення правового регулювання: усунення законодавчих прогалин і колізій, встановлення мінімальних стандартів кібербезпеки для учасників ринку, визначення особливостей відповідальності за порушення кібербезпеки, вдосконалення доказування у спорах щодо цифрових активів та гармонізацію національного законодавства з європейськими підходами.

Ключові слова: віртуальні активи; цифрові речі; кібербезпека; кіберзахист; інформаційна безпека; кіберзагрози; цифрове середовище; захист прав; цифрова економіка; правове регулювання.

Abstract

The article examines doctrinal and legislative issues concerning the reliability of virtual assets in the context of cybersecurity and cyber protection. The relevance of improving the legal regulation of virtual assets is substantiated in view of the widespread adoption of digital technologies, the increasing number of cyber threats, fraudulent activities, hacker attacks, and the risks of digital asset loss. The provisions of the Civil Code of Ukraine, under which virtual assets are classified as digital things, as well as the legislation governing cybersecurity and the legal regulation of virtual asset circulation, are analyzed. The relationship between the legal status of virtual assets and the need to ensure their integrity, confidentiality, availability, and reliability is established.

The provisions of the Law of Ukraine “On Virtual Assets” concerning the powers of the National Securities and Stock Market Commission and the National Bank of Ukraine to establish information security and cybersecurity requirements for service providers involved in the circulation of virtual assets are examined. It is emphasized that the current regulatory framework remains fragmented.

The main types of threats to information security are considered, including the copying, destruction, modification, and blocking of information, as well as deception. The principal technological and organizational measures for improving information security are identified, including the use of strong passwords, software updates, antivirus protection, two-factor authentication, and data backup.

The main directions for improving legal regulation are proposed, including eliminating legislative gaps and conflicts, establishing minimum cybersecurity standards for market participants, determining specific forms of liability for

cybersecurity violations, improving evidentiary procedures in disputes concerning digital assets, and harmonizing national legislation with European approaches.

Keywords: virtual assets; digital things; cybersecurity; cyber protection; information security; cyber threats; digital environment; rights protection; digital economy; legal regulation

Постановка проблеми. Попри динамічне становлення та розвиток сфери віртуальних активів в Україні, механізми правового регулювання їх обігу, а також забезпечення та захисту цивільних прав користувачів і інвесторів залишаються недостатньо результативними. Однією з ключових проблем є те, що чинна нормативно-правова база, зокрема Закон України «Про віртуальні активи» № 2074-IX від 17.02.2022 року, не забезпечує повною мірою належний рівень захисту учасників відповідного ринку. Це зумовлено, зокрема, недостатньою визначеністю правового статусу віртуальних активів, неповною регламентацією відповідальності постачальників послуг, пов’язаних з їх оборотом, а також недостатнім розвитком судової практики. Наявні прогалини породжують правову невизначеність, збільшують імовірність шахрайських дій та втрати активів, а також негативно впливають на рівень довіри до ринку, що набуває особливого значення в умовах розвитку цифрової економіки [1].

Аналіз досліджень. Постійний розвиток технічних і технологічних засобів у сфері інформаційних відносин зумовлює необхідність формування належних механізмів захисту як персональної інформації, так і інформації, що має значення на державному рівні. Водночас застосування відповідних програм і технологічних засобів захисту не завжди забезпечує бажаний результат [2, с. 157]. Проблематика кіберзахисту віртуальних активів при цьому залишається недостатньо дослідженою як у науковій літературі, так і в публіцистичних джерелах. Так, у роботі [3] звертається увага на те, що поряд

із численними перевагами, віртуальні активи пов'язані з низкою ризиків і викликів, серед яких особливе місце займають питання регулювання, нестабільність ринку, кібербезпека та шахрайство. У зв'язку з цим актуальним є формування дієвих регуляторних механізмів і заходів безпеки, спрямованих на мінімізацію зазначених ризиків [3, с. 15].

До основних проблем функціонування ринку віртуальних активів належить, зокрема, відсутність достатньо чіткої правової основи його регулювання, що породжує невизначеність для інвесторів, компаній та користувачів. Окремим суттєвим викликом є кібербезпека, оскільки високий рівень шахрайства, хакерських атак на криптовалютні біржі та криптогаманці створює безпосередню загрозу збереженню активів [3, с. 16].

У публікації [4] кібербезпека розглядається як комплекс заходів, спрямованих на захист цифрових активів, комп'ютерних систем, мереж і даних від несанкціонованого доступу та пошкодження. Її призначення полягає, зокрема, у забезпеченні безперервності діяльності, збереженні конфіденційності інформації та дотриманні встановлених законодавством вимог. Окремі аспекти кібербезпеки також досліджувалися співавторами у попередніх наукових працях [5, 6].

Мета роботи – розкрити доктринальні і законодавчі проблеми захисту надійності віртуальних активів в системі кібербезпеки та кіберзахисту.

Виклад результатів. Відповідно до статті 177 Цивільного кодексу України в редакції Закону України від 10.08.2023 року № 3320-IX «Про внесення змін до Цивільного кодексу України щодо розширення кола об'єктів цивільних прав» до об'єктів цивільних прав належать речі, гроші, цінні папери, цифрові речі, майнові права, роботи та послуги, результати інтелектуальної та творчої діяльності, інформація, а також інші матеріальні й нематеріальні блага.

При цьому об’єкти цивільних прав можуть існувати як у матеріальному світі, так і в цифровому середовищі. Середовище існування відповідного об’єкта визначає форму його існування та особливості набуття, реалізації й припинення цивільних прав та обов’язків щодо нього.

Водночас стаття 179-1 Цивільного кодексу України, також у редакції Закону № 3320-IX від 10.08.2023 року, визначає цифрову річ як благо, яке створюється та існує виключно в цифровому середовищі й має майнову цінність. До цифрових речей віднесено, зокрема, віртуальні активи, цифровий контент та інші блага, щодо яких застосовуються відповідні положення цієї статті. Правовий режим цифрових речей має визначатися законом. При цьому до них застосовуються положення Цивільного кодексу України щодо речей, якщо інше не передбачене самим Кодексом або законом чи не випливає із сутності цифрової речі.

Таким чином, на законодавчому рівні віртуальні активи визначені як цифрові речі.

Водночас відповідно до ч. 1 ст. 4 Закону України від 05.10.2017 року № 2163-VIII «Про основні засади забезпечення кібербезпеки України» до об’єктів кібербезпеки належать, серед іншого, конституційні права і свободи людини та громадянина, а також суспільство, сталий розвиток інформаційного суспільства і цифрового комунікативного середовища.

З огляду на те, що віртуальні активи законодавчо віднесені до цифрових речей, на них мають поширюватися відповідні способи та механізми забезпечення кібербезпеки й кіберзахисту. Однак зазначений підхід не отримав достатнього нормативного розвитку ні в Законі України «Про віртуальні активи», ні в Законі України «Про основні засади забезпечення кібербезпеки України», ні на доктринальному рівні, що свідчить про необхідність подальшого окремого дослідження цієї проблематики.

Віртуальні активи традиційно характеризуються як нематеріальні блага, що мають майнову цінність, існують у цифровій формі та обертаються із застосуванням інформаційно-комунікаційних технологій. Надійність таких активів має комплексний характер і включає їх захищеність від несанкціонованого доступу, забезпечення цілісності даних, стабільності роботи відповідних платформ та реєстрів, а також формування довіри з боку користувачів та інвесторів.

За відсутності належного кіберзахисту забезпечення зазначених характеристик є проблематичним, що, своєю чергою, збільшує ризики шахрайства, втрати активів і різноманітних маніпуляцій. Отже, високий рівень кібербезпеки для віртуальних активів слід розглядати не як факультативний елемент, а як одну з фундаментальних умов їх надійного функціонування.

Закон України від 17.02.2022 року № 2074-IX «Про віртуальні активи» лише фрагментарно передбачає необхідність забезпечення надійності функціонування відповідного ринку за допомогою механізмів кібербезпеки.

Так, відповідно до ч. 1 ст. 16 цього Закону, державне регулювання ринку віртуальних активів полягає у здійсненні державою в особі Національної комісії з цінних паперів та фондового ринку і Національного банку України комплексу заходів щодо організації, контролю та нагляду за ринком віртуальних активів, регулювання діяльності постачальників послуг, пов’язаних з оборотом таких активів, а також запобігання і протидії зловживанням та правопорушенням на відповідному ринку.

Згідно з пунктом 26 ч. 3 ст. 16 зазначеного Закону Національна комісія з цінних паперів та фондового ринку в межах своїх повноважень, зокрема, визначає вимоги щодо забезпечення інформаційної безпеки та кібербезпеки постачальниками послуг, пов’язаних з оборотом віртуальних активів.

Відповідно до пункту 8 ч. 1 ст. 17 цього Закону Національний банк України у сфері обороту віртуальних активів визначає, зокрема, вимоги до забезпечення інформаційної безпеки та кібербезпеки постачальниками послуг, пов'язаних з оборотом забезпечених віртуальних активів, забезпечених валютними цінностями.

Таким чином, кібербезпека є фундаментальним елементом надійного функціонування системи обігу віртуальних активів та охоплює організаційні, правові й технічні заходи, спрямовані на захист інформації, інформаційних систем і мереж від кіберзагроз.

Оскільки віртуальні активи існують виключно в цифровому середовищі, будь-які недоліки програмного забезпечення, криптографічних механізмів або цифрової інфраструктури можуть спричинити істотні наслідки. Хакерські атаки, фішингові схеми, шкідливе програмне забезпечення, компрометація чи злам криптогаманців безпосередньо створюють загрозу надійності операцій із віртуальними активами. Саме тому належний рівень кібербезпеки має розглядатися як необхідна передумова їх існування та обігу.

Взаємодія законодавства про віртуальні активи із законодавством у сфері кібербезпеки зумовлена спільною спрямованістю на забезпечення безпечного цифрового середовища. Нормативне регулювання обігу віртуальних активів визначає їх правовий статус, встановлює правила діяльності постачальників відповідних послуг, спрямоване на захист прав користувачів та передбачає механізми запобігання фінансовим правопорушенням. Натомість законодавство про кібербезпеку встановлює вимоги до захисту інформаційних систем, управління ризиками та реагування на кіберінциденти.

Взаємозв'язок цих двох напрямів нормативного регулювання можна простежити за кількома основними напрямами.

По-перше, це вимоги до безпеки. Учасники ринку віртуальних активів мають забезпечувати впровадження належних заходів кіберзахисту з урахуванням загальних вимог у сфері кібербезпеки.

По-друге, захист користувачів. Механізми кібербезпеки доповнюють правові засоби захисту прав власників віртуальних активів, забезпечуючи додатковий рівень їх безпеки.

По-третє, запобігання правопорушенням. Ефективний кіберзахист дозволяє зменшити ризики шахрайства, легалізації доходів та інших протиправних дій, які можуть здійснюватися в цифровому середовищі.

По-четверте, відповідальність і контроль. Нормативно-правові акти встановлюють відповідні механізми контролю та відповідальності за недотримання вимог як у сфері обігу віртуальних активів, так і у сфері кібербезпеки.

Оскільки віртуальні активи функціонують виключно в цифровому середовищі, їх цілісність, доступність та конфіденційність безпосередньо залежать від рівня захищеності такого середовища. Зазначені характеристики становлять основні складові інформаційної безпеки. Наприклад, втрата або компрометація криптографічних ключів через недостатній рівень захисту може позбавити власника можливості отримати доступ до належних йому активів. Аналогічно атаки на інфраструктуру криптовалютних бірж, обмінних платформ чи гаманців здатні спричинити значні фінансові збитки. Отже, закріплення кіберзахисту як правового обов'язку суб'єктів цифрового ринку є важливим засобом зменшення відповідних ризиків.

Правові приписи мають доповнювати технологічні механізми захисту. Законодавство про віртуальні активи формує основу їх цивільно-правового регулювання, однак без встановлення чітких та обов'язкових вимог у сфері кібербезпеки його практична ефективність залишається обмеженою.

У цьому контексті нормативні акти у сфері кібербезпеки передбачають обов'язки щодо застосування технологічних засобів захисту інформаційних систем, оцінювання ризиків, забезпечення безпеки критичної інформаційної інфраструктури та реагування на кіберінциденти. Реалізація таких вимог посилює правові механізми захисту власників віртуальних активів від шахрайських дій, втрати даних та кібератак.

Забезпечення інформаційної безпеки за допомогою кіберзахисту являє собою комплекс заходів і засобів, спрямованих на гарантування цілісності, конфіденційності та доступності інформації та її захист від природних і штучних загроз. Така система включає фізичний і кіберзахист, контроль доступу, використання антивірусного програмного забезпечення та брандмауерів, своєчасне оновлення програмних систем, резервне копіювання інформації та дотримання встановленої політики безпеки.

До основних принципів і цілей інформаційної безпеки належать: цілісність – забезпечення достовірності та повноти інформації, а також недопущення її несанкціонованої зміни; конфіденційність – обмеження доступу до інформації виключно для уповноважених користувачів; доступність – забезпечення можливості безперешкодного отримання інформації авторизованими користувачами у разі необхідності; автентичність, відстежуваність, неспростовність та надійність – додаткові характеристики, які можуть використовуватися для підвищення загального рівня безпеки.

Відповідно до пункту 5 статті 1 Закону України «Про основні засади забезпечення кібербезпеки України» кібербезпека визначається як захищеність життєво важливих інтересів людини та громадянина, суспільства і держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, а також своєчасне виявлення, попередження та

нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

Пункт 6 статті 1 цього Закону визначає кіберзагрозу як наявні або потенційно можливі явища та чинники, які становлять небезпеку для життєво важливих національних інтересів України у кіберпросторі, негативно впливають на стан кібербезпеки держави, а також на кібербезпеку та кіберзахист відповідних об'єктів.

Відповідно до пункту 7 статті 1 цього ж Закону, кіберзахист охоплює сукупність організаційних, правових, інженерно-технічних, криптографічних та технічних заходів захисту інформації, спрямованих на протидію кіберзагрозам, забезпечення кібербезпеки, стійкості, цілісності, доступності та конфіденційності інформаційних ресурсів у кіберпросторі, а також забезпечення здатності відповідної інфраструктури здійснювати їх обробку.

У доктринальному розумінні кібербезпека, яку також визначають як комп'ютерну безпеку або безпеку інформаційних технологій, передбачає захист комп'ютерних систем і мереж від розкриття інформації, пошкодження чи викрадення обладнання, програмного забезпечення та електронних даних, а також від порушення або неналежного спрямування послуг, що ними надаються [7, с. 56–57].

Кібербезпеку також можна розглядати як застосування сучасних технологій, процедур і засобів контролю, спрямованих на захист комп'ютерних систем, мереж, програм, пристроїв і даних від кібератак та на зменшення ризику їх здійснення [8].

У монографії [9] розглянуто різні види шкоди, яка може бути заподіяна особі внаслідок порушення інформаційної безпеки в інформаційно-комунікаційній системі [9, с. 34–35]. До них належать копіювання комп'ютерної інформації, тобто її відтворення та стійке збереження на іншому носії; знищення інформації шляхом її стирання з пам'яті електронно-

обчислювальної машини; модифікація інформації через несанкціоноване внесення змін до електронних даних; блокування інформації шляхом штучного обмеження доступу автентифікованих користувачів, у тому числі власників інформації, без її фізичного знищення; а також обман, що полягає в умисному викривленні або приховуванні істини з метою введення зацікавлених осіб в оману, зокрема шляхом поширення неправдивої інформації.

Для підвищення рівня інформаційної безпеки доцільним є застосування комплексу практичних заходів, серед яких: використання складних та унікальних паролів для різних сервісів із їх періодичною зміною [10, с. 4]; систематичне оновлення операційної системи та встановленого програмного забезпечення; застосування антивірусних програм і брандмауерів; відмова від відкриття підозрілих електронних листів, завантаження неперевірених файлів та переходу за сумнівними посиланнями; використання двофакторної автентифікації як додаткового способу підтвердження особи; регулярне створення резервних копій інформації для мінімізації ризику її втрати; використання виключно ліцензійного та офіційного програмного забезпечення.

З урахуванням наведеного можна визначити такі основні перспективи вдосконалення правового регулювання.

1. Усунення колізій і прогалин у законодавстві щодо віртуальних активів та кібербезпеки. Незважаючи на існування базових нормативно-правових актів, регулювання відносин у сфері обігу віртуальних активів в Україні залишається неповним і фрагментарним. Закон України «Про віртуальні активи» не встановлює детального переліку вимог до забезпечення кібербезпеки суб’єктів відповідного ринку, фактично залишаючи значну частину такого регулювання на рівні підзаконних

нормативно-правових актів. Водночас загальне законодавство про кібербезпеку не враховує повною мірою специфіку цифрових активів.

Серед основних проблем можна виокремити відсутність чітко визначених стандартів кіберзахисту для постачальників послуг, пов'язаних із віртуальними активами; недостатню врегульованість відповідальності за втрату активів у результаті кіберінцидентів; а також складнощі з правовою кваліфікацією криптоактивів у цивільному та кримінальному процесах. Такі прогалини ускладнюють реалізацію відповідних правових норм та зменшують ефективність захисту прав власників віртуальних активів.

2. Основні напрями вдосконалення національного законодавства. Для підвищення надійності обігу віртуальних активів доцільно законодавчо встановити мінімальні стандарти кібербезпеки для суб'єктів відповідного ринку; визначити особливості цивільно-правової та кримінальної відповідальності за порушення вимог кібербезпеки у сфері віртуальних активів; а також удосконалити процесуальні механізми доказування у спорах, що стосуються цифрових активів. Реалізація зазначених заходів сприятиме підвищенню рівня правової визначеності та зміцненню довіри до цифрових фінансових інструментів.

3. Гармонізація з європейськими підходами. Європейський Союз у процесі формування правил функціонування цифрових фінансових ринків поступово переходить до комплексного регулювання віртуальних активів, у межах якого поєднуються вимоги фінансового законодавства та стандарти кібербезпеки. Для України актуальним є врахування відповідних європейських підходів з одночасним урахуванням особливостей національної правової системи. Гармонізація українського законодавства з європейськими стандартами сприятиме подальшій інтеграції України до європейського цифрового ринку та забезпеченню належного рівня захисту прав учасників відносин у сфері обігу віртуальних активів.

Висновки. Забезпечення надійності віртуальних активів є неможливим без належного рівня кібербезпеки. Технологічна та правова складові цього процесу перебувають у тісному взаємозв'язку та формують комплексну систему захисту цифрових цінностей. Правове регулювання віртуальних активів і законодавство у сфері кібербезпеки не повинні розглядатися як відокремлені нормативні масиви, оскільки вони мають взаємодоповнювальний характер. Подальше вдосконалення правового регулювання має враховувати динаміку розвитку кіберзагроз і бути спрямоване на формування належного рівня довіри до віртуальних активів як складової сучасної цифрової економіки.

Подальші законодавчі ініціативи та розвиток судової практики повинні забезпечити перехід від формального визначення прав та обов'язків учасників ринку до встановлення реальних і дієвих стандартів кіберзахисту для постачальників послуг, пов'язаних з обігом віртуальних активів.

Список джерел

1. Починок О.В. Захист прав власників віртуальних активів: пропозиції щодо вдосконалення законодавства України. *Український політико-правовий дискурс*. 2025. № 8. URL: https://ppdnz.com.ua/index.php/home/article/view/160/93

2. Шевченко С.М., Складанний П.М., Негоденко О.В., Негоденко В.П. Дослідження прикладних аспектів теорії конфліктів у системах безпеки. *Кібербезпека: освіта, наука, техніка*. 2022, № 2 (18), С. 150-162. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/411/339

3. Микитенко Т.П. Віртуальні активи в умовах цифрових трансформацій економіки. *Вчені записки ТНУ імені В. І. Вернадського. Серія: Економіка і управління*. 2024. Том 35 (74). № 3. С. 14-19.

4. Колесніков Д. Що таке кібербезпека? *BRAINLAB*. 30.08.2024. URL: https://brainlab.com.ua/uk/blog-uk/shho-take-kiberbezpeka

5. Бєлкін Л.М., Юринець Ю.Л., Бєлкін М.Л., Криволап Є.В. Співвідношення понять «інформаційна безпека», «безпека інформації», «кібербезпека» в контексті безпекових стратегій України 2020-2021 років. *Наукові праці Національного авіаційного університету: Серія «Юридичний вісник. Повітряне і космічне право»*. 2022. № 3 (64). С. 78-86.

6. Юринець Ю.Л., Криволап Є.В., Бєлкін Л.М., Бєлкін М.Л. Захист надійності віртуальних активів в системі кібербезпеки та кіберзахисту. *Актуальні питання у сучасній науці*. 2026. № 1 (43). С. 1120-1129.

7. Lubenets S., Harchenko I., Pavlenko Y. Current problems of international information security. *The Journal of V.N. Karazin Kharkiv National University*. 2023. Vol. 17, pp. 42–48.

8. Luidold C., Jungbauer C. Cybersecurity policy framework requirements for the establishment of highly interoperable and interconnected health data spaces. *Frontiers in Medicine*. 2024. Vol. 11.

9. Юдін О.К., Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних. К. Вид-во ТОВ «НВП «ІНТЕРСЕРВІС» 2009. 716 с.

10. Парольний захист комп'ютерного та телекомунікаційного обладнання. Наук.-практ. посіб. Авт. кол.: М.Г. Вербенський, В.О. Криволапчук, Д.В. Смерницький та ін. Київ: «Видавництво Людмила», 2022. 42 с.

References:

1. Pochynok O.V. (2025). Zakhyst prav vlasnykiv virtualnykh aktyviv: propozytsii shchodo vdoskonalennia zakonodavstva Ukrainy. *Ukrainskyi polityko-pravovyi dyskurs*. № 8. URL: https://ppdnz.com.ua/index.php/home/article/view/160/93

2. Shevchenko S.M., Skladannyi P.M., Nehodenko O.V., Nehodenko V.P. (2022). Doslidzhennia prykladnykh aspektiv teorii konfliktiv u systemakh bezpeky. *Kiberbezpeka: osvita, nauka, tekhnika*. № 2 (18), S. 150-162. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/411/339

3. Mykytenko T.P. (2024). Virtualni aktyvy v umovakh tsyfrovykh transformatsii ekonomiky. *Vcheni zapysky TNU imeni V. I. Vernadskoho. Seriia: Ekonomika i upravlinnia*. 2024. Tom 35 (74). № 3. S. 14-19.

4. Kolesnikov D. Shcho take kiberbezpeka? [What is cybersecurity?] *BRAINLAB*. 30.08.2024. URL: https://brainlab.com.ua/uk/blog-uk/shho-take-kiberbezpeka

5. Bielkin L.M., Yurynets Yu.L., Bielkin M.L., Kryvolap Ye.V. (2022). Spivvidnoshennia poniat «informatsiina bezpeka», «bezpeka informatsii», «kiberbezpeka» v konteksti bezpekovykh stratehii Ukrainy 2020-2021 rokiv. *Naukovi pratsi Natsionalnoho aviatsiinoho universytetu: Seriia «Iurydychnyi visnyk. Povitriane i kosmichne pravo»*. № 3 (64). S. 78-86.

6. Yurynets Yu.L., Kryvolap Ye.V., Bielkin L.M., Bielkin M.L. (2026). *Zakhyst nadiinosti virtualnykh aktyviv v systemi kiberbezpeky ta kiberzakhystu*. Aktualni pytannia u suchasnii nautsi. № 1 (43). S. 1120-1129.

7. Lubenets S., Harchenko I., Pavlenko Y. (2023). Current problems of international information security. *The Journal of V.N. Karazin Kharkiv National University*. Vol. 17, pp. 42-48.

8. Luidold C., Jungbauer C. (2024). Cybersecurity policy framework requirements for the establishment of highly interoperable and interconnected health data spaces. *Frontiers in Medicine*. 2024. Vol. 11.

9. Yudin O.K., Korchenko O.H., Konakhovych H.F. (2022). Zakhyst informatsii v merezhakh peredachi danykh. K. Vyd-vo TOV «NVP «INTERSERV1S» 2009. 716 s.

10. Parolnyi zakhyst kompiuternoho ta telekomunikatsiinoho obladnannia

(2022). Nauk.-prakt. posib. Avt. kol.: M.H. Verbenskyi, V.O. Kryvolapchuk, D.V. Smernytskyi ta in. Kyiv: «Vydavnytstvo Liudmyla», 2022. 42 s.