Технічні науки

УДК 004.056.5:343.326 (045)

Горліченко Сергій Олександрович

науковий співробітник

Науково-дослідного центру

Інститут спеціального зв'язку та захисту інформації

Національного технічного університету України

"Київський Політехнічний Інститут імені Ігоря Сікорського"

Horlichenko Serhii

Researcher of the

Scientific Research Center

Institute of Special Communication and Information Protection

National Technical University of Ukraine

"Ihor Sikorsky Kyiv Polytechnic Institute"

ОСОБЛИВОСТІ ФОРМУВАННЯ СУЧАСНИХ ДЕФІНІЦІЙ КІБЕРПРОСТОРУ
PECULIARITIES OF FORMING MODERN DEFINITIONS OF CYBERSPACE

Анотація. *На початку дослідження наголошено на тому, що науково-технічна революція початку XXI століття спричинила в усьому світі глибокі системні перетворення, які привели до формування кіберпростору. Перелічено існуючі на даний час головні підходи до трактування поняття «кіберпростір» у поглядах відомих вчених. Приведено найбільш вдале тлумачення даного поняття та вказано недоліки одностороннього його опису. Проаналізовано структурні елементи кіберпростору та сказано, що людина, в силу своїх фізіологічних особливостей поки не може безпосередньо підключитися до*

кіберпростору. Відмічено що національна система кібербезпеки у віртуальному середовищі є сукупністю суб'єктів забезпечення захисту та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру. Названо законодавчі недоліки в описі функціонування сучасного кіберпростору, адже вони повинні врегульовувати основні аспекти спільної діяльності суб'єктів забезпечення кібербезпеки.

Ключові слова: *кібербезпека, інформаційна безпека, кіберзагрози, інформаційно-комунікаційні технології.*

Summary. *At the beginning of the study, it is emphasized that the scientific and technical revolution of the beginning of the 21st century caused profound systemic transformations throughout the world, which led to the formation of cyberspace. The currently existing main approaches to the interpretation of the concept of "cyberspace" in the views of famous scientists are listed. The most successful interpretation of this concept is presented and the shortcomings of its one-sided description are indicated. The structural elements of cyberspace were analyzed and it was said that a person, due to his physiological characteristics, cannot yet directly connect to cyberspace. It is noted that the national system of cyber security in the virtual environment is a set of entities providing protection and interrelated measures of a political, scientific and technical, informational, and educational nature. The legislative shortcomings in the description of the functioning of modern cyberspace are named, because they should regulate the main aspects of the joint activity of the subjects of cyber security.*

Key words: *cyber security, information security, cyber threats, information and communication technologies.*

Вступ. Розвиток цифрової економіки у сучасному світі спрямований на створення та об'єднання комунікативного суспільства, забезпечення

соціального зростання інформаційних платформ та стартапів, прискорення грошових транзакцій, цифровізацію адміністративно-цивільних послуг. Кіберпростір широко визнається як фундаментальний факт повсякденного життя в сучасному світі. Інтернет, як важлива складова сучасного кіберпростору, в своєму розвитку пройшов шлях від професійної сфери спілкування програмістів до сфери вільного спілкування, що реалізує більш широкі в порівнянні з професійними особисті інтереси. Інтернет сьогодні – це не просто мережа взаємопов'язаних комп'ютерів, а спільнота людей, які користуються Інтернетом. У зв'язку з цим в науковій літературі затверджуються різні підходи до трактування поняття «кіберпростір» [2].

Аналіз останніх досліджень і публікацій. Існуючий на даний час кіберпростір та його базова інфраструктура вразливі до широкого спектру ризиків, що виникають від кіберзагроз і небезпек. Наукові праці багатьох дослідників висвітлюють проблематику моніторингу цифрових процесів, виявлення загроз в інформаційній сфері та кібербезпеці, захисту інформаційного простору від кібератак та кібертероризму. Зокрема, цим питанням присвячені праці В. Бурячка, Д. Дубова, М. Ожевана, В. Толубка, В. Хорошка.

Мета дослідження полягає в аналізі сутності поняття «кіберпростір» у поглядах науковців. Узагальненні властивостей сучасного кіберпростору та оцінці його ролі в функціонуванні держави.

Постановка проблеми. Науково-технічна революція початку XXI століття спричинила в усьому світі глибокі системні перетворення. Передусім завдяки поєднанню досягнень у сфері новітніх інформаційно-комунікаційних технологій із надбаннями, що постали на базі стрімкого розвитку інформаційно-телекомунікаційних систем, сформувалися принципово нові глобальні субстанції – інформаційне суспільство, а також інформаційний та кібернетичний простори, які мають практично необмежений потенціал і відіграють провідну роль в економічному та

соціальному розвитку кожної країни світу. Сучасність характеризується глобальною зміною парадигми і становленням інформаційного суспільства, в якому інформація і знання стають основним стратегічним ресурсом. Відзначимо, що протягом останніх тридцяти років феномен кіберпростору став предметом для численних дискусій, а також об'єктом дослідження для гуманітарних і технічних наукових дисциплін.

Виклад основного матеріалу. Питання становлення кіберпростору в якості нового соціального інституту розглядають вітчизняні та зарубіжні дослідники. З огляду на необхідність введення понятійного апарату, слід не забувати про те, що єдиного визначення для кіберпростору не існує. Поняття «кіберпростір» можна розглядати як греко-латинську комбінацію, що складається з двох частин: «кібер-» (cyber -) і «простір» (space). В Оксфордському словнику англійської мови зазначено, що префікс «cyber» буквально перекладається як «правителі». Стародавні греки використовували слово «кібернетика» в прямому сенсі як «мистецтво рульового», а в переносному – як «мистецтво державного управління».

Вперше про кіберпростір написав Вільям Гібсон в «пророчому» оповіданні «спалення Хром», що опубліковане в липневому номері журналу Omni в 1982 р. З поширенням на початку 1990-х рр. інтернету термін «кіберпростір» отримав практичне застосування для опису онлайн світу, в якому взаємодії індивідів і груп здійснюються за допомогою електронних мереж, з'єднаних засобами інформаційно-комунікаційних технологій.

Стець В. під поняттям «кіберпростір» розуміє сукупність взаємопов'язаних інформаційних ресурсів, програмного забезпечення, баз і банків даних, які обробляються у комп'ютерних мережах та у пов'язаній із ними інфраструктурі разом із об'єктами, що підпадають під їхній контроль та управління [9].

Ревак І. О. зазначає, що в понятті «кіберпростір» розуміє середовище існування, що виникло в результаті взаємодії людей, програмного забезпечення і послуг в інтернеті за допомогою технологічних пристроїв і мереж, під'єднаних до них, якого не існує в будь-якій фізичній формі [8]. Капітон А. наголошує, що «кіберпростір» – це сфера, що характеризується можливістю використання електронних та електромагнітних засобів для запам'ятовування, модифікування та обміну даними через мережні системи та пов'язану з ними фізичну інфраструктуру [5].

Відповідно до формулювань Ткача Ю. М., «кіберпростір» – це віртуальний простір, в якому циркулюють електронні дані світових персональних комп'ютерів [11]. У своїх дослідженнях Фролова О. наголошує, що «кіберпростір» – це всі форми мережної, цифрової активності, що включають у себе контент та дії, здійснювані через цифрові мережі [14].

Відповідно до підходів до трактування науковцем Федонюк С., під поняттям «кіберпростір» слід розуміти всю інформаційну інфраструктуру, що доступна через інтернет поза будь-якими територіальними кордонами [13]. З огляду на сказане, а також з урахуванням результатів проведеного багатокритеріального аналізу розумітимемо під кіберпростором віртуальне комунікаційне середовище, утворене системою зв'язків між користувачами та об'єктами інформаційної інфраструктури, такими як електронний інформаційний ресурс, системи й мережі всіх форм власності, керовані автоматизованими системами управління, що використовуються не лише для перетворення та передавання інформації, котра в них циркулює, із метою забезпечення інформаційних потреб суспільства, а й для впливу на аналогічні об'єкти протиборчої сторони (табл. 1).

Інший підхід до визначення пропонує український науковець Заболоцький Т. Він характеризує кіберпростір як середовище, яке створене організованою сукупністю інформаційних процесів на підставі об'єднаних

загальними принципами та правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем незалежно від форми власності [3]. Згідно із ще одним українським дослідником Бурим А. С., «кіберпростір» – інформаційне середовище, що існує за допомогою комп'ютерних систем при взаємодії людей, комп'ютерних систем та при керуванні людьми такими системами [1]. Отож можемо підсумувати, що кіберпростір – це середовище, яке створене та функціонує завдяки комп'ютерним системам і даним з використанням мережі Інтернет, та уможливлює комунікацію і реалізацію суспільних відносин.

Таблиця 1

Аналіз дефініцій поняття «кіберпростір» за базовими критеріями

Походження дефініції чи її автори	Базовий критерій									
	Virt	HF	Soft	PhI	Net	INet	IServ	IRes	MSys	IPr
Стандарт ISOO / IES 27032	+	+	+	+	+	+	+			
Ревак І. О. [8]				+	+			+		+
Стець В. [10]	+							+		
Капітон А. [5]					+			+		+
Фролова О. [14]				+		+				
Федонюк С. [13]	+									+
Бурячок В. Л. [2]	+		+	+	+			+		+
Заболоцький Т. [3]				+	+		+	+	+	+
Бурий А. С. [1]					+			+		+
Пантєлєєва Н. М. [7]								+	+	

Примітка. Для позначення базових критеріїв використано такі ідентифікатори [2]: Virt – критерій віртуальності; HF – критерій урахування людського чинника; Soft – критерій урахування ПЗ; PhI – критерій наявності фізичної інфраструктури; Net – критерій наявності мережної складової; INet – критерій урахування поняття «Інтернету»; IServ – критерій можливості надання інформаційних послуг; IRes – критерій урахування інформаційних ресурсів; MSys – критерій наявності системи управління; IPr – критерій урахування інформаційних процесів.

Мальцева І. Р. вказує, що кіберпростір складається з операцій, взаємин і самої думки, що утворюють подобу хвильового візерунка в мережі наших комунікацій [6].

Якщо звернутися до питання походження терміну «кіберпростір», змістивши акцент з цифрових основ префіксу «cyber-» на основу другої

частини слова «space», то доречним видається тут точка зору Анрі Лефевра, який вважав, що кожне суспільство виробляє свій простір. Мислитель розробив «унітарну теорію простору», що містить три компоненти: фізичний, психічний та соціальний простори.

Згідно досліджень Гафіяка А. в 2019 році в західному дискурсі вже налічувалося близько 28 визначень терміну «кіберпростір». Під кіберпростором він розуміє конкретне місце (точку) з'єднання між комп'ютерами, що перетворилася в глобальне віртуальне співтовариство, а мережа Інтернет переважно визначається з функціональних позицій [15].

Узагальнивши відомі трактування досліджуваного поняття можемо привести його узагальнене тлумачення. Кіберпростір – це принципово новий простір, який не може бути не врегульований нормами права, проте в процесі правозастосування законодавцю необхідно враховувати дискусійні питання застосовності поняття державного суверенітету в ньому, відсутності універсального міжнародного договору, що дозволяє регулювати поведінку держав у кіберпросторі, а також єдиної системи.

Проаналізуємо структурні елементи кіберпростору. Об'єднання елементів кіберпростору дозволяє визначити його фізичну структуру. З функціональної точки зору, елементами кіберпростору, що утворюють його фізичну структуру, є:

- штучне і природне середовище поширення сигналів;
- засоби каналоутворення;
- засоби розподілу ресурсів кіберпростору (маршрутизатори, комутатори);
- засоби вимірювання та збору первинних характеристик елементів кіберпростору та оброблюваного трафіку;
- обчислювальні засоби зберігання та комплексної обробки первинних даних;

– засоби розмежування та захисту інформаційних ресурсів (у тому числі: засоби аутентифікації та ідентифікації);
– засоби управління фрагментами кіберпростору і їх функціями;
– засоби зберігання та обробки інформаційних ресурсів;
– автоматизовані джерела і споживачі інформаційних ресурсів (IoT, АСУ ТП, роботи і т.д.);
– засоби визначення навігаційних даних;
– пристрої комунікаційного сполучення інформаційних потреб людини і можливостей кіберпростору.

Людина, в силу своїх фізіологічних особливостей поки не може безпосередньо підключитися до кіберпростору. Для отримання доступу до ресурсів кіберпростору і задоволення своїх потреб людина змушена використовувати пристрої введення-виведення, які дозволяють перетворити запит людини в коректний для сприйняття кіберпростором, вигляд.

Результатом об'єднання функціональних елементів кіберпростору є реалізація процесів забезпечення інформаційного обміну та формування інформаційних послуг.

До процесів забезпечення інформаційного обміну відносяться: маршрутизація, комутація, обробка даних, каналоутворення, передача даних, зберігання даних, забезпечення безпеки (у тому числі ідентифікація та аутентифікація). Крім цього, об'єднання структурних елементів кіберпростору дозволяє формувати комплексні об'єкти, наприклад лінії і вузли зв'язку [10].

Віртуальна реальність створює штучне середовище. За допомогою засобів віртуальної реальності індивіди занурюються в кіберпростір. На відміну від віртуальної реальності, кіберпростір не заснований на чуттєвому моделюванні з метою створення ілюзії реальності. У кіберпросторі відбувається переважно текстове спілкування, яке

співвідноситься з об'єктивною реальністю, а двозначність терміну «кіберпростір» і накладення кіберпростору на реальне соціальне життя є результатом безпрецедентної кількості соціальних відносин, які породжують сучасні технології.

І, нарешті, слід зазначити, що швидкість розробки, впровадження і повсюдного поширення технологічних новацій в сучасному світі часто створює серйозні перешкоди для здійснення актуального аналізу і спроб прогнозування навіть в перспективі від одного року до трьох років. Те, що ще зовсім недавно сприймалося багатьма дослідниками як навколонаукові міркування письменників-футурологів, сьогодні стало частиною повсякденного життя більшості.

Кіберпростір, або по-іншому цифрове середовище – це простір функціонування продуктів інформаційно-комунікаційних технологій, що дозволяють створювати надзвичайно складні системи взаємодій агентів з метою отримання інформації, обміну та управління нею, а також здійснення комунікацій в умовах безлічі різних мереж. Межі кіберпростору рухливі і мінливі. Кіберпростір розсіяний всюди, і одночасно він не відображений на жодній карті світу. Кіберпростір єдиний і неподільний кордонами національних держав і він являє собою нескінченні можливості для комунікації. Для багатьох дослідників кіберпростір цікавий з точки зору внутрішніх відносин – нові форми соціалізації, а також його співвіднесення з реальним географічним, фізичним простором [12].

Згідно моделі, що була запропонована Кларком (2010), кіберпростір складається з різних рівнів: фізичний, логічний, інформаційний, людський (люди). Дана модель кіберпростору інтегрує два важливих аспекти: технічний і соціальний. Фізичний і логічний рівні пов'язані з технологіями. Фізичний рівень включає матеріальні засоби, що забезпечують стабільну роботу мережі Інтернет, до них відноситься

«залізо» (апаратні засоби) – комп'ютери, дата-центри, сервера, маршрутизатори, дроти. На логічному рівні – це протоколи і програмне забезпечення. У той час як інформаційний (динамічна і статична інформація, включаючи всі види контенту) і людський рівні пов'язані з соціальною сферою. Слід виділити те, що кіберпростір задовольняє одну з основних суспільних потреб – потребу в комунікації. У кіберпросторі формуються нові суспільні взаємини. Люди можуть отримати нові ролі та статуси, відмінні від тих статусів та ролей, які вони мають у реальному житті.

Датські вчені Мортен Хойсгаард та Маргіт Варбург стверджують, що індивідуальні дії людини створюють кіберпростір як нову форму соціального інституту. В даному випадку дослідники дотримуються концепції в якій соціальні інститути розуміються як комплекси дій індивідів. Соціальна спільність кіберпростору є формою суспільного життя людей, що вперше в історії людства носить глобальний, наднаціональний, надкласовий і надполітичний характер. В кіберпросторі можна виділити два базових рівні організації діяльності людини: груповий та індивідуальний. Кіберпростір стає важливим джерелом інформації для людей, прискорюючи інформаційний обмін між індивідами і різними соціальними групами людей.

Міжнародна стратегія для кіберпростору прописує основні принципи, які є дорожньою картою для держав щодо міжнародних зобов'язання в кіберпросторі. Такими нормами є: підтримка основних свобод, тобто свободу вираження поглядів та єднання онлайн так само, як і у фізичному світі; повага до права інтелектуальної власності, зокрема патенти, комерційні таємниці, торгові марки та авторські права; конфіденційність користувачів Інтернету від незаконного втручання держави; державний захист користувачів від злочинності; право на самооборону: відповідно до Статуту Організації Об'єднаних Націй,

держави мають право на захист від будь-яких агресивних дій у кіберпросторі [4].

Характеристики кіберпростору. Визначивши кіберпростір, як нове середовище існування сучасної людини, слід звернутися до ключових його характеристик. Однією з таких характеристик є його віртуальність. Сучасне вживання поняття «віртуальність» все частіше виходить за рамки галузі інформатики та комп'ютерної техніки. У побут увійшли такі, ще до недавнього часу колишні «нереальні» поєднання, як «віртуальна корпорація», «віртуальні гроші», «віртуальна демократія», «віртуальне навчання». Віртуальна реальність, таким чином, стає максимально об'єктивованою, гранично конкретною і відчутною. Це означає, що кіберпростір жорстко не прив'язаний і не залежить від конкретного просторово-часового розташування.

Місце взаємодії в кіберпросторі не вимагає, щоб агенти взаємодії перебували в одному конкретному місці в певний момент часу для того, щоб їх зустріч в кіберпросторі відбулася. Звичайно, взаємодія в кіберпросторі пов'язана з фізичним субстратом, але вона може бути синхронною або асинхронною, і вона може бути доступна агентам практично в будь-якому географічному просторі. Віртуальність тут не виступає протилежністю дійсності, але віртуальність позначає те, що щось в кіберпросторі може бути зовсім не тим, чим здається.

Таким чином, кіберпростір, будучи віртуальним місцем, не є місцем у звичному сенсі, коли місце або простір для взаємодії обмежено просторово-часовими рамками. Іншою важливою характеристикою кіберпростору є зв'язок між кіберпростором та мережею. Кіберпростір не можна ототожнювати з мережею або описувати як сукупність даних, що зберігаються на комп'ютерах, і надаються через комп'ютерні мережі. Однак кіберпростір багато в чому залежить від функціонування інформаційно-комунікаційних мереж (переважно мова йде про інтернет).

Більш конкретно, кіберпростір є місцем або простором, яке контролює існування і роботу взаємопов'язаних мереж комп'ютерів. Отже, будь-яка зміна стану відповідних взаємопов'язаних комп'ютерів, таких як втрата потужності, також буде пов'язана зі зміною взаємодії в кіберпросторі: наприклад, неможливістю взаємодії.

Кіберпростір як простір для взаємодії є ще однією важливою характеристикою віртуального середовища. Прикладами взаємодії в кіберпросторі є: Інтернет-банкінг, геймінг, соціальні мережі, електронні торги, новини, онлайн-шопінг, пошукові системи, електронний уряд, краудсорсинг. Окремо розглянемо таку характерну рису кіберпростору, яка пов'язана з тим, що він не є чітко визначеним і заданим. Мальцева І. Р. в зв'язку з цим наводить порівняння кіберпростору з картою, що має нескінченну безліч входів, яку ніколи неможливо побачити цілком, оскільки вона завжди відкривається лише частково і з будь-якого місця. Ця карта постійно змінюється, що відображає мобільність кіберпростору, а протяжність інтервалів між інформаційними масивами, як правило, невідома. У зв'язку з цим автор описує кіберпростір як гіпертекст або мережу. Гіпертекст нелінійний і містить безліч різнорідних зв'язків, що створює власне сприйняття кіберпростору у кожного агенту, що знаходиться в цифровому середовищі. За аналогією з мережею, кіберпростір в цьому випадку характеризується децентралізацією і розмитістю меж. Ще однією особливістю кіберпростору є можливість розглядати його як приватне, інтимне, або відкрите, публічне. Множинність зв'язків мережевої структури кіберпростору створює нескінченну кількість варіантів індивідуальної репрезентації, а також полів для взаємодій [7].

Конфлікти в кіберпросторі відрізняються за характером від відомих конфліктів у минулому. Як кажуть, кожна епоха має свою власну війну, відповідну рівню технологічного і соціального розвитку суспільства.

Дійсно, це видно по способам ведення війни і в заходах, які вживаються в ході війни. Доступ до інформації, що зберігається, обробляється та передається в кіберпросторі, дає суспільству нову якість життя, зробивши можливими соціальні функції, які були просто мрією та фантазією в не далекому минулому. Це проявляється не тільки в швидкому розвитку суспільства, але має такі важливі економічні виміри, як показує зменшення вартості функціонування суспільства при прискоренні реалізації цього функціонування.

Національна система кібербезпеки у віртуальному середовищі є сукупністю суб'єктів забезпечення захисту та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури.

Створення та впровадження ефективної й результативної національної системи кіберзахисту визначено одним з пріоритетів державної політики національної безпеки України; ці процеси динамічно розгортаються й спрямовані на її адекватне й випереджальне реагування на дедалі вищі виклики та загрози в національному кіберпросторі. Розбудова національної системи кіберзахисту триває від створення незалежної держави Україна, хоча слова «кібербезпека» та «кібертероризм» з'явилися набагато пізніше. До 2006 року, у Законі України «Про основи національної безпеки» в редакції 2003 року, загрозами національним інтересам і національній безпеці України в інформаційній сфері визначено комп'ютерні злочини та комп'ютерний тероризм.

Закон України «Про основні засади забезпечення кібербезпеки України» ухвалено у жовтні 2017 року. Відповідно до Закону про кібербезпеку Державна служба спеціального зв'язку та захисту інформації

України яка один із двох основних суб'єктів забезпечення кібербезпеки (другий – Національна поліція України) підпорядковується Кабінету Міністрів України, забезпечує і виконує низку завдань. На сьогодні це єдиний орган, уповноважений формувати та реалізовувати державну політику у сфері кібербезпеки. Проблемою залишається відсутність нормативно-правової бази, яка врегулювала б основні аспекти спільної діяльності суб'єктів забезпечення кібербезпеки, суб'єктів кіберзахисту та власників (розпорядників) об'єктів критичної інформаційної інфраструктури, алгоритмів інформаційного обміну між ними, послідовності дій і розподілу їхніх функцій задля ефективної взаємодії під час запобігання кібератакам та кіберінцидентам, їх виявлення та припинення, а також під час усунення їх наслідків.

Висновки. В дослідженні проаналізовано підходи науковців до трактування поняття «кіберпростір». Наведено узагальнене тлумачення даного терміну та зроблено його характеристичний опис. Встановлено, що неврегульованими залишаються питання пошуку вразливостей як об'єктів критичної інфраструктури, так і інших інформаційно-телекомунікаційних систем державного і приватного сектора.

Відкрите також і питання врегулювання державно-приватного партнерства, а не взаємодії. Крім того, необхідно закрити ще одну шпарину в нормативно-правовому акті: це законодавство з питань кібербезпеки не вимагає створення та використання інформаційно-аналітичних систем підтримки прийняття управлінських рішень, зокрема в умовах криз та кризового реагування.

Література

1. Бурий А. С., Ловцов Д. А. Перспективи стандартизації інформаційного простору «розумного міста». *Інформаційно-економічні аспекти стандартизації та технічного регулювання.* 2022. № 2 (66). С. 4–11.
2. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник; за заг. ред. професора В. Б. Толубка. К. : ДУТ, 2015. 288 с.
3. Заболоцький Т. Кіберпростір як інструмент соціального впливу на сучасну молодь. *Ввічливість. Humanitas.* 2021. № 1. С. 22–27.
4. Завгородня Ю. В. Кіберпростір як сучасна платформа для вирішення конфліктів. History, political science, philosophy and sociology: european development direction. Riga, Latvia: Baltija Publishing. 2021. С. 53–56.
5. Капітон А. Перспективи розвитку кіберпростору та його соціально-психологічні наслідки. *Системи управління, навігації та зв'язку. Збірник наукових праць*. Полтава : ПНТУ, 2021. Т. 3 (65). С. 89–91. doi: https://doi.org/10.26906/SUNZ. 2021.3.089.
6. Мальцева І. Р. Аналіз деяких кіберзагроз в умовах війни. *Кібербезпека: освіта, наука, техніка.* 2022. № 4(16). С. 37–43. doi: 10.28925/2663–4023.2022.16.3744.
7. Пантєлєєва Н. М. Кіберзагрози в умовах цифрової економіки. *Фінансовий простір.* 2019. № 1. С. 130–139.
8. Ревак І. О. Особливості формування безпечного кіберпростору в умовах розвитку цифрової економіки. *Інформаційні технології та економічна безпека.* 2021. № 3–4. С. 164–169.
9. Стець В. Кіберпростір як об'єкт публічного управління в сфері забезпечення кібербезпеки. *Публічне управління: традиції, інновації, глобальні тренди: матеріали Всеукраїнської наук.-практ. конф. за міжнар. участю*. Одеса : ОРІДУ НАДУ, 2021. С. 290–292.

10. Стець В. В. Ккіберпростір як основний об'єкт публічного управління у сфері забезпечення кібербезпеки. *Наукові перспективи.* 2022. № 8(26). С. 98–115.
11. Ткач Ю. Концептуальна модель безпеки кіберпростору. *Технічні науки та технології.* 2021. № 4(22). С. 96–108. doi: https://doi.org/10.25140/2411-5363-2020-4(22)-96-108.
12. Ткач Ю. М. Тенденції розвитку сучасного кіберпростору та його захищеності в умовах інформаційного протиборства. *Безпека інформації.* 2020. Т. 26 (2). С. 74–80.
13. Федонюк С. Міжнародні аспекти безпеки кіберпростору. Луцьк : Вежа-Друк, 2022. 178 с.
14. Фролова О. Міжнародне співробітництво в галузі забезпечення інформаційної безпеки. *Вісник Львівського університету. Серія: Міжнародні відносини*. 2019. Вип. 46. С. 123–136.
15. Hafiiak A. Problems of professional competence of future specialists on information and communication technologies in universities. *Series: Education and Pedagogy*. 2019. № 10 (2). С. 15–18.

References

1. Burij A. S., Lovcov D. A. (2022). Perspektivi standartizaciyi informacijnogo prostoru «rozumnogo mista». *Informacijno-ekonomichni aspekti standartizaciyi ta tehnichnogo regulyuvannya.* № 2 (66). S. 4–11.
2. Buryachok V. L. (2015). Informacijna ta kiberbezpeka: sociotehnichnij aspekt: pidruchnik; za zag. red. profesora V. B. Tolubka. K. : DUT. 288 s.
3. Zabolockij T. (2021). Kiberprostir yak instrument socialnogo vplivu na suchasnu molod. *Vvichlivist. Humanitas*. № 1. S. 22–27.
4. Zavgorodnya Yu. V. (2021). Kiberprostir yak suchasna platforma dlya virishennya konfliktiv. History, political science, philosophy and

sociology: european development direction. Riga, Latvia : Baltija Publishing. S. 53–56.

5. Kapiton A. (2021). Perspektivi rozvitku kiberprostoru ta jogo socialno-psihologichni naslidki. Sistemi upravlinnya, navigaciyi ta zv'yazku. *Zbirnik naukovih prac*. Poltava : PNTU. T. 3 (65). S. 89–91. doi: https://doi.org/10.26906/SUNZ. 2021.3.089.
6. Malceva I. R. (2022). Analiz deyakih kiberzagroz v umovah vijni. *Kiberbezpeka: osvita, nauka, tehnika*. № 4 (16). S. 37–43. doi: 10.28925/2663–4023.2022.16.3744.
7. Pantyelyeyeva N. M. (2019). Kiberzagrozi v umovah cifrovoyi ekonomiki. *Finansovij prostir.* № 1. S. 130–139.
8. Revak I. O. (2021). Osoblivosti formuvannya bezpechnogo kiberprostoru v umovah rozvitku cifrovoyi ekonomiki. *Informacijni tehnologiyi ta ekonomichna bezpeka.* № 3–4. S. 164–169.
9. Stec V. (2021). Kiberprostir yak ob'yekt publichnogo upravlinnya v sferi zabezpechennya kiberbezpeki. *Publichne upravlinnya: tradiciyi, innovaciyi, globalni trendi: materiali Vseukrayinskoyi nauk. – prakt. konf. za mizhnar. uchastyu*. Odesa : ORIDU NADU. S. 290–292.
10. Stec V. V. (2022). Kkiberprostir yak osnovnij ob'yekt publichnogo upravlinnya u sferi zabezpechennya kiberbezpeki. *Naukovi perspektivi.* № 8 (26). S. 98–115.
11. Tkach Yu. (2022). Konceptualna model bezpeki kiberprostoru. *Tehnichni nauki ta tehnologiyi.* № 4 (22). S. 96–108. doi: https://doi.org/10.25140/2411-5363-2020-4(22)-96-108.
12. Tkach Yu. M. (2020). Tendenciyi rozvitku suchasnogo kiberprostoru ta jogo zahishenosti v umovah informacijnogo protiborstva. *Bezpeka informaciyi*. T. 26 (2). S. 74–80.
13. Fedonyuk S. (2022). Mizhnarodni aspekti bezpeki kiberprostoru. Luck: Vezha-Druk. 178 s.

14. Frolova O. (2019). Mizhnarodne spivrobitnictvo v galuzi zabezpechennya informacijnoyi bezpeki. *Visnik Lvivskogo universitetu. Seriya: Mizhnarodni vidnosini.* Vyp. 46. S. 123–136.
15. Hafiiak A. (2019). Problems of professional competence of future specialists on information and communication technologies in universities. *Series: Education and Pedagogy*. № 10 (2). S. 15–18.