DOI 10.20535/2411-1031.2023.11.1.283710
УДК 004.056.53

ВІКТОР ГОРЛИНСЬКИЙ,
БОРИС ГОРЛИНСЬКИЙ

КОНСТИТУЮВАННЯ НАЦІОНАЛЬНОГО КІБЕРПРОСТОРУ ТА ЙОГО ОСВІТНЯ ЗНАЧУЩІСТЬ ДЛЯ ФАХІВЦІВ В ГАЛУЗІ КІБЕРБЕЗПЕКИ

Показано, що в умовах ескалації воєнної експансії російської федерації, яка супроводжується перенесенням бойових дій у кіберпростір, питання його надійного захисту з боку держави, стає чинником її виживання і вимагає наукового аналізу його змісту. Уточнено сутність національного кіберпростору як цифрового комунікативного середовища на функціонування якого поширюється юрисдикція держави. Визначено ознаки відокремлення національного кіберпростору від глобального інформаційного, а саме: способи захисту, засоби організації та контролю кіберпростору, які ґрунтуються на національній системі права; юридична відповідальність суб'єктів за організацію технічного і криптографічного захисту інформації та інформаційно-комунікаційних систем на національних правових засадах; застосування національних телекомунікаційних систем і електронних засобів зв'язку, на які розповсюджується юрисдикція держави; державна значущість інформації, яка підлягає криптографічному і технічному захисту, систем електронних комунікацій, управління технологічними процесами, електронних інформаційних ресурсів, що обробляються в комунікаційних та технологічних системах національного призначення. Розкрито структурний зміст національного кіберпростору, якій складається внаслідок інституалізації взаємозалежних підструктур і сегментів, утворюючих цифрове комунікативне середовище і визначаючих його усталене функціонування на національних засадах як складової глобального інформаційного простору, а саме: функціональна підструктура; інформаційно-телекомунікаційна інфраструктура; національна система кібербезпеки; організаційно-управлінська підструктура; освітня та науково-дослідна підструктури, соціальне, психологічне і культурне середовище. Показано, що значущість знання про системний характер національного кіберпростору у підготовці кадрів в галузі кібербезпеки визначається: роллю професійних і соціальних компетентностей в практичній діяльності фахівців; системним характером професійної діяльності із забезпечення захисту національного кіберпростору; освітньою роллю знання про кіберпростір та використанням його можливостей у сфері електронної освіти, дистанційного навчання і самостійного набуття знань в галузі, особливо в умовах воєнного стану.

Ключові слова: національна безпека, кібербезпека, глобальний інформаційний простір, структура національного кіберпростору, підготовка фахівців.

Постановка проблеми. Аналіз воєнно-політичних, соціальних і економічних подій, що відбуваються в державі і навколо України, з використанням можливостей та інструментів глобального кіберпростору свідчить, що ефективність, сталість і захищеність державного кіберпростору є важливим чинником надійного забезпечення національної безпеки [1]. В умовах воєнно-політичної експансії російської федерації, розв'язання проблеми вдосконалення національної системи кібербезпеки і забезпечення надійного захисту національного кіберпростору, постає найактуальнішим питанням теорії і практики забезпечення національної безпеки України [1], [2]. У зв'язку з розвитком галузі кібербезпеки, формуванням нової нормативної бази стандартів, виникає низка наукових завдань, спрямованих на аналіз і уточнення знань про змістовний бік кіберпростору як умови його надійного захисту. Одним з ключових чинників розв'язання цієї проблеми є визначення

можливостей держави щодо ефективного управління і контролю функціонування структурних елементів і сегментів національного кіберпростору. Але питання управління, контрольованості та надійного захисту національного кіберпростору багато в чому залежить від адекватного розуміння його конституювання як процесу становлення і формування структурних і функціональних параметрів в межах глобального інформаційного простору та впровадження знань про структурний зміст національного кіберпростору в систему підготовки фахівців в галузі кібербезпеки.

Аналіз останніх досліджень і публікацій. Значущість надійного захисту кіберпростору у забезпеченні національної безпеки обґрунтовано у працях [2] - [12]. Безпосередньо, завдання методології конституювання кіберпростору вирішувалось в роботах [3] - [6], [33]. Питання щодо знань фахівців в галузі кібербезпеки розкриті в [9], [12], [13]. Але проблематика щодо відповідності поглядів на зміст кіберпростору вимогам швидкоплинного техніко-технологічного розвитку потребує більш глибокого і системного вивчення. Актуальним питанням зберігається розроблення і обґрунтування теоретичних положень побудови кіберпростору як визначальних вимог щодо його надійного захисту та їх подальшого впровадження в систему підготовки фахівців. Розв’язання поставленої проблеми, в першу чергу, потребує з’ясування теоретичних засад її розроблення на підставі аналізу чинників конституювання національного кіберпростору.

Метою статті є визначення і обґрунтування ключових факторів конституювання національного кіберпростору і ознак його розмежування з глобальним, як теоретичного підґрунтя визначення системних засад його структурування, управління, контрольованості, захисту та з’ясування освітньої значущості здобутих знань для фахівців в галузі кібербезпеки.

Виклад основного матеріалу дослідження. Глобалізація кіберпростору, яка проявляється у перерозподілі сфер впливу між світовими центрами сили, його використанні терористичними організаціями, подоланні національних кордонів кіберзлочинністю, перетворенні кіберпростору на театр воєнних дій, зростанні інтенсивності міждержавного протиборства і перенесення “гібридних війн” у кіберпростір, виникненні нових кіберзагроз, свідчить про підвищення його ролі у забезпеченні національної безпеки України [1]. Питання побудови усталеної системи захисту національного кіберпростору, особливо в умовах війни, стає чинником виживання держави [1], [4], [5]. Але ключовим фактором забезпечення кібербезпеки зберігається контрольованість процесів, що відбуваються в національному кіберпросторі, остаточне визначення яких, відповідно до вимог техніко-технологічного розвитку, потребує обґрунтування теоретичних засад, що зумовлюють його конституювання і структурування.

Процес формування структурно-функціональних параметрів, організаційна і правова інституалізація національного кіберпростору в межах глобального, описується на підставі аналізу і узагальнення факторів його конституювання як системного утворення.

Висвітлюючи генезис поняття “кіберпростір”, необхідно зауважити, що вперше воно було застосовано у значенні “надпростору”, з’явилося ще до появи Інтернету наприкінці 1960-х років у словосполученні “Ательє Кіберпростір” (Atelier Cyberspace) як виду образотворчого просторового мистецтва – інсталяцій, завдяки творчості Сюзанни Уссінг і Карстена Хоффа. Але введення у вжиток поняття кіберпростору, що безпосередньо пов’язано з комп’ютерними мережами, приписується Вільяму Гібсону, завдяки новелі “Спалити Chrome” (Burning Chrome) (1982), в якої кіберпростір ототожнювався з пам’яттю всього людства, що зберігається в комп’ютерних мережах як “масові галюцинації консенсусу”. Подальший розвиток це поняття набуло в маніфесті Джона Перрі Барлоу та Мітчелла Капора “Перетинаючи електронні кордони” (1990), де було відзначено інтерактивну компоненту кіберпростору.

Проте формальною підставою конституювання кіберпростору, як системного утворення світового масштабу, вважають офіційне застосування терміну “кіберпростір” в Окінавській Хартії глобального інформаційного суспільства (2000), в якій зазначено необхідність

спрямування зусиль міжнародного співтовариства на розвиток глобального інформаційного суспільства і забезпечення безпечного та вільного від злочинності кіберпростору [15].

Необхідність з'ясування сутності національного кіберпростору та уточнення його реальних кордонів, потребує звернення до сенсу, що розкривається на підставі семантичного або смислового аналізу поняття "кіберпростір". Необхідно враховувати, що розуміння цієї категорії утворюються на підставі поєднання смислів понять "кібернетика" і "простір", що породжує певну термінологічну невизначеність та може впливати на можливості організації його контролювання. Подвійний смисл терміну "кібернетика" зумовлюється різними підходами до розуміння природи походження управляючої системи, які не відрізняють технічні та електронні системи управління від соціальних і власно природничих систем, що створює труднощі у відокремленні функцій кібербезпеки від інформаційної безпеки [8]. З метою розв'язання цього питання у дослідженнях пропонується підхід, згідно з яким, поняття інформаційного простору в широкому сенсі розуміється як сфера функціонування будь яких інформаційних систем, зокрема кібернетичних. Тоді як кіберпростір, є більш вузькім поняттям, – сферою функціонування лише кіберсистем як електронних систем управління і комунікацій [8].

Інша складова словосполучення "кіберпростір", а саме – "простір", також містить багато вимірів, що впливають на його конституювання [4]. Поряд з фізичним виміром, що характеризується фізичною тримірністю та пов'язаний з часовим виміром, простір, як форма буття та взаємної координації предметів і явищ, може описуватись ознаками віртуального, інформаційного, соціокультурного, технологічного, географічного, геополітичного, правового, соціально-економічного, воєнно-політичного і антропологічного вимірів, які підкреслюють різні аспекти взаємодії, архітектоніку, взаємного розташування його фізичних і віртуальних компонентів. Саме тому, дослідниками пропонується різноманітні варіанти розуміння кіберпростору, що гуртуються на його розумінні як *середовища, що охоплює область взаємовпливу елементів кіберсистеми та її соціальних складових*, яке не виключає інших ознак, що розширюють його зміст та характеризують їх прояв у кожній конкретній підструктурі або сегменті національного кіберпростору [5].

Але, двозначність сутності кіберпростору, як єдності фізичного і віртуального середовища та труднощі окреслення останнього, фундують питання необхідності *визначення реальних кордонів національного кіберпростору* [5]. Віртуальний вимір кіберпростору зумовлюється можливістю створення у свідомості людини віртуальної реальності з допомогою інформаційних технологій, технічного та програмного забезпечення, як єдності суб'єктивних і об'єктивних властивостей. Така амбівалентність властивостей кіберпростору не виключає можливість прихованого цілеспрямованого і деструктивного впливу на свідомість і психіку людини. Врахування цього чиннику потребує уточнення і додержання певних правових, технічних, санітарних і соціальних стандартів, що визначають безпечні для психіки людини, параметри функціонування технічних засобів телекомунікацій та зв'язку, а також виключають можливості деструктивного впливу змістовного боку інформації на колективну свідомість громадян. Отже, кордони віртуального виміру національного кіберпростору в границях глобального інформаційного, набувають реальності як межі аудиторії громадян, на свідомість яких розраховано вплив інформації або спеціальних технічних засобів, що вимагає державного контролювання інформаційних потоків в контексті захисту національних інтересів. Водночас, "кіберпростір є надзвичайно фізичним середовищем: він створений абсолютно фізичними мережами та системами, поєднаними між собою та підпорядкованими певним правилам, вираженим через програмне забезпечення та комунікативні протоколи" [16].

Питання визначення реальних кордонів національного кіберпростору пов'язане також з поглядами на неприпустимість обмеження глобального кіберпростору національними рамками, згідно з базовими принципами інформаційного суспільства. Так, Окінавська Хартія глобального інформаційного суспільства, прийнята лідерами "сімки" найбільш розвинених

держав світу в Окінаві 22 липня 2000 року, проголошує можливість вільного обміну інформацією і знаннями, толерантність і повагу до особливостей інших людей [15].

Неприпустимість обмежень глобального кіберпростору втручанням держави проголошується, також у Декларації незалежності кіберпростору, що оприлюднена в 1996 році Джоном Перрі Барлоу, засновником Фонду електронних кордонів, (Electronic Frontier Foundation). Основою кіберпростору декларацією проголошується його екстериторіальність та не підвладність державній юрисдикції [17]. "Загальна декларація прав людини", що прийнята Генеральною Асамблеєю ООН 10 грудня 1948 року у 19 статті, також проголошує право особи на "свободу шукати, отримувати і розповсюджувати інформацію та ідеї будь якими засобами і незалежно від державних кордонів" [18].

Враховуючи наведені положення, а також тенденцію застосування у наукових працях і нормативних документах, понять "інформаційний простір", "глобальній інформаційний простір" і "кіберпростір", "національний кіберпростір" без з'ясування їх змістовної основи [3], доцільно виявити *місце національного кіберпростору в структурі глобального інформаційного простору, уточнити його сутність і структурний зміст*.

Аналіз і узагальнення різноманітних варіантів визначення кіберпростору, що пропонуються в дослідженнях, дозволяє уточнити сутність цього поняття як *цифрового соціально-технічного комунікативного середовища*. Але змістовним визначенням, що розкриває соціальну і технологічну сторони комунікативного середовища і застосовується як технічний стандарт в країнах Європейському Союзу і НАТО є дефініція кіберпростору як "середовища існування, отриманого в результаті взаємодії людей, програмного забезпечення і послуг в Інтернет за допомогою технологічних пристроїв і мереж, підключених до них, яке не існує у будь-якій фізичній формі" [19]. В даному визначенні, поряд з техніко-технологічною, підкреслено соціальну і віртуальну ознаки кіберпростору та його соціально-часовий вимір. З погляду на сферу охоплення, це визначення можна розглядати як таке, що стосується, перш за все, *глобального виміру кіберпростору*.

Більш широким, що містить соціальну мету і прийнятим до застосування в правовому полі нашої держави як стандарту, вважається визначення, що міститься в Законі України "Про основні засади кібербезпеки України". "Кіберпростір – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних" [14]. Парадоксально, але поняття кіберпростору, наведене у Законі, спрямованому на забезпечення захисту саме національних інтересів України у кіберпросторі, не відокремлюється певними ознаками від глобального кіберпростору. Постає питання відповідності контролюючих і безпекових функцій держави, щодо глобальних, суспільних, недержавних інформаційних і комунікаційних систем. Вивчення джерел [14], [23] [24], дозволяє такими ознаками національного кіберпростору вважати державну юрисдикцію і приналежність (форми власності) засобів організації кіберпростору державним інституціям, підконтрольність не державних і суспільних юридичних суб'єктів державним органам влади.

З погляду на сферу охоплення, поняття кіберпростору, наведене у Законі, також не містить ознак, що відокремлюють його від області функціонування засобів масової інформації та публічної інформаційної сфери з використанням Інтернету, тобто стає ідентичним розумінню інформаційного простору. Адже змістовна характеристика інформаційного простору держави містить сегменти, що охоплюють сфери позитивного іміджу держави на міжнародному рівні, інформаційних прав і свобод її громадян, інформаційного суверенітету, інформаційно-психологічного протиборства, здійснення правоохоронної та контррозвідувальної діяльності з цих питань [12]. Отже, поняття кіберпростору, за ознаками, наведеними у Законі, не дає можливості чітко відокремити його від глобального інформаційного, саме тому, що інформаційний простір не виключає функціонування телекомунікацій та Інтернету. Розв'язання цього питання стає можливим за умови введення

таких ознак кіберпростору, як *способи його захисту* – криптографічний, технічний та *засоби організації та контролю*, а саме техніко-технологічний, програмний, нормативний та організаційний, на відміну від суто правового, соціального, психологічного та ідеологічного, властивих інформаційному простору.

В контексті з'ясування меж національного кіберпростору в границях інформаційного простору, суттєвим може бути акцентуація *системоутворювальної ознаки*, навколо якої відбувається процес його конституювання. Для національного кіберпростору такою ознакою можна вважати використання *національних телекомунікаційних мереж та електронних комунікацій* [14], тоді як для інформаційного простору – це, перш за все, інформація і національні інформаційні ресурси.

Не менш важливою ознакою для з'ясування абрису національного кіберпростору в межах інформаційного є визначення *об'єкта і предмета захисту*, стосовно яких, конституюється той чи інший вимір кіберпростору. З погляду на предмет захисту, в межах загального об'єкту забезпечення інформаційної безпеки – інтересів людини, суспільства і держави, в наукових працях, в одному випадку, пропонується розглядати предметом захисту інформаційні ресурси і телекомунікаційні системи держави, що характерно для кібербезпеки, в іншому, – індивідуальну, суспільну, національну свідомість та інтереси громадян, що властиво інформаційній безпеці [8]. Отже, з погляду на *об'єкт кіберзахисту*, національний кіберпростір утворюється *навколо інформації, що має державну значущість і підлягає криптографічному і технічному захисту, системи електронних комунікацій, системи управління технологічними процесами, електронні інформаційні ресурси, що обробляються (передаються, зберігаються) в комунікаційних та технологічних системах* [14]. Тоді як національний інформаційний простір, поряд з функцією захисту інформації у телекомунікаційних системах, містить функцію захисту взагалі всіх інформаційних ресурсів держави, життєво важливих інформаційних інтересів людини і суспільства, а в контексті впливу інформації та інформаційних технологій на людину, – *колективну та індивідуальну свідомість*.

Іншою ознакою відокремлення національного кіберпростору від інформаційного, може бути визнано сфери *відповідальності* структур, що організують і контролюють національний кіберпростір, відповідно до завдань і функціональних обов'язків. Мається на увазі відокремлення правової та адміністративної відповідальності державних структур за технічний і криптографічний захист інформації та інформаційно-комунікаційних систем, від юридичної відповідальності за деструктивний вплив інформації, що розповсюджується в інформаційному просторі, на колективну свідомість громадян.

Змістовним документом, з огляду на запропоновані новації з забезпечення захисту національного кіберпростору, стала Стратегія кібербезпеки України (2021-2025 роки) "Безпечний кіберпростір – запорука успішного розвитку країни" (далі – Стратегія), у якій на засадах стримування, кіберстійкості та взаємодії, ґрунтовно окреслено коло умов для безпечного функціонування кіберпростору України на 2021-2025 роки [1]. У Стратегії оприлюднено коло теоретичних і практичних питань, вивчення яких, майбутніми фахівцями кібербезпеки, буде сприяти опануванню базовими засадами її організації. Але, нажаль, поряд з багаторазовим застосуванням поняття *"національний кіберпростір",* документ не містить його конкретного визначення.

Проте, з погляду на констатацію чинників забезпечення захисту національного кіберпростору, однією з принципових вимог Стратегії, є необхідність врахування шостого технологічного укладу, що характеризується тенденцією конвергенції біо-, нано-, інфо-, когнотехнологій з технологіями штучного інтелекту та характеризується ризиками, з якими стикається цивілізація внаслідок їх провадження і використання у кіберпросторі [1]. Синергетична взаємодія нанонаук, генної інженерії, інформаційних і новітніх гуманітарних технологій, на думку науковців, все більш радикально змінює людину, трансформуючи її власно людську природу [20]. Значущість контролювання і захисту кіберпростору

посилюється завдяки поєднанню сучасних інформаційних і мережевих технологій з гуманітарними технологіями, спрямованими на маніпулювання колективною свідомістю [21], кіберризиками, породженими поєднанням виробничого і мережевого середовищ шляхом використання кіберфізичних виробничих систем [22]. *Проблема поєднання інформаційних і новітніх гуманітарних технологій, труднощі у визначені кордонів національного кіберпростору в межах глобального, розвиток інформаційних технологій, потребує врахування небезпечного впливу його віртуальної складової на свідомість людини, та опанування майбутніми фахівцями теоретичними і соціально-психологічними засадами захисту власної свідомості та психіки.*

На погляд авторів, іншими факторами, що потребують врахування у дослідженні питання конституювання національного кіберпростору є такі: системний характер процесів, що розгортаються в сучасному глобальному кіберпросторі, його конкретних секторах і національному рівні в умовах воєнної агресії російської федерації; складність практичного розмежування процесів, які відбуваються на глобальному і національному рівнях функціонування кіберпростору та контролювання інформаційних потоків з метою захисту національних інтересів; концептуальні зміни у підходах до розуміння змісту кібербезпеки і розширення функцій; швидкий розвиток інформаційних технологій та їх перехід на квантову основу, що потребує врахування завдань з кіберзахисту у перехідний та постквантовий періоди; загрози, що виникають із конвергенції інформаційно-комунікаційних технологій з новітніми високими технологіями; необхідність оперативного і ефективного реагування на кібератаки, спрямовані на державні установи і структури національної безпеки; спроби деструктивного інформаційно-психологічного впливу на особовий склад сектору безпеки і оборони; курс України на євроатлантичну інтеграцію, узгодження національної системи стандартів у кібербезпеці з стандартами НАТО і формування нової нормативної бази; вступ людства в період підвищеного соціального, екологічного і технологічного ризиків; підвищення ризикогенності професійної діяльності військовослужбовців в умовах бойових дій; виклики ґендерної політики щодо досягнення ґендерної рівності у сфері безпеки і оборони України в умовах воєнного часу і міжнародні вимоги до гендерної політики держави, стосовно гендерного інтегрування [9]. Наведений перелік актуальних чинників зосереджує увагу на ключових моментах сьогодення, що впливають на конституювання національного кіберпростору і потребують врахування при внесенні змін в систему освітніх компетентностей фахівців з кібербезпеки.

Узагальнюючи наведені міркування, доцільно підкреслити, що умовна лінія відокремлення національного кіберпростору в структурі глобального інформаційного середовища визначається за такими ознаками: способи захисту кіберпростору – криптографічний, технічний та засоби організації та контролю кіберпростору, а саме організаційний, техніко-технологічний і нормативний, організація яких ґрунтується на національній системі нормативно-правових актів; види юридичної відповідальності суб'єктів за організацію технічного і криптографічного захисту інформації та інформаційно-комунікаційних систем; застосування національних інформаційно-комунікаційних систем і електронних засобів зв'язку, на які розповсюджується юрисдикція держави; державна значущість інформації, яка підлягає криптографічному і технічному захисту, систем електронних комунікацій, управління технологічними процесами, електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та технологічних системах національного, або державного призначення.

Проведений аналіз дозволяє конкретизувати сутність і сформулювати визначення національного кіберпростору. *За своєю сутністю, національний кіберпростір являє собою цифрове комунікативне середовище на функціонування якого поширюється юрисдикція держави.* Поглиблюючи зміст наведеної дефініції і спираючись на дефініції кіберпростору [14], [33], можна сформулювати наступне уточнене визначення: *національний кіберпростір це середовище функціонування електронних комунікаційних мереж державної форми власності*

та/або інших форм власності, підконтрольних державним органам влади, із застосуванням національних електронних інформаційних ресурсів з метою забезпечення інформаційно-комунікаційних і управлінських інтересів людини, суспільства і держави, національних інтересів України у кіберпросторі.

Обґрунтування меж і уточнення сутності національного кіберпростору, дозволяє перейти до розкриття змістовного боку його конституювання – *формування структурно-функціональних і організаційних параметрів*. Процес конституювання національного кіберпростору доцільно розкривати, спираючись, по-перше, на загальнонаукове розуміння простору як форми взаємної координації предметів і явищ, що існує в нерозривній єдності з часом як універсальна, цілісна форма організації та координації буття, по-друге, враховуючи теоретичне положення про те, що кожен фрагмент світу має свій власний час і простір, які й творять його якісну специфіку. На підставі положень теорії структурно-функціонального аналізу можна стверджувати, що в основі процесу конституювання національного кіберпростору, лежить утворення функціональної підструктури, на ґрунті якої відбудовується змістовна і організаційно-управлінська підструктури, супроводжуючись соціальною і правовою інституалізацією на національних правових засадах.

Формування онтологічної або сутнісної структури кіберпростору, в єдності віртуального, соціального і фізичного вимірів, визначається сукупністю предметів, явищ і процесів, що утворюють цифрове комунікативне середовище та складається з певних взаємодіючих і взаємозалежних підструктур і сегментів які визначають його усталене функціонування на системних засадах. На переконання дослідників, кіберпростір, як середовище існування процесів функціонування інформаційно-телекомунікаційних систем, опосередковано визначається через її характеристики як складної динамічної системи, а саме через структурні, функціональні, часові, інформаційні, характеристики надійності, енергетичні характеристики, характеристики видів забезпечення інформаційних систем [3]. Виходячи з офіційного визначення, наведеного у Законі [14], можна відокремити низку базових підструктурних компонентів, що утворюють *сутнісну структуру національного кіберпростору*. Ними є: власно середовище в єдності віртуального, соціального і фізичного (просторово-часового) вимірів; здійснення комунікацій як атрибутивний процесуальний вимір; реалізація суспільних відносин – соціальний цільовий вимір; сумісні комунікаційні системи і мережі Інтернет та інші глобальні мережі передачі даних, які утворюють техніко-технологічний – базовий вимір національного кіберпростору та його головну особливість, що локалізує його функціонування в межах глобального інформаційного простору.

Необхідно відзначити, що системоутворювальною підструктурою національного кіберпростору, є *функціональна підструктура*, яка формується згідно з базовими функціями, що визначають сутнісні, атрибутивні ознаки національного кіберпростору. Такою визначальною атрибутивною функцією є здійснення комунікацій в національних інтересах. Але реалізація цієї функції може ефективно здійснюватися внаслідок взаємодії функцій організації, регулювання, координації, контролю і захисту комунікаційних процесів та інформаційних потоків у кіберпросторі в інтересах держави, суспільства і громадян [1]. До процесів, що структурують функціональну підструктуру, забезпечують інформаційний обмін відносяться: маршрутизація, комутація, обробка даних, каналоутворення, передача даних, збереження даних, забезпечення захисту і безпеки (ідентифікація, аутентифікація) тощо. Але з погляду на об’єктивні обставини воєнного часу і загальну спрямованість даної роботи, необхідно зазначити, що суттєвою функцією національного кіберпростору зберігається захист об’єктів критичної інформаційної інфраструктури, яка визначається як організаційні, нормативно-правові, інженерно-технічні та інші заходи, спрямовані на забезпечення безпеки об’єктів критичної інформаційної інфраструктури [25]. Функціями, що спрямовані на здобуття наукових знань і забезпечення підготовки національних кадрів в галузі кібербезпеки, є науково-дослідна і освітня функції. Професійне вдосконалення, кіберобізнане суспільство та

науково-технічне забезпечення кібербезпеки відзначено в Стратегії кібербезпеки України однією з стратегічних цілей [1].

Змістовною складовою національного кіберпростору, що організується відповідно до функціональної структури, є *інформаційно-телекомунікаційна інфраструктура* як середовище, що забезпечує технічну можливість збору, зберігання, передавання, автоматизованої обробки та поширення інформації на підставі використання національних електронних інформаційних ресурсів, розподілених по WEB-сайтам у мережі Internet. Її зміст складають національні *інформаційні комунікаційні системи* [26] Згідно з напрямами розвитку електронного урядування в Україні, відокремлюють інформаційні комунікаційні системи підтримки прийняття управлінських рішень та автоматизації адміністративних процесів у сферах: охорони здоров'я; екології та природних ресурсів; освіти і науки; соціального захисту; фінансової та бюджетної політики; охорони прав і свобод людини; транспорту та інфраструктури; регіонального розвитку та реформування місцевого самоврядування і територіальної організації влади; у виборчій і архівній сферах. [27]. Поряд із зазначеним, до складових національної інформаційної комунікаційної системи відносять такі підсистеми: формування та забезпечення зберігання інформаційних ресурсів; забезпечення доступу до інформаційних комунікаційних систем, систем зв'язку та електронних інформаційних ресурсів; інформаційних послуг та національного інформаційного ринку.

Важливими компонентами національної інформаційної комунікаційної інфраструктури, поряд з національною інформаційною комунікаційною системою, є *національна телекомунікаційна мережа*, що являє собою сукупність спеціальних телекомунікаційних систем (мереж), систем спеціального зв'язку, інших комунікаційних систем, які використовуються в інтересах органів державної влади [14] та *національні електронні інформаційні ресурси* – систематизовані електронні інформаційні ресурси, які містять інформацію незалежно від виду, змісту, форми, часу і місця її створення (включаючи публічну інформацію, державні інформаційні ресурси та іншу інформацію), призначену для задоволення життєво важливих суспільних потреб громадянина, особи, суспільства і держави. Під електронними інформаційними ресурсами розуміється будь-яка інформація, що створена, записана, оброблена або збережена у цифровій чи іншій нематеріальній формі за допомогою електронних, магнітних, електромагнітних, оптичних, технічних, програмних або інших засобів [14], [28]. Зміст національних електронних інформаційних ресурсів визначено у Положенні про Національний реєстр електронних інформаційних ресурсів, а саме: кадастри, державні та інші обов'язкові класифікатори, а також інформаційні системи, які забезпечують їх функціонування та використовують інформацію з них [31]. Національні електронні інформаційні ресурси можуть бути державними та недержавними та знаходитися у власності громадян, органів державної влади, органів місцевого самоврядування, підприємств, організацій, установ та громадських об'єднань, але їхньою провідною ознакою має бути національна юрисдикція.

Сегментом попередньо визначеної інформаційної комунікаційної інфраструктури є *критична інформаційна інфраструктура*, яку утворює сукупність об'єктів критичної інформаційної інфраструктури. Сутнісною ознакою об'єктів критичної інформаційної інфраструктури є надання послуг, згідно з Постановою КМУ, вважаються збої та переривання у наданні (виконанні) яких призводять до негативних наслідків для населення, суспільства, соціально-економічного стану та національної безпеки і оборони України [25].

Треба зауважити, що окремою підструктурою національного кіберпростору, що утворюється на підставі життєво важливої функції і визначає його устелене і надійне функціонування в інтересах національної безпеки, постає *національна система кібербезпеки* як сукупність суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних

інформаційних ресурсів, кіберзахисту об’єктів критичної інформаційної інфраструктури [14]. Засади розбудови національної системи кібербезпеки докладно конкретизовано в Стратегії кібербезпеки України [1].

На підставі попередньо визначених змістовних складових, формується *організаційно-управлінська підструктура національного кіберпростору*, як організаційно поєднана, системою організаційних, управлінських, функціональних, просторово-часових зав’язків, сукупність органів, процедур, організаційно-правових засад, що дозволяють регулювати, координувати і контролювати і забезпечувати функціонування, безпеку і захист процесів, що відбуваються у національному кіберпросторі.

Складовою організаційної підструктури національного кіберпростору є підструктура, що утворюється на підставі відносин, які складаються між суб’єктами кіберпростору (постачальниками – операторами основних послуг, користувачами і регулятором – уповноваженим органом комунікаційних послуг, та визначають їх права і обов’язки, стосовно створення, збереження, передачі, використання і захисту інформації в інформаційно-телекомунікаційних системах відповідно до вимог національних нормативно-правових актів [24], [25]. Іншою суттєвою складовою організаційно-управлінської підструктури національного кіберпростору є *система оперативно-технічного управління телекомунікаційними мережами*, яка призначена для забезпечення сталого функціонування телекомунікаційних мереж в умовах надзвичайних ситуацій, надзвичайного та воєнного стану [6], [32]. До складу системи оперативно-технічного управління телекомунікаційними мережами входять: Національний центр оперативно-технічного управління телекомунікаційними мережами; центри оперативно-технічного управління операторів телекомунікацій та центри оперативно-технічного управління телекомунікаційними мережами центральних органів виконавчої влади, підприємств, установ та організацій; технічні засоби, призначені для оперативно-технічного управління телекомунікаційними мережами в умовах надзвичайних ситуацій, надзвичайного та воєнного стану [32]. Але, ключову об'єднувальну та координаційну роль у цьому процесі відіграватиме Національний координаційний центр кібербезпеки [1].

Аналіз джерел, надає підстави стверджувати, що надзвичайно впливовою підструктурою національного кіберпростору, що утворюється на підставі реалізації науково-дослідної та освітньої функцій, є *підструктура, що поєднує науково-дослідну діяльність і підготовку фахівців в сфері комунікацій та кібербезпеки в країні* [2], [9], [12], [13]. У цьому контексті в Стратегії відзначено, що Україна проведе докорінну реформу системи підготовки та підвищення кваліфікації фахівців у сфері кібербезпеки, а також здійснить заходи щодо збереження наявного кваліфікованого кадрового потенціалу суб'єктів кібербезпеки, стимулювання досліджень і розробок у сфері кібербезпеки з урахуванням появи нових кіберзагроз і викликів, створення національних інформаційних систем, платформ і продуктів [1]. Не менш впливовою складовою національного кіберпростору, пов’язаною з попередньою, на погляд дослідників, є його соціальне, психологічне та культурне середовище. Зміст цієї підструктури утворюється сукупністю базових принципів інформаційного суспільства, професійних норм, стандартів, провідних цінностей та мотивів, що характеризують культуру професіональної діяльності, спілкування і взаємовідносин в кіберпросторі. [29], [30].

Узагальнюючи аналіз конституювання національного кіберпростору, необхідно відзначити, що зміст його структури складається з взаємозалежних підструктур і сегментів, що утворюють цифрове комунікативне середовище і визначають його усталене функціонування на національних засадах як складової глобального інформаційного простору, а саме: онтологічної або сутнісної структури кіберпростору; функціональної підструктури; інформаційно-телекомунікаційної інфраструктури; національної системи кібербезпеки; організаційно-управлінської підструктури; освітньої та науково-дослідної підструктури, соціального, психологічного і культурного середовища кіберпростору.

У зв'язку з революційним розвитком галузі кібербезпеки, формуванням нової нормативної бази стандартів, виявляється низка наукових і освітніх завдань, спрямованих на аналіз і уточнення знань про змістовний бік національного кіберпростору як фактору його надійного захисту в умовах війни з російською федкрацією. Значущість знання про системний характер національного кіберпростору у підготовці кадрів в галузі кібербезпеки визначається, по-перше, роллю професійних і соціальних компетентностей в практичній діяльності фахівців в умовах революційних технологічних змін в цієї сфері, по-друге, системним характером самої професійної діяльності із забезпечення захисту національного кіберпростору, по-третє, освітньою роллю знань про кіберпростір, ефективним використанням його можливостей для реалізації форм організації електронної освіти, дистанційного навчання і самостійного набуття знань в галузі в умовах воєнного стану. Враховуючи системоутворювальну роль феномена кіберпростору в організації функціонування телекомунікацій, забезпечення державного контролю і кібербезпеки, доцільно зауважити про потребу залучення знань про структуру національного кіберпростору в систему підготовки фахівців. Необхідність опанування теоретичними засадами конституювання національного кіберпростору, знання його змістовних складових, складають підґрунтя формування системи компетентностей фахівців в галузі кібербезпеки.

Висновки. Отже, розробка і обґрунтування принципових теоретичних положень побудови національного кіберпростору, уточнення знань про його змістовний бік як умови контролювання і надійного захисту, впровадження знань про структурний зміст національного кіберпростору в систему підготовки фахівців в галузі кібербезпеки постає актуальним питанням, шо має теоретичну і практичну значущість для надійного захисту інформаційного простору, особливо в умовах воєнного стану. Подальша розробка науково-теоретичних і освітніх питань захисту національного кіберпростору є одним з пріоритетних завдань наукової та освітньої спільноти на шляху забезпечення національної безпеки України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Президент України. (2021, трав. 14). *Указ № 447/2021, Про рішення Ради національної безпеки і оборони України "Про Стратегію кібербезпеки України"*. [Електронний ресурс]. Доступно: https://www.president.gov.ua/documents/4472021-40013. Дата звернення: Січ. 10, 2023.

[2] О. Потій, Zoom-конференція, *"Цифрова трансформація держави: перспективи та ризики кібербезпеки"* Вер. 25, 2020. [Електронний ресурс]. Доступно: https://galinfo.com.ua/news/dlya_posylennya_kiberbezpeky_neobhidna_spivpratsya_naukovyh_ustanov_pidpryiemstv_ta_navchalnyh_zakladiv__potiy_351916.html. Дата звернення: Січ. 10, 2023.

[3] С. О. Гахов, "Кіберпростір як основна категорія науки кібернетика", *Сучасний захист інформації. Державний університет телекомунікацій*, № 1, с. 53-57, 2017. [Електронний ресурс]. Доступно: http://journals.dut.edu.ua/index.php/dataprotect/article/view/1412. Дата звернення: Січ. 10, 2023.

[4] Д. В. Дубов, *Кіберпростір як новий вимір геополітичного суперництва: монографія*, Київ, Україна: НІСД, 2014, 328 с. [Електронний ресурс]. Доступно: https://niss.gov.ua/sites/default/files/2015-02/Dubov_mon-89e8e.pdf. Дата звернення: Січ. 10, 2023.

[5] Д. В. Дубов, та М. А. Ожеван, *Кібербезпека: світові тенденції та виклики для України: аналітична доповідь*, Київ, Україна: НІСД, 2011, 31 с. [Електронний ресурс]. Доступно: https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/kiberbezpeka-svitovi-tendencii-ta-vikliki-dlya-ukraini-analitichna. Дата звернення: Січ. 10, 2023.

[6] С. В. Рибка, Є. В. Кільчицький, та О. М. Післегін, "Кіберпростір, управління інфраструктурою, кібербезпека", *Стратегічна панорама*, 2015, № 1, с. 126-134. [Електронний ресурс]. Доступно: http://nbuv.gov.ua/UJRN/Stpa_2015_1_17. Дата звернення: Січ. 10, 2023.

[7] І. Діордіца, "Система забезпечення кібербезпеки: сутність та призначення", *Підприємство, господарство і право. Інформаційне право* № 7, 2018. [Електронний ресурс]. Доступно: http://nbuv.gov.ua/UJRN/Pgip_2017_7_24. Дата звернення: Січ. 10, 2023.

[8] В. В. Горлинський, та Б. В. Горлинський, "Кібербезпека як складова інформаційної безпеки України", *Information Technology and Security*. July-December, vol. 7, iss. 2 (13), pp. 136-148. 2019, doi: https://doi.org/10.20535/2411-1031.2019.7.2.190559.

[9] В. В. Горлинський, та Б. В. Горлинський, "Аналіз ключових чинників формування системи компетентностей фахівців у галузі кібербезпеки", *Information Technology and Security*, vol. 9, iss. 2, pp. 219-231. 2021, doi: https://doi.org/10.20535/2411-1031.2021.9.2.249976.

[10] З. О. Звездова, та А. Вакалюк, "Стратегія забезпечення кібербезпеки в гібридній війні", *Acta De Historia & Politica: Saeculum XXI*, 3, с. 82–90, 2020. [Електронний ресурс]. Доступно: https://ahpsxxi.org/index.php/journal/article/view/51. Дата звернення: Січ. 10, 2023.

[11] Ю. Л. Яковенко, Ю. В. Деркаченко, С. В. Кухтик, та Д. О. Березовський, "Шляхи удосконалення системи кібербезпеки в Україні", *Проблеми сучасних трансформацій, серія: право, публічне управління та адміністрування*, *Публічне управління та адміністрування*, № 1, с. 88-93, 2021, doi: https://doi.org/10.54929/pmtl-issue1-2021-13.

[12] Ю. Даник, та О. Корнейко, "Основи методології формування кіберкомпетенцій у фахівців сектору безпеки і оборони України", *Information Technology and Security*, vol. 6, iss. 2, (11), 2018, doi: https://doi.org/ 10.20535/2411-1031.2018.6.2.153495.

[13] Ю. Ф. Щиголь, та О. О. Пучков, "Шляхи підвищення якості підготовки фахівців з кібербезпеки в інтересах сектору безпеки і оборони України", на *наук.-практ. конф. "Інформаційно-телекомунікаційні системи і технології та кібербезпека: нові виклики, нові завдання",* Київ, 2020, с. 16.

[14] Верховна Рада України. 7 сесія. (2017, жовт. 5). *Закон № 2163-VIII. Про основні засади кібербезпеки України*. [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/2163-19#Text. Дата звернення: Січ. 10, 2023.

[15] "Окінавська хартія глобального інформаційного суспільства" у *М. З. Згуровський, Розвиток інформаційного суспільства в Україні: правове регулювання у сфері інформаційних відносин*, Київ, Україна: НТУУ "КПІ", 2006.

[16] F. Kramer, S. H. Starr, and L. Wentz, *Cyberpower and National Security*, Washington, USA: Potomac Books, 2009. [Електронний ресурс]. Доступно: https://www.worldcat.org/title/755573496. Дата звернення: Січ. 16, 2023.

[17] Дж. П. Барлоу, *Декларація незалежності кіберпростору,* Давос, Швейцарія, 1996. [Електронний ресурс]. Режим доступу: https://ccl.org.ua/positions/deklaracziya-nezalezhnosti-kiberprostoru/. Дата звернення: Січ. 10, 2023.

[18] Генеральна Асамблея ООН. (1948, груд. 10). *Загальна декларація прав людини. Прийнята і проголошена резолюцією 217 А (III)*. [Електронний ресурс]. Режим доступу: https://ips.ligazakon.net/document/mu48001d?an=287&ed=1948_12_10. Дата звернення: Січ. 10, 2023.

[19] ISO/IEC 27032, *Information technology – Security techniques – Guidelines for cybersecurity*. 2012, 50 p. [Електронний ресурс]. Режим доступу: https://www.iso.org/standard/44375.html. Дата звернення: Січ. 10, 2023.

[20] В. С. Лукьянец, "Наука нового века. Гуманитарные трансформации", у *Наука и образование: современные трансформации: монография. Киев*, Україна: ПАРАПАН, 2008, с. 8-36.

[21] В. Покровська, "Аналіз методів виявлення інформаційно-психологічного впливу в соціальних мережах", *Information Technology and Security*, vol. 8, iss. 1 (14), pp. 40-48, 2020, doi: https://doi.org/10.20535/2411-1031.2020.8.1.218002.

[22] Ю. Кожедуб, Ю. Крамська, та В. Гирда, "Аналіз впливу людського фактору на кіберфізичну систему", *Information Technology and Security*, vol. 8, iss. 1, (14), pp. 102-115, 2020, doi: https://doi.org/10.20535/2411-1031.2020.8.1.218013.

[23] М. Шевченко, "Поняття національного інформаційного простору та його характеристики", *Український інформаційний простір. Теорія і практика сучасної журналістики*, № 1, с. 103-112. [Електронний ресурс]. Режим доступу: http://ukrinfospace.knukim.edu.ua/article/download/141098/138228/302273. Дата звернення: Січ. 15, 2023.

[24] Верховна Рада України. 4 сесія. (2020, груд. 16). *Закон № 1089-IX. Про електронні комунікації*. [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/1089-20#Text. Дата звернення: Січ. 20, 2023.

[25] Кабінет Міністрів України. *Постанова від 9 жовтня 2020 р. № 943, Київ. Деякі питання об'єктів критичної інформаційної інфраструктури*. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#n13. Дата звернення: Січ. 23, 2023.

[26] Міністерство інфраструктури України *Наказ від 23 грудня 2020 р. № 841, Київ. Про створення інформаційно-телекомунікаційних систем*. [Електронний ресурс]. Режим доступу: https://mtu.gov.ua/files/Dok_NORMATUVKA/841.pdf. Дата звернення: Січ. 10, 2023.

[27] Кабінет Міністрів України. *Розпорядження від 20 вересня 2017 р. № 649-р. Київ. Про схвалення Концепції розвитку електронного урядування в Україні*. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/649-2017-%D1%80#Text. Дата звернення: Січ. 10, 2023.

[28] А. І. Марущак, та С. Г. Петров, "Зміст поняття державні електронні інформаційні ресурси", *Інформація і право*, № 4 (27), 2018, с. 15-21. [Електронний ресурс]. Режим доступу: http://ippi.org.ua/sites/default/files/4_10.pdf. Дата звернення: Січ. 10, 2023.

[29] В. М. Богуш, В. В. Богуш, В. Д. Бровко, та В. П. Настрадін, *Основи кіберпростору, кібербезпеки та кіберзахисту: навч. посіб.* Київ, Україна: Ліра-К, 2020.

[30] В. О. Ананьїн, В. В. Горлинський, Л. О. Євдоченко, та О. О. Пучков, *Інформаційні виклики і ціннісні пріоритети суспільства Безпека України: актуальні проблеми та критерії оцінки: монографія*. Київ, Україна: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2018, 240 с.

[31] Кабінет Міністрів України. *Постанова від 17 березня 2004 р. № 326. Київ. Про затвердження Положення про Національний реєстр електронних інформаційних ресурсів*. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/326-2004-%D0%BF#Text. Дата звернення: Січ. 10, 2023.

[32] Кабінет Міністрів України. *Постанова від 29 червня 2004 р. №812. Київ. Порядок оперативно-технічного управління телекомунікаційними мережами в умовах надзвичайних ситуацій, надзвичайного та воєнного стану.* [Електронний ресурс]. Режим доступу: https://www.kmu.gov.ua/npas/7133105. Дата звернення: Січ. 10, 2023.

[33] В. В. Горлинський, Б. В. Горлинський, та В. П. Романенко, "Інституційно-правові аспекти конституювання національного кіберпростору України", *на II Всеукр. наук.-практ. конф. Соціальна і цифрова трансформація: теоретичні та практичні проблеми правового регулювання,* Київ, 2022, с. 49-52. [Електронний ресурс]. Режим доступу: http://ippi.org.ua/sites/default/files/konferenciya_2022_maket_0.pdf. Дата звернення: Січ. 10, 2023.

Стаття надійшла до редакції 21.01.2023.

REFERENCES

[1] President of Ukraine. (2021, May 14). Decree № 447/2021, *On the Decision of the National Security and Defense Council of Ukraine "On the Cyber Security Strategy of Ukraine"*. [Online]. Available: https://www.president.gov.ua/documents/4472021-40013. Accessed on: Jan. 10, 2023.

[2] O. Potyi, Zoom-conference *"Digital transformation of the state: prospects and risks of cybersecurity"*, Sept. 25, 2020. [Online]. Available: https://galinfo.com.ua/news/dlya_posylennya_kiberbezpeky_neobhidna_spivpratsya_naukovyh_ustanov_pidpryiemstv_ta_navchalnyh_zakladiv__potiy_351916.html. Accessed on: Jan. 10, 2023.

[3] S. O. Gakhov, "Cyberspace as the main category of cybernetics science", *Modern information security. State University of Telecommunications*, № 1. pp. 53-57, 2017. [Online]. Available: http://journals.dut.edu.ua/index.php/dataprotect/article/view/1412. Accessed on: Jan. 10, 2023.

[4] D. V. Dubov, *Cyberspace as a New Dimension of Geopolitical Rivalry: monograph*, Kyiv, Ukraine: NISD, 2014. [Online]. Available: https://niss.gov.ua/sites/default/files/2015-02/Dubov_mon-89e8e.pdf. Accessed on: Jan. 10, 2023.

[5] D. V. Dubov, and M. A. Ozhevan, *Cyber Security: Global Trends and Challenges for Ukraine: analytical Report*, Kyiv, Ukraine: NISD, 2011. 31 p. [Online]. Available: https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/kiberbezpeka-svitovi-tendencii-ta-vikliki-dlya-ukraini-analitichna. Accessed on: Jan. 10, 2023.

[6] S. V. Rybka, E. V. Kilchytskyiб and O. M. Pislegin, "Cyberspace, infrastructure management, cyber security", *Strategic Panorama*, 2015, no. 1, pp. 126-134. [Online]. Available: http://nbuv.gov.ua/UJRN/Stpa_2015_1_17. Accessed on: Jan. 10, 2023.

[7] I. Diordica, "Cybersecurity: Essence and Purpose, Enterprise*", Business and Law. Information law*, №7, 2017. [Online]. Available: http://nbuv.gov.ua/UJRN/Pgip_2017_7_24. Accessed on: Jan. 10, 2023.

[8] V. V. Horlynskyi, and B. V. Horlynskyi, "Cybersecurity as a component of information security of Ukraine", *Information Technology and Security.* July-December, vol. 7, iss. 2 (13), pp. 136-148, 2019, doi: https://doi.org/10.20535/2411-1031.2019.7.2.190559.

[9] V. V. Horlynskyi, and B. V. Horlynskyi, "Analysis of key factors of formation of the system of competences of professionals in the field of Cybersecurity" *Information Technology and Security.* July-December, vol. 9, iss. 2, pp. 219-231, 2021, doi: https://doi.org/10.20535/2411-1031.2021.9.2.249976

[10] Z. O. Zvezdova, and A. Vakalyuk, The strategy of ensuring cyber security in hybrid warfare, *Acta De Historia & Politica: Saeculum XXI*, iss. 3, pp. 82–90, 2020. [Online]. Available: https://ahpsxxi.org/index.php/journal/article/view/51. Accessed on: Jan. 10, 2023.

[11] Yu. L. Yakovenko, Yu. V. Derkachenko, S. V. Kukhtyk, and D. O. Berezovsky, Ways to improve the cybersecurity system in Ukraine, *Problemy suchasnykh transformatsii, Seriia: pravo, publichne upravlinnia ta administruvannia, Publichne upravlinnia ta administruvannia*, no. 1, pp. 88-93, 2021, doi: https://doi.org/10.54929/pmtl-issue1-2021-13.

[12] Yu. Danyk, and O. Korneiko, "Basics of methodology of cybercompetence formation in specialists of the security and defense sector of Ukraine", *Information Technology and Security.* July-December, vol. 6, iss. 2-11, 2018, doi: https://doi.org/10.20535/2411-1031.2018.6.2.153495.

[13] Yu. F. Shchigol, and O. O. Puchkov, "Ways to improve the quality of training of cybersecurity specialists in the interests of the security and defense sector of Ukraine", *in Proc. The scientific-practical conference "Information and telecommunication systems and technologies and cybersecurity: new challenges, new tasks"*, Kyiv, 2020, p. 16.

[14] Verkhovna Rada of Ukraine. 7th Session. (2017, Oct. 5). *Law no. 2163-VIII. About the Basic Principles of Cyber Security of Ukraine*. [Online]. Available: http://zakon.rada.gov.ua/laws/show/. Accessed on: Jan. 10, 2023.

[15] "Okinawa Charter of the Global Information Society", in *Zgurovskyi M.Z. Development of the Information Society in Ukraine: Legal Regulation in the Field of Information Relations*. Kyiv, Ukraine: NTUU "KPI", 2006.

[16] F Kramer, S. H. Starr, and L Wentz, *Cyberpower and National Security*, Washington, USA: Potomac Books, 2009. [Online]. Available: https://www.worldcat.org/title/755573496 Accessed on: Jan. 16, 2023.

[17] John Perry Barlow, *"A Declaration of the Independence of Cyberspace",* Davos, Switzerland: 1996. [Online]. Available: https://ccl.org.ua/positions/deklaracziya-nezalezhnosti-kiberprostoru/. Accessed on: Jan. 10, 2023.

[18] Universal Declaration of Human Rights. *Adopted and proclaimed by resolution 217 A (III) of the UN General Assembly* of December 10, 1948. [Online]. Available: https://ips.ligazakon.net/document/mu48001d?an=287&ed=1948_12_10. Accessed on: Jan. 10, 2023.

[19] ISO/IEC 27032, Information technology – Security techniques – Guidelines for cybersecurity. 2012. 50 p. [Online]. Available: https://www.iso.org/standard/44375.html. Accessed on: Jan. 10, 2023.

[20] V. S. Lukkyanets, "Science of the new century. Humanitarian transformations", in *Science and education: modern transformations: monograph. Institute of Philosophy named after. G. S. Skovoroda pans of the National Academy of Sciences of Ukraine.* Kiev, Ukraine: PARAPAN, 2008. pp. 8-36.

[21] V. Pokrovska, "Analysis of information-psychological impact detection methods in social networks", *Information Technology and Security*, January-June, vol, 8, iss. 1 (14), pp. 40-48, 2020, doi: https://doi.org/10.20535/2411-1031.2020.8.1.218002.

[22] Yu. Kozhedub, Yu. Kramska, and V. Hyrda, "Analysis of the human factor influence on the cyber-physical system", *Information Technology and Security*, January-June, vol. 8, iss. 1 (14), pp. 102-115, 2020, doi: https://doi.org/10.20535/2411-1031.2020.8.1.218013.

[23] M. Shevchenko, "The Notion of National Information Space and its characteristics", *Theory and Practice of Contemporary Journalism, Ukrainian Information Space*, iss. 1, pp.103-112. [Online]. Available: http://ukrinfospace.knukim.edu.ua/article/download/141098/138228/302273. Accessed on: Jan. 15, 2023.

[24] Verkhovna Rada of Ukraine. 6th Session. (2020, Dec. 16). *Law of Ukraine no. 1089-IX. About electronic communications*. [Online]. Available: https://zakon.rada.gov.ua/laws/show/1089-20#Text. Accessed on: Jan. 20, 2023.

[25] Cabinet of Ministers of Ukraine. (2020, Oct. 9). *The resolution no. 943, Some issues of critical information infrastructure*. [Online]. Available: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#n13. Accessed on: Jan. 23, 2023.

[26] Ministry of Infrastructure of Ukraine. (2020, Dec. 23). *Order no. 841. About the creation of information and telecommunication systems*. [Online]. Available: https://mtu.gov.ua/files/Dok_NORMATUVKA/841.pdf. Accessed on: Jan. 10, 2023.

[27] Cabinet of Ministers of Ukraine. (2017. Sept. 20). *Order no. 649-p. About approval of the concept of e -government development in Ukraine*. [Online]. Available: https://zakon.rada.gov.ua/laws/show/649-2017-%D1%80#Text. Accessed on: Jan. 10, 2023.

[28] A. I. Marushchak, and S. G. Petrov, "The content of the concept of state electronic information resources", *Information and law*, no. 4 (27), 2018, pp. 15-21. [Online]. Available: http://ippi.org.ua/sites/default/files/4_10.pdf. Accessed on: Jan. 10, 2023.

[29] V. M. Bogush, V. V. Bogush, V. D. Brovko, and V. P. Nastradin, *The basics of Cyberspace, Cybersecurity and Cyber Protection: Textbook.* Kiev, Ukraine: Lyra-K, 2020.

[30] V. O. Ananin, V. V. Horlynskyi, L. O. Evdochenko, and O. O. Puchkov, *Information challenges and value priorities of society Safety of Ukraine: Actual problems and evaluation criteria: Monograph*. Kiev, Ukraine: ISCIP Ihor Sikorskyi KPI, 2018. 240 p.

[31] Cabinet of Ministers of Ukraine. (2004. Mar. 20). *Order no. 326. About approval of the Regulations on the National Register of Electronic Information Resources*. [Online]. Available: https://zakon.rada.gov.ua/laws/show/326-2004-%D0%BF#Text. Accessed on: Jan. 10, 2023.

[32] Cabinet of Ministers of Ukraine. (2004. Jun. 29). *Order no. 812. The order of operational and technical management of telecommunications networks in emergency, surrounding situations and martial law*. [Online]. Available: https://www.kmu.gov.ua/npas/7133105. Accessed on: Jan. 10, 2023.

[33] V. V. Horlynskyi, B. V. Horlynskyi, and V. P. Romanenko, "Institutional and legal aspects of the constitution of the national cyberspace of Ukraine", *on the II All-Ukrainian science and practice conf. Social and digital transformation: theoretical and practical problems of legal regulation,* Kiev, 2022, pp. 49-52. [Online]. Available: http://ippi.org.ua/sites/default/files/konferenciya_2022_maket_0.pdf. Accessed on: Jan. 10, 2023.

VICTOR HORLYNSKYI,
BORIS HORLYNSKYI

CONSTITUTION OF NATIONAL CYBER SPACE AND ITS EDUCATIONAL SIGNIFICANCE FOR CYBER SECURITY PROFESSIONALS

It is shown that the construction of an established system of cybersecurity of the state in the context of globalization, development of information technologies, transfer of “hybrid wars” to cyberspace, requires improving the quality of training, on which depends the reliability of national cyberspace. It is specified that the key indicator of qualification of specialists in the field of cybersecurity is competence, but their final definition and actual content, in accordance with the requirements of rapid technical and technological development, requires substantiation of theoretical principles that are the object of study. It is substantiated that an essential component of the theoretical basis for determining the system of competencies is a certain set of factors that determine its constitution and determine the subject and purpose of the study. The key factors that need to be taken into account in determining professional competencies are the following: the requirements of the modern education system; the systemic nature of the processes unfolding in global cyberspace; conceptual principles of cybersecurity; rapid development of information technologies and the transition to a quantum basis; new threats to national security arising from the convergence of information and high-tech technologies; cyberattacks aimed at government agencies and national security structures; attempts at destructive psychological influence on the personnel of the security and defense sector; Ukraine's course towards Euro-Atlantic integration, harmonization of the national system of standards with NATO standards in the field of cyber security; increasing the riskiness of professional activity; challenges of gender policy to achieve gender equality in the field of security and defense of Ukraine. Therefore, it should be noted that the training of specialists in the field of cybersecurity in the interests of the future of the country should be based on a certain, methodologically sound system of competencies, the implementation of which should lead to quality training in professional activities in the field of cyberspace.

Keywords: national security, cyber security, global information space, structure of national cyberspace, training of specialists.

Горлинський Віктор Вікторович, кандидат філософських наук, доцент, доцент кафедри військово-гуманітарних дисциплін, Інститут спеціального зв’язку та захисту інформації Національного технічного університету України “Київський політехнічний інститут імені Ігоря Сікорського”, Київ, Україна, ORCID 0000-0003-1190-5991, gvv1004@gmail.com.

Горлинський Борис Вікторович, кандидат технічних наук, Адміністрація Державної служби спеціального зв’язку та захисту інформації України, Київ, Україна, ORCID 0000-0002-9993-2427, vjzgoxnf@gmail.com.

Horlynskyi Viktor, candidate of philosophical sciences, associate professor, associate professor at the military and humanitarian disciplines academic department, Institute of special communication and information protection of National technical university of Ukraine “Igor Sikorsky Kyiv polytechnic institute”, Kyiv, Ukraine.

Horlynskyi Borys, candidate of technical sciences, Administration of State serves of special communication and information protection of Ukraine, Kyiv, Ukraine.