CYBERSECURITY AND CRITICAL INFRASTRUCTURE PROTECTION

DOI 10.20535/2411-1031.2025.13.1.328980
УДК 004.056.53

ВІКТОР ГОРЛИНСЬКИЙ,
БОРИС ГОРЛИНСЬКИЙ

КІБЕРВІЙНА ЯК СИСТЕМНИЙ ВИКЛИК КІБЕРБЕЗПЕЦІ УКРАЇНИ

На підставі аналізу наукових джерел і узагальнення знань щодо протистояння у глобальному кіберпросторі, з'ясовано чинники генезису кібервійни, а саме: зростання залежності світових і національних процесів від телекомунікаційних технологій і мереж; анонімність та важкість виявлення джерел кібератак; відносно невисокі економічні витрати; широкі можливості у застосуванні електронних засобів для досягнення стратегічних і військових цілей в геополітичних конфліктах і гібридних війнах. Узагальнено базові ознаки кібервійни: сторонами кібервійни можуть бути держави, коаліції або інші суб'єкти міжнародних відносин; основними цілями у кібервійні є державні стратегічні та військові об'єкти, фінансові установи, критична інфраструктура країни; основним засобом кібервійни є комплексне, скоординоване в часі і просторі, застосування різноманітних видів кіберзброї; базовою формою застосування кіберзброї у кібероперації є кібератака; залучення до превентивних кібероперацій кібервійськ і кіберпідрозділів; організація превентивної кібероборони як протидії деструктивному впливу на кіберпростір у формах кібершпигунства, кібердиверсій, кібертероризму і кіберзлочинності. Запропоноване розуміння сутності кібервійни – як способу розв'язання геополітичних і соціально-економічних протиріч між суб'єктами міжнародних відносин з комплексним застосуванням кіберзброї та інших форм деструктивного впливу на кіберпростір. Розкрито змістовну сторону кібервійни, що визначається складом і функціями структурних компонентів організації упереджувальної активної протидії у кібервійні. Обґрунтовано чинники функціонування національного сегменту кіберпростору в умовах кібервійни, а саме:

– наявність кіберпотенціалу протиборства у кіберпросторі – стримування кіберзлочинності, кібертероризму та інших кіберзагроз;

– дієва кібероборона на підставі застосування кіберпідрозділів з повноваженнями ведення протиборства в кіберпросторі та ефективної взаємодії основних суб'єктів національної системи кібербезпеки та сил оборони;

– кіберстійкість, захищеність і кіберготовність національної критичної інфраструктури; національний кіберсуверенітет – як правова захищеність усталеного функціонування кіберпростору на національних та міжнародних правових засадах;

– наявність професійно-освітнього потенціалу держави, забезпеченість кадрових потреб фахівцями з кібербезпеки.

Ключові слова: кібербезпека, кібервійна, кіберзахист, кіберзброя, кіберпростір, кіберпотенціал, кібероборона, кіберсили.

Постановка проблеми. Аналіз подій, що відбуваються в сучасному глобальному кіберпросторі із застосуванням можливостей та цифрових інструментів, стосовно національного кіберпростору України в умовах озброєного повномасштабного вторгнення російської федерації, свідчить про перехід у використанні різних форм цифрової агресії із застосуванням сил, способів, засобів та масштабів протистояння на новий якісний рівень, якій може бути визначено як кібервійна. За таких умов, питання надійного захисту національного

кіберпростору та організації ефективної системної протидії у кібервійни, постає пріоритетним чинником забезпечення національної безпеки України та передбачає подальші теоретичні дослідження [1]–[4]. В умовах, коли проти України ведеться кібервійна, визначення і обґрунтування можливостей держави щодо забезпечення кібербезпеки, постає її теоретичною передумовою та залежить від адекватного розуміння змін структурних і функціональних параметрів захисту національного кіберпростору, спричинених кібервійною. Потреба в науковому обґрунтуванні шляхів ефективної та системної протидії у кібервійні, зумовлює необхідність теоретичного розв'язання наукових завдань, спрямованих на аналіз і уточнення знань про сутність, ознаки, зміст і засоби кібервійни, її вплив на національний кіберпростір з наступним впровадженням відповідних знань як компетентнісної складової підготовки фахівців в галузі кібербезпеки.

Аналіз останніх досліджень і публікацій. Контент аналіз масиву праць, у яких ставиться питання про появу нового типу протистояння у кіберпросторі як феномену кібервійни, надає підстави віднести до теоретичних витоків "концепту кібервійни" праці закордонних дослідників [5]–[11]. Вивчення теоретичних джерел з проблем, що стосуються аналізу кібербезпеки в умовах кібервійни, дозволяє зауважити зростання наукового інтересу до цієї проблематики серед українських науковців. Питання щодо аналізу і визначення ознак кібервійни вирішувалось у працях [12], [13], [16], [19]–[23], [32]. Різноманітні аспекти протидії у кібервійні висвітлено [12], [28]–[32], [36]. Аналіз насильства, що здійснюється в кіберпросторі в період збройних конфліктів, застосування кіберзброї та інші військові аспекти кібервійни розкрито в [16], [17], [21]–[23], [27]–[31]. Питання, щодо забезпечення кібербезпеки об'єктів критичної інфраструктури в умовах кібервійни, досліджувалось у роботах [27], [31], [32]. Політико-правові та економічні аспекти кібервійни проаналізовано в [16], [17], [19], [21]–[23]. Незважаючи на інтерес вчених до певних аспектів протидії кібервійнам, питання щодо наукового обґрунтування сутності та змісту кібервійни, досі залишається дискусійним. Потреба в теоретичній розробці напрямів, форм, способів і засобів ефективній та системній протидії у кібервійні збоку держави, вимагає подальших досліджень, спрямованих на поглиблення знань про зміст і ознаки кібервійни, з'ясування особливостей захисту кіберпростору в умовах кібервійни з наступним впровадженням відповідних знань в систему підготовки фахівців з кібербезпеки.

Метою статті *є* поглиблення знань про сутність, ознаки і зміст поняття "кібервійна", розкриття особливостей захисту кіберпростору в умовах кібервійни.

Виклад основного матеріалу дослідження. Після повномасштабного озброєного вторгнення російської федерації в Україну, глобальний кіберпростір як середовище інформаційної взаємодії, перетворився на середовище розгортання кібервійни між його національними секторами та різноманітними сегментами [2], [4]. У "Річному аналітичному огляді: ключові події, тенденції та виклики у сфері кібербезпеки у 2024 році", ситуація, що склалася навколо російсько-української кібервійни, визначено як "*перша світова кібервійна"* [4, с. 28]. Виникає запитання: які зміни відбуваються в національному кіберпросторі України як середовищі розгортання кібервійни та яка їх роль і значущість у забезпечення кібербезпеки в умовах кібервійни? Відповідь на це питання можлива на підставі з'ясування генезису, сутності, ознак і змісту кібервійни та її впливу на національний сектор кіберпростору.

Висвітлюючи генезис поняття "кібервійна", потрібно відзначити, що перші спроби застосування в публікаціях цього терміну, наприкінці сімдесятих – початку восьмидесятих років XX ст., відображали футурологічні погляди на кібервійну як війну кіборгів у майбутньому. Наближеним до сучасного розуміння кібервійни, вважається її передбачення у праці [5], в якій головна роль у кібервійні відводиться хакерам. До більш фундаментальних досліджень кібервійни, відносять роботи [6], [7], у яких кібервійна характеризується як дії однієї національної держави з проникнення в комп'ютери або мережі іншої національної держави для досягнення цілей нанесення збитку або руйнування [7]. Узагальнена сутність кібервійни у сучасних дослідженнях переважно визначається як конфлікт інтересів,

протистояння або зіткнення у кіберпросторі та пов'язується з використанням Інтернету, технологічних та інформаційних засобів [12], [19], [21].

Проте, незважаючи на велику кількість публікацій, застосування терміну "кібервійна" характеризується відсутністю єдиного науково обґрунтованого підходу або використанням поняття у символічному значенні. У публікаціях нерідко наводяться авторські визначення кібервійни, сформульовані на підставі різноманітних, але не систематизованих ознак. Зустрічаються публікації, у яких кібервійною називають одиничні кібератакі, окремі акти кібертероризму, кібершпигунство чи кіберзлочини, але такі, що не мають нічого спільного з міждержавними конфліктами, підкреслюють дослідники [12, с. 26]. Поряд із зазначеним, необхідно зауважити некоректність, пов'язану з використанням, стосовно поняття "кібервійна", більш широкого, за своїм змістом, терміну – "інформаційна війна" [13]. Або коли у визначенні кібервійни, наводяться ознаки, що характеризують інформаційну війну в її широкому розумінні. В цьому контексті можна частково погодитись з зауваженням, що кібервійна – це технічний вимір інформаційної війни [9, с. 245-284]. На погляд авторів, умовна "червона лінія" відокремлення кібервійни від інформаційної, має проходити за принциповими ознаками відрізнення кіберпростру від інформаційного простору [14]. В контексті підходу, що застосовується воєнними науками, кібервійну розглядають як воєнну стратегію, спрямовану на створення несприятливих умов, шляхом виведення з ладу комп'ютерів противника, керуючих життєво важливими функціями держави, перехоплення і спотворення інформації, впровадження у програмне забезпечення вірусів, закладок і логічних бомб [12, с. 26]. Заслуговує на увагу підхід, згідно з яким, кібервійну вважають частиною звичайної війни, розуміючи її як "дії проти військових цілей під час війни [6].

Контент аналіз наукових джерел надає можливість віднести до основних чинників генезису кібервійни, наступні: зростання залежності світових і національних процесів від телекомунікаційних технологій і мереж, які пронизують майже всі сфери життя суспільства; анонімність та важкість виявлення джерел кібератак; відносно невисокі економічні витрати у порівнянні з іншими засобами; розширення можливостей у застосуванні електронних засобів для: досягнення цілей в геополітичних конфліктах і гібридних війнах в інтересах воєнної та економічної розвідки; в цілях дестабілізації країни, дезорганізації управління державою; розширення можливостей кібератак і аналітичної розвідки завдяки застосуванню технологій штучного інтелекту та квантових технологій.

Аналіз міжнародних і національних джерел права дозволяє відокремити певні ознаки порушення норм права у кіберпросторі, які можна екстраполювати на розуміння поняття і змісту кібервійни. Так, документи Генеральної Асамблеї ООН, щодо захисту кіберпростору і забезпечення кібербезпеки, пропонують систему заходів для запобігання використанню глобального кіберпростору для військових цілей, не використовуючи поняття "кібервійна" [15]. Міжнародний комітет Червоного Хреста (МКЧХ) у своїх документах, звітах, роз'ясненнях розглядає питання застосування міжнародного гуманітарного права до кіберконфліктів та кібероперацій, наголошуючи, що воно обмежує застосування в час озброєного конфлікту кіберзброї, так само, як і будь-якої іншої зброї, засобів та методів ведення війни – і нових, і старих [16], [17]. Застосуванням міжнародного гуманітарного права до кіберпростору в умовах війни знаходиться у центрі уваги фахівців з кібербезпеки України та її партнерів. Так, Національний координаційний центр кібербезпеки обговорює з партнерами питання щодо статусу комбатантів у "кібервійні", міжнародний досвід щодо застосування міжнародного гуманітарного права до проведення кібероперацій, правовий аналіз кібератак, що відбувались під час російсько-української війни [4, с. 29]. У контексті правового регулювання процесів, що відбуваються у глобальному кіберпросторі, документом, спрямованим на боротьбу з кіберзлочинами, що розглядаються як складова кібервійни, є Конвенція про кіберзлочинність (Будапешт, 2001 р.) [18]. У цій міжнародній угоді визначені правові аспекти, стосовно використання кіберпростору із злочинними цілями. Хоча безпосередньо термін "кібервійна" не використовується, Конвенція є важливим інструментом

для боротьби з кіберзлочинами, зокрема, в умовах війни. Хоча, з погляду на те, що кіберпростір не є повною мірою контрольованим нормами міжнародного права, він залишає великі можливості для втручання. [19, с. 12-22].

Серед нормативно-правових джерел України, можна відокремити декілька документів, у яких прямо термін "кібервійна" не застосовується, але у певній мірі відображені питання, що стосуються кібервійни. Так, у Законі "Про основні засади забезпечення кібербезпеки України" (далі – Закон) визначено принципові положення щодо боротьби з кіберзагрозами, включаючи кібератакі, які за певних обставин, можуть бути класифіковані як акти кібервійни [1]. У Законі наведено визначення таких понять як "кібератака", "кіберзлочин", "кібероборона", "кіберрозвідка", "кібертероризм", "кібершпигунство", які за певних обставин, можуть розглядатися як складові кібервійни. У документі, також, наведено поняття, що певною мірою, корелюють з дефініцією "кібервійна", а саме:

– "активна протидія агресії у кіберпросторі" – як дії, спрямовані на підвищення рівня кіберзахисту шляхом нейтралізації кібератак держави-агресора, його систем і мереж, джерел походження кіберзагроз та кібератак, які використовуються для завдання шкоди національній безпеці України;

– "система активної протидії агресії у кіберпросторі", що трактується як сукупність організаційних, правових, наукових та технічних заходів, спрямованих на підвищення рівня кіберзахисту держави шляхом здійснення впливу на інформаційні (автоматизовані) та інформаційно-комунікаційні системи держави-агресора, джерела походження кіберзагроз та кібератак.

Стратегія кібербезпеки України (далі – Стратегія) окреслює стратегічні плани України щодо зміцнення кібербезпеки та реагування на кібератаки, які за своєю сутністю утворюють засади організації протидії кіберзагрозам в умовах кібервійни [2]. У Стратегії визначено виклики для України у сфері кібербезпеки, серед яких – мілітаризація кіберпростору та розвиток кіберзброї, що дає можливість приховано проводити кібератаки для підтримки бойових дій і розвідувально-підривної діяльності у кіберпросторі [2], які також можуть тлумачиться як базові ознаки кібервійни. У документі відзначено низку тенденцій, які можуть свідчити про розгортання кібервійни, зокрема, створення кібервійськ, до завдань яких належить не лише забезпечення захисту критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі, що включає виведення з ладу критично важливих об'єктів інфраструктури противника шляхом руйнування інформаційних систем, які управляють такими об'єктами [2]. Серед інших нормативно-правових джерел, що визначають норми забезпечення кібербезпеки і захисту кіберпростору в умовах кібервійни, доцільне відзначити Указ Президента України Про рішення РНБО України "Про невідкладні заходи з кібероборони держави", спрямований на створення у системі Міністерства оборони України кібервійськ та набуття ними відповідних спроможностей [20]. В цілому, визначені документи, надають правову базу для аналізу та протидії кіберзагрозам в контексті міжнародного права і національної безпеки України в умовах кібервійни. Але незважаючи на чисельні наукові публікації, що висвітлюють різноманітні аспекти кібервійни, єдиного, науково обґрунтованого підходу до визначення її сутності, яке застосовувалося б у міжнародному чи національному праві, на цей час немає, [12, с. 26], [19], [21, с. 17], [22, с23-24].

Вивчення джерел дозволяє відзначити, що одним з центральних проблематичних питань з аналітики кібервійни, що потребує розв'язання, є уточнення і систематизація базових ознак, на підставі яких, має ґрунтуватися визначення сутності кібервійни. Компаративний аналіз змісту публікацій, надає підстави відокремити декілька груп сутнісних характеристик або ознак кібервійни, що мають відповідати логічним принципам утворення визначення. *Перша група* системних ознак, стосується характеристики кіберпростору як середовища розгортання кібервійни. *Друга група* ознак спрямована на з'ясування особливостей та змісту кібервійни як техніко-технологічної складової інформаційної війни та має характеризувати

засоби ведення кібервійни, серед яких, головним і системоутворювальним, вважається застосування кіберзброї. *Третя група* – має охоплювати системні та організаційні ознаки, що належать поняттю кібервійни як геополітичному явищу і кіберскладової військового конфлікту або війни [22, с. 26].

Розкриваючи сутнісні характеристики кібервійни, варто підкреслити, що *основною та невід'ємною ознакою кібервійни аналітики вважають деструктивний вплив на кіберпростір як середовище розгортання кібервійни та електронного цифрового протиборства між суб'єктами міжнародних відносин* [12, с. 26]. Кібервійна відбувається у кіберпросторі, що є однією із сутнісних ознак цього явища [22, с. 27]. У Стратегії кібербезпеки України (2021) відзначено, що кіберпростір разом з іншими фізичними просторами визнано одним з можливих театрів воєнних дій [2]. Саме реалізація прояву сили у кіберпросторі, на думку дослідників, надає підстави позначати це явище як кібервійна. Про зростання значущості кіберпростору для досягнення цілей військових операцій свідчить докладний аналіз ключових подій, тенденцій та викликів у сфері кібербезпеки у 2024 році [4]. З погляду на зазначене, кібервійна визначається як озброєне протистояння у кіберпросторі, яке ведеться за допомогою комп'ютерних технологій з метою завдання шкоди. Відзначено, що кібервійна ведеться переважно державними суб'єктами, за участі приватних, і може супроводжувати збройний чи інший конфлікт між ними [21, с.15]. Зауважено, що тривала атака в кіберпросторі з елементами захисту інформаційних систем та протидією опоненту з масштабними наслідками для сторін кіберпротиборства та пересічних користувачів кіберпростором, надає певні підстави називати це явище кібервійною [23, с. 42].

Досліджуючи особливості організації кіберпростору в умовах кібервійни, треба відзначити, що реалізація російською федерацією концепції інформаційного протиборства, базованої на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, створює реальну загрозу вчинення актів кібертероризму та кібердиверсій, стосовно національної інформаційної інфраструктури [2]. Останнім часом спостерігається зростання інтенсивності міждержавного протиборства і розвідувально-підривної діяльності у кіберпросторі із залученням міжнародних хакерських угруповань [2], [4]. Все більшого розповсюдження набувають політично вмотивовані атаки. За результатами дослідження ENISA, опублікованого в грудні 2023 року, 60% DDoS атак наразі мають політичне підґрунтя [4, с. 16]. Кібервимір російсько-української війни змінює ставлення щодо наступальних кібероперацій, які раніше офіційно не оголошувались, але, починаючи з 2023 року, держави вже публічно заявляють про кібернаступальні операції та створюють кіберсили [4, с. 9].

Про важливу роль і значущість ефективного використання і управління глобальним кіберпростором, в інтересах забезпечення кібебезпеки, свідчить Стратегія, прийнята у США "Міжнародний кіберпростір і стратегія цифрової політики США" (2024). Концепція цифрової солідарності, що лежіть в основі Стратегії, ґрунтується на зусиллях із створення цифрових і кіберпотенціалів, для побудови захищеної та стійкої цифрової екосистеми в довгостроковій перспективі, та можливості реагувати та швидко відновлюватись у разі виникнення інцидентів і затримувати злочинців [24]. Стратегія США становить особливий інтерес у контексті сучасного розуміння специфічних рис глобального кіберпростору, в якому поняття "цифрова екосистема" використовується як синонім терміну "кіберпростір" з доданням екологічної складової [24]. Ця екосистема містить:

- апаратне забезпечення;
- програмне забезпечення;
- протоколи;
- технічні стандарти;
- постачальників, операторів, користувачів і ланцюжки поставок, що охоплюють телекомунікаційні мережі;
- підводні кабелі;
- хмарні обчислення;

– центри обробки даних та супутникову мережеву інфраструктуру;
– операційні технології; програми;
– веб-платформи та споживчі технології;
– Інтернет речей;
– штучний інтелект та інші критичні та нові технології.

Узагальнюючи, доцільно перелічити *особливості, притаманні сучасному кіберпростору,* що потребують врахування у забезпеченні кібербезпеки держави, а саме [2], [4], [24]:

– зростання інтенсивності міждержавного протиборства і розвідувально-підривної діяльності у кіберпросторі;

– використання глобального кіберпростору для політично вмотивованих кібератак і досягнення геополітичних цілей; мілітаризація глобального кіберпростору, розвиток кіберзброї та створення державами кібервійськ;

– застосування кіберсил для превентивних наступальних кібероперацій; залучення міжнародних хакерських угруповань для здійснення актів кібертероризму і кібердиверсій;

– зростання загроз для об'єктів критичної інфраструктури; використання інформаційних ресурсів і технологій у злочинних, терористичних цілях, стосовно як цивільної, так і військової сфери;

– суттєвий вплив на сферу кібербезпеки технологій ШІ та квантових технологій; посилення кіберзагроз для космічних об'єктів та підводної цифрової інфраструктури.

В сучасних умовах збройного протиборства в глобальному кіберпросторі, вирішення проблеми надійного захисту його національного сегменту, постає найактуальнішим питанням забезпечення національної безпеки України [1], [2], [4]. В умовах зростання геополітичного суперництва та посилення інтенсивності міждержавного протиборства [2], виникає питання управління і захисту національного сегменту кіберпростору, що потребує конкретизації поняття "національний кіберпростір". Ґрунтуючись на положеннях, наведених у Законі [1], можна стверджувати, що національний кіберпростір утворюється в наслідок функціонування і взаємодії компонентів, що складають комунікативне середовище держави, а саме [1], [14]:

– інформації, що має державну значущість та підлягає захисту;
– системи електронних комунікацій; системи управління технологічними процесами;
– електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах.

Узагальнюючи, *сутність національного кіберпростору* доцільно розглядати як цифрове комунікативне середовище, на функціонування якого поширюється юрисдикція держави [14]. Саме розповсюдження юрисдикції держави, надає можливість створювати додаткові інструменти надійного захисту національного сегменту кіберпростору в умовах посилення інтенсивності міждержавного протиборства [2], [14].

Центральним елементом у розумінні забезпечення національних інтересів у кіберпросторі вважається концепт могутності, що застосовується у геополітиці [25, с.41. Найбільш обгрунтованим вважається підхід, згідно з яким, під кібермогутністю пропонується розуміти здатність до використання кіберпростору для створення переваг та впливу в усіх інших операційних просторах через інструменти могутності [25, с. 38]. "Інструменти могутності" тлумачаться як міра здатності використовувати кіберпростір, де технології вважаються одним з ключових чинників, що забезпечують базову можливість його використання [25, с. 39]. До основних складових кібермогутності, відносять розвинену кібернетичну інфраструктуру і цифровий суверенітет держави що розуміється як здатність держави самостійно й незалежно забезпечувати національні інтереси в кіберсфері, самостійно розпоряджатися власними інформаційними (цифровими) ресурсами та національною інформаційною інфраструктурою [25, с. 222].

Основним способом впливу на кіберпростір в умовах кібервійни, вважається кібератака. Згідно із Законом**,** кібератака – це спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту [1]. Комплексне застосування кібератак проти військових об'єктів та об'єктів критичної інформаційної структури, аналітики відносять до кібероперації, як форми деструктивного впливу на кіберпростір в умовах кібервійни. У Стратегії підкреслено, що кібератаки російської федерації спрямовані, насамперед, на інформаційно-комунікаційні системи державних органів України та об'єкти критичної інформаційної інфраструктури з метою виведення їх з ладу (кібердиверсія), отримання прихованого доступу і контролю, здійснення розвідувальної та розвідувально-підривної діяльності [2]. З повідомлення пресслужби Держспецзв'язку, в 2024 році кількість кібератак на Україну зросла на 70%, досягнувши 4315 інцидентів, у порівнянні з 2541 роком раніше. Найчастіше атакам піддаються енергетичний сектор, урядові установи, органи безпеки та інформаційно-комунікаційні системи, спостерігалася тенденція до зростання атак на критичну інфраструктуру, особливо в енергетиці. Отже, кіберпростір залишатиметься гарячою точкою війни [26].

Сутнісною ознакою кібервійни та дієвим інструментом збройного протиборства в кіберпросторі вважається кіберзброя. Використання державами озброєння, яке функціонує в межах кіберпростору для спричинення деструктивного впливу на реальний світ, відносять до суттєвих ознак кібервійни [10, с. 609]. У цьому контексті, можна частково погодитись з визначенням кібервійни – як значних, масштабних, цілеспрямованих та систематичних кібератак із застосуванням кіберзброї, здійснюваних збройними силами та/або спеціальними підрозділами держави проти суверенітету, територіальної цілісності, незалежності іншої держави та міжнародного миру і стабільності [22, с. 30]. Одним з перших прикладів застосування кіберзброї, визначається вірус Stuxnet, який у 2010 році заразив програмне забезпечення щонайменше 14 промислових об'єктів в Ірані, зокрема завод зі збагачення урану. Першим комп'ютерним вірусом, застосованим проти України у 2014 році експерти називають руткіт "Uroburos". Докладний аналіз особливостей кібератак на державні установи та об'єкти критичної інфраструктури України з початком повномасштабного військового вторгнення в країну, здійснено у праці [27].

За своєю сутністю, *"кіберзброя"* – це певний комп'ютерний код, програма, що призначена для цілеспрямованого заподіяння шкоди інформаційним, комунікаційним, технологічним системам в умовах воєнно-політичного і економічного протистояння суб'єктів міжнародних відносин. Існують різноманітні підходи до визначення поняття "кіберзброя". Так, можна частково погодитись з визначенням кіберзброї, як найрізноманітніших технічних та програмних засобів, спрямованих на експлуатацію вразливостей у системах передачі та обробки інформації або програмно-технічних системах [22]. Але в наведеному визначенні відсутня базова ознака, що вказує на можливість застосування означених цифрових засобів як *вражаючого фактору*, що застосовується у *воєнних цілях*. Більш повною є дефініція кіберзброї як технічно-технологічного комплексу, що складається зі спеціального комп'ютерного обладнання, технологій та програм, призначених для цілеспрямованого порушення роботи інформаційно-технічних систем, викривлення, пошкодження, заволодіння або знищення критично важливої інформації, що може призвести до катастрофічних наслідків техногенного характеру [28, с. 45].

До особливостей кіберзброї, що впливають на її поширення відносять такі [4], [28], [29]:

– надзвичайна швидкість проведення кібератак;

– складність ідентифікації і встановлення джерела кібератаки; раптовість, несподіваність і прихованість початку кібератаки;

– дистанційна необмеженість кібератаки;

– невисока вартість виробництва кіберзброї;

– можливість застосування з мінімальним рівнем ризику;

– ефективність застосування за умов використання противником операційно-технологічної інфраструктури та АСУ;

– перспективи використання кіберзброї в комплексі з технологіями штучного інтелекту;

– різноманітність методів застосування.

Останнім часом, кіберзброя стала розглядатись як зброя першого удару. *До видів кіберзброї відносять такі* [4], [12], [28], [29]:

– шкідливе програмне забезпечення та внесення змін в налаштуваннях системи (Malware) – віруси, трояни, черв'яки, програми-вимагачі, які проникають у системи для викрадення або знищення даних;

– експлойти: програми або коди, що використовують вразливості в програмному забезпеченні;

– руткіти: програми, що приховують присутність шкідливого ПЗ в системі;

– засоби фішингу, що імітують повідомлення з метою викрадення особистих даних; інструменти для кібератак типу "відмова в обслуговуванні" (DDoS – Distributed Denial of Service), що перевантажують ресурси системи, роблячи її недоступною для користувачів;

– віруси типу Flame, зомбімережі.

На підставі аналізу джерел, узагальнення ідеї та підходів, авторами запропоновано уточнене визначення, а саме*: "кіберзброя*" – це сукупність технічних пристроїв і програмних засобів, призначених для цілеспрямованого застосування у стратегічних і воєнних цілях, шляхом порушення роботи систем передачі та обробки інформації, операційно-технологічних, інформаційно-технічних систем, критичної інформаційної інфраструктури, електронних комунікацій та систем управління силами безпеки і оборони держави.

Основними цілями застосування кіберзброї, за матеріалами аналітичних досліджень, є критична інфраструктура:

– енергетичні системи, транспорт, зв'язок;

– фінансові установи: банки та фінансові організації;

– державні установи;

– складові сил безпеки і оборони.

Але найбільш уразливою складовою національного кіберпростору в умовах кібервійни, вважають критичну інформаційну інфраструктуру [1], [2], [27], [31], [32]. Правові та організаційні засади створення та функціювання національної системи захисту критичної інфраструктури, визначено у Законах України [1], [33], [34]. Згідно із Законом України "Про критичну інфраструктуру", до об'єктів критичної інфраструктури відносять об'єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких, може завдати шкоди життєво важливим національним інтересам [33]. Віднесення об'єктів до критичної інфраструктури та формування Реєстру об'єктів критичної інфраструктури здійснюється відповідно до Закону України "Про критичну інфраструктуру" [33]. Під час дії воєнного стану, а також протягом 12 місяців після його припинення чи скасування, повноваження уповноваженого органу у сфері захисту критичної інфраструктури України, здійснюються Державною службою спеціального зв'язку та захисту інформації України [34]. Розроблення нормативно-правових актів з незалежного аудиту інформаційної безпеки на об'єктах

критичної інфраструктури здійснюється на основі міжнародних стандартів, стандартів Європейського Союзу та НАТО [1].

До суттєвих ознак кібервійни також відносять системне застосування кібервійськ однією державою проти іншої держави або групи держав. Про роль готовності до ведення військових дій в кіберпросторі свідчить факт створення в США та інших розвинених країнах кіберкомандування, кібервійськ і кіберпідрозділів. Однією з перших держав у світі, у якій на базі Агентства національної безпеки в 2009 році було створено Кіберкомандування (USCYBERCOM) є США [30]. Керівництво Євросоюзу розпочало обговорення створення європейських кіберсил, що будуть мати наступальні можливості. Німеччина планує створити окремий рід військ – кіберсили, щоб швидше реагувати на нові загрози та посилити свою кібероборону. Китай завершує реформу кіберсил, створивши у квітні 2024 року Сили інформаційної підтримки [4, с. 9]. У Стратегії кібербезпеки України, також, зауважено необхідність забезпечення розвитку підрозділів з повноваженнями ведення збройного протиборства в кіберпросторі як основи дієвої кібероборони [2]. З цією метою утворено центри і підрозділи забезпечення кібербезпеки в державних органах України [2].

До інших ознак кібервійни, поряд із зазначеними, відносять такі:

– визначеність стратегічних і військових цілей; спрямованість проти держави або інших суб'єктів міжнародних відносин [18, с.19];

– системний, комплексний, скоординований характер організації кіберзаходів [2];

– спрямованість кібератак на інформаційно-комунікаційні системи державних органів та об'єкти критичної інформаційної інфраструктури [2];

– розвідувально-підривна діяльність у кіберпросторі [2].

Отже, вивчення наукових джерел, присвячених аналізу російсько-українського протистояння у кіберпросторі, дозволяє узагальнити перелік *сутнісних ознак кібервійни,* а саме:

– сторонами кібервійни можуть бути держави, коаліції або інші суб'єкти міжнародних відносин;

– основними цілями у кібервійні мають бути державні стратегічні та військові об'єкти, фінансові установи, критична інфраструктура країни;

– основним засобом у кібервійні є комплексне, скоординоване в часі і просторі, застосування різноманітних видів кіберзброї;

– базовою формою застосування кіберзброї є цілеспрямована кібератака, як елемент кібероперації;

– залучення до превентивних кібероперацій кібервійськ і кіберпідрозділів; комплексний і системний характер організації кіберзаходів;

– організація превентивної кібероборони як протидії деструктивному впливу на кіберпростір у формах кібершпигунства, кібердиверсій, кібертероризму і кіберзлочинності.

Узагальнення і систематизація базових ознак кібервійни надає можливість уточнити розуміння її *сутності* – як способу розв'язання геополітичних і соціально-економічних протиріч між суб'єктами міжнародних відносин, завдяки масштабному застосуванню кіберзброї та інших форм деструктивного впливу на кіберпростір держави противника. Також пропонується розгорнуте або змістовне визначення: *"кібервійна"* – це організоване і тривале зіткнення держав та інших суб'єктів міжнародних відносин у кіберпросторі із застосуванням кіберзброї та залученням кіберсил з метою досягнення геополітичних, стратегічних і воєнних цілей, що характеризується масштабним і руйнівним впливом на життєво важливі процеси суспільства і держави.

На підставі наведеної аргументації, з'ясовано змістовну сторону кібервійни, що *визначається складом і функціями структурних компонентів організації активної упереджувальної протидії у кібервійні, якими є:* національні, регіональні та глобальні або міжнародні інтереси в сфері забезпечення захисту кіберпростору; національні, колективні і міжнародні суб'єкти забезпечення кібербезпеки, їх функції та відповідальність; об'єкти

кіберзахисту; виклики та небезпеки в глобальному кіберпросторі, кіберзагрози національним інтересам та їх джерела; методи, організаційні форми, технологічні способи і технічні засоби забезпечення кібербезпеки; сили кіберзахисту, активного протиборства у кіберпросторі та підготовка фахівців з кібербезпеки; стратегічні та оперативні цілі протидії у кібервійні та очікувані результати; нормативно-правова база організації активної протидії у кібервійні.

Вивчення теоретичних джерел, у яких розкриваються змістовні аспекти кібервійни, дозволяє відокремити дві взаємопов'язаних групи основних форм впливу на кіберпростір в умовах кібервійни. З одного боку, це акти кібертероризму та кібердиверсій, розвідувально-підривна діяльність у кіберпросторі, кібершпигунство і кіберзлочини, що застосовуються проти державних інститутів влади, оборони і безпеки. З іншого боку, – форми активного протиборства у кіберпростор [1], [2], [4]:

– кіберрозвідка; кіберстримування;

– дієва кібероборона, попередження та активна протидія агресії та кіберзлочинам у кіберпросторі.

Розуміння змістовного боку кібервійни поглиблюється внаслідок розгляду *аспектів кібервійни* як чинників, що зумовлюють організацію адекватної протидії у кібервійні, а саме:

– політологічний аспект, що визначає зумовленість цілей кібервійни, політичними інтересами національних і міжнародних суб'єктів та характеризує кібервійну, як інструмент політичного протиборства в кіберпросторі [23];

– правовий аспект, якій характеризує зв'язок організаційно-правового і нормативного забезпечення протидії у кібервійні, нормами міжнародного і національного права, правовими угодами з захисту кіберпростору [19], [22], [24], [25];

– воєнний аспект, що визначає обумовленість стратегічних цілей кібервійни воєнною доктриною та стратегією держави або альянсу [2], [24], [35];

– економічний аспект, якій визначає залежність економічних ресурсів і потужностей, застосованих у кібервійні, від економічних можливостей держави й характеризує кібервійну, як чинник економічного протиборства в кіберпросторі [12], [24];

– професійно-освітній аспект, як зумовленість ефективної протидії у кібервійні можливостями держави у забезпеченні кібервійськ фахівцями [36];

– технологічний аспект, що відображує зумовленість кібервійни розвитком телекомунікаційних технологій та можливостями виробництва засобів протидії у кібервійні, зокрема кіберзброї [2];

– зовнішньополітичний аспект, якій обумовлює потенційні можливості протидії у кібервійні, розвитком міжнародного співробітництва в галузі інформаційних технологій та кібербезпеки [2], [4], [24].

Узагальнюючи наведені положення, до складу чинників безпечного функціонування національного сегменту кіберпростору в умовах кібервійни, доцільно віднести наступні: наявність кіберпотенціалу протиборства і протидії розвідувально-підривній діяльності у кіберпросторі, стримування кіберзлочинності, кібертероризму та інших кіберзагроз; дієва кібероборона на підставі застосування кіберпідрозділів з повноваженнями ведення збройного протиборства в кіберпросторі та ефективної взаємодії основних суб'єктів національної системи кібербезпеки та сил оборони; кіберстійкість, захищеність і кіберготовність національної критичної інформаційної інфраструктури; кіберсуверенітет – правова захищеність усталеного функціонування кіберпростору на національних та міжнародних правових засадах; розвиток міжнародного співробітництва щодо обміну досвідом активної протидії в кіберпросторі в умовах кібервійни; забезпеченість кадрових потреб фахівцями з кібербезпеки з врахуванням досвіду підготовки, отриманому в умовах кібервійни [1], [2], [12], [14], [24], [25].

Висновки. Узагальнюючи аналіз кібервійни як системного виклику кібербезпеці України, необхідно відзначити, що питання надійного захисту національного кіберпростору та організації ефективної системної протидії у кібервійни, постає одним з пріоритетних

чинників забезпечення національної безпеки України та залежить від адекватного розуміння структурних і функціональних параметрів захисту національного кіберпростору, спричинених кібервійною. Враховуючи системний вплив кібервійни на всебічне забезпечення кібербезпеки та організацію кіберзахисту, доцільно зауважити потребу в залученні знань про особливості забезпечення кібербезпеки і захисту національного кіберпростору в умовах кібервійни, в систему підготовки фахівців з кібербезпеки. Подальша розробка науково-теоретичних і освітніх питань щодо захисту національного кіберпростору в умовах кібервійни, має бути одним з пріоритетних завдань наукової та освітньої діяльності на шляху всебічного забезпечення кібербезпеки України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Верховна Рада України. (2017, Жовт. 5). *Закон № 2163-VIII. Про основні засади кібербезпеки України.* [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/2163-19#top. Дата звернення: Січ. 10, 2025.

[2] Президент України. (2021, Трав. 14). *Указ № 447/2021, Про рішення Ради національної безпеки і оборони України "Про Стратегію кібербезпеки України"*. [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/447/2021#n12. Дата звернення: Січ. 10, 2025.

[3] О. Потій, "Кібербезпека залишається такою самою ареною бойових дій, як і інші домени", *Держспецзв'язку*. [Електронний ресурс]. Доступно: https://cip.gov.ua/ua/news/oleksandr-potii-kiberbezpeka-zalishayetsya-takoyu-samoyu-arenoyu-boiovikh-dii-yak-i-inshi-domeni. Дата звернення: Січ. 10, 2025.

[4] РНБО України. (2025, Січ. 09). *Річний аналітичний огляд: ключові події, тенденції та виклики у сфері кібербезпеки у 2024 році*. [Електронний ресурс]. Доступно: https://www.rnbo.gov.ua/ua/Diialnist/7095.html. Дата звернення: Січ. 10, 2025.

[5] J. Arcvilly, and D. Rothfeldt, "Cyberwar is Coming*", In Athena's Camp: Preparing for Conflict in the Information Age, RAND/MR-880-OSD/RC,* 1997. [Online]. Available: https://www.rand.org/pubs/reprints/RP223.html. Accessed on: Jan. 10, 2025.

[6] M. Libicki, "Cyber Deterrence and Cyber Warfare", *RAND Corporation,* 2009. [Online]. Available: https://www.rand.org/pubs/monographs/MG877.html#document-details. Accessed on: Jan. 10, 2025.

[7] R. Clarke, and R. Knake, *Cyber War: The Next Threat to National Security and What to Do*. Glasgow, UK: Harper Collins, 2010. [Online]. Available: https://books.google.com.ua/books/about/Cyber_War.html?id=rNRlR4RGkecC&redir_esc=y Accessed on: Jan. 10, 2025.

[8] J. Carr, *Inside Cyber Warfare*, Sebastopol, CA, USA: O'Reilly Media, Inc., 2012. [Online]. Available: https://books.google.com.ua/books/about/Inside_Cyber_Warfare.html?id=nFP9wrNmGhcC&redir_esc=y. Accessed on: Jan. 10, 2025.

[9] E. Filiol, "Operational Aspects of a Cyberattack: Intelligence, Planning and Conduct", in *Cyberwar and Information Warfare*, D. Ventre, Ed. London, UK: Wiley Online Library, pp. 245-284, 2013, doi: https://doi.org/10.1002/9781118603482.ch5.

[10] B. Raboin, "Corresponding Evolution: International Law and the Emergence of Cyber Warfare", *Journal of the National Association of Administrative Law Judiciary*, pp. 81-99, 2011. [Online]. Available: https://digitalcommons.pepperdine.edu/naalj/vol31/iss2/5. Accessed on: Jan. 10, 2025.

[11] O. Buxton, "Cyber Warfare: Types, Examples, and How to Stay Safe", *Academy*, 2023. [Online]. Available: https://www.avast.com/c-cyber-warfare. Accessed on: Jan. 10, 2025.

[12] Ю. Когут, "Кібервійна та безпека об'єктів критичної інфраструктури", 2-ге видання. Київ, Україна: Сідкон. 2024. [Електронний ресурс]. Доступно: https://nashformat.ua/products/ebook-kibervijna-ta-bezpeka-ob-ektiv-krytychnoi-infrastruktury-629032?srsltid=AfmBOor0cXRP2XUE4VrxwfkTvPik5wBBsMQxUkOhI_njh9RS1zUjUw9c. Дата звернення: Січ. 10, 2025.

[13] M. Buchyn, and Y. Kurus, "Information war and its particularities at the contemporary stage", *Humanitarian visions*, vol. 4, iss. 2, pp. 1-6, 2018, doi: https://doi.org/10.23939/shv2018.02.001.

[14] V. Horlynskyi, and B. Horlynskyi, "Constitution of national cyber space and its educational significance for cyber security professionals", *Information Technology and Security*, vol. 11, iss. 1, pp. 69-83, 2023, doi: https://doi.org/10.20535/2411-1031.2023.11.1.283710.

[15] United Nations, (2018, Dec. 22). Resolution adopted by the General Assembly 73/266 "*Advancing responsible State behaviour in cyberspace in the context of international security*". [Online]. Available: https://ccdcoe.org/uploads/2019/10/UN-190102-GA-Resolution-A_RES_73_266.pdf. Accessed on: Jan. 10, 2025.

[16] "Cyber Warfare", *ICRC*. [Online]. Available: https://casebook.icrc.org/highlight/cyber-warfare. Accessed on: Feb. 26, 2025.

[17] ICRC. (2019, Nov. 28). ICRC position paper. "*International Humanitarian Law and Cyber Operations during Armed Conflicts*". [Online]. Available: https://www.icrc.org/en/download/file/108983/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf. Accessed on: Jan. 10, 2025.

[18] European Treaty Series. (2001, Nov. 23). "*Convention on Cybercrime*". Budapest, no. 185. [Online]. Available: https://rm.coe.int/1680080f0b. Accessed on: Jan. 10, 2025.

[19] М. Камчатний, "Основні ознаки поняття кібервійна в сучасному міжнародному праві", *Альманах міжнародного права*, вип. 15, с. 2-22, 2017. [Електронний ресурс]. Доступно: http://nbuv.gov.ua/UJRN/amp_2017_15_4. Дата звернення: Січ. 10, 2025.

[20] Президент України. (2021, серп. 26). *Указ № 446/2021, Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про невідкладні заходи з кібероборони держави"*. [Електронний ресурс]. Доступно: https://www.president.gov.ua/documents/4462021-40009. Дата звернення: Січ. 10, 2025.

[21] Ю. Размєтаєва, "Кібервійна: загальнотеоретичні аспекти", *Вісник Академії митної служби України. Серія: Право*, № 1, с. 12-22, 2015. [Електронний ресурс]. Доступно: http://nbuv.gov.ua/UJRN/vamsup_2015_1_4. Дата звернення: Січ. 15, 2025.

[22] М. Яцишин, "Використання сили у кіберпросторі в рамках міжнародного права", *Інформація і право*, № 4 (27), с. 22-32, 2018. [Електронний ресурс]. Доступно: https://www.researchgate.net/publication/332849607_Vikoristanna_sili_u_kiberprostori_v_ramkah_miznarodnogo_prava. Дата звернення: Січ. 22, 2025.

[23] Ю. Завгородня, "Історія становлення кібервійни як складової політичного процесу", *Актуальні проблеми політики*, вип. 72, с. 42-46, 2023, doi: https://doi.org/10.32782/app.v72.2023.6.

[24] United States. Department of State. (2024, May 6). United States International Cyberspace & Digital Policy Strategy, *U.S. Department of State, An official website of the United States Government*. [Online]. Available: https://www.state.gov/united-states-international-cyberspace-and-digital-policy-strategy. Accessed on: Jan. 10, 2025.

[25] Д. Дубов, *Кіберпростір як новий вимір геополітичного суперництва: монографія*. Київ, Україна: НІСД, 2014. [Електронний ресурс]. Доступно: https://shron1.chtyvo.org.ua/Dubov_Dmytro/Kiberprostir_iak_novyi_vymir_heopolitychnoho_supernytstva.pdf. Дата звернення: Січ. 10, 2025.

[26] "CERT-UA минулого року опрацювала 4315 кіберінцидентів", *Держспецзв'язку. Новини*. [Електронний ресурс]. Доступно: https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv. Дата звернення: Січ. 10, 2025.

[27] H. Bondar, "Cyber War in Ukraine and National Security Challenges: Cyber Attacks on Digital Infrastructure (Government Agencies, Critical Infrastructure and Third Sector Organizations)", *Public Administration and Regional Development*, no. 1, pp. 30-67, 2022, doi: https://doi.org/10.34132/pard2022.15.02.

[28] А. Білюга, "Кіберзброя: сучасні загрози національній безпеці та шляхи протидії", *Наука і оборона*, № 2, с. 42-49, 2021, doi: https://doi.org/10.33099/2618-1614-2021-15-2-42-49.

[29] Ю. Міхєєв, М. Павленко, та В. Лобода, "Вимоги до перспективного кіберозброєння Збройних сил України", *Системи і технології зв'язку, інформатизації та кібербезпеки*, № 6, с. 146-152, 2024. doi: https://doi.org/10.58254/viti.6.2024.11.146.

[30] Н. Ткачук, "Досвід США зі створення та розбудови кіберкомандування: уроки для України", *Інформація і право*, № 1 (48), с. 139-149, 2024, doi: https://doi.org/10.37750/2616-6798.2024.1(48).300798.

[31] Я. Мануілов, "Забезпечення кібербезпеки об'єктів критичної інфраструктури в умовах кібервійни", *Інформація і право*, № 1 (44), с. 154-157, 2023. [Електронний ресурс]. Доступно: https://ippi.org.ua/manuilov-yas-zabezpechennya-kiberbezpeki-ob%E2%80%99%D1%94ktiv-kritichnoi-infrastrukturi-v-umovakh-kiberviini-s-1. Дата звернення: Січ. 10, 2025.

[32] М. Кулешов, "Об'єкти критичної інфраструктури як об'єкт забезпечення кібербезпеки в умовах збройної агресії", *Вісник пенітенціарної асоціації України*, № 4 (22), с. 50-58, 2022, doi: https://doi.org/10.34015/2523-4552.2022.4.05.

[33] Верховна Рада України. (2021, лист. 16), *Закон № 1882. Про критичну інфраструктуру.* [Електронний ресурс]. Доступно: https://ips.ligazakon.net/document/T211882. Дата звернення: Січ. 22, 2025.

[34] Верховна Рада України. (2022, жовт. 18), *Закон № 2684-IX. Про внесення змін до деяких законів України щодо повноважень уповноваженого органу у сфері захисту критичної інфраструктури України.* [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/2684-20#Text. Дата звернення: Січ. 15, 2025.

[35] O. Zvezdova, and A. Vakalyuk, "Cyber security strategy in hybrid war", *Acta De Historia & Politica: Saeculum XXI*, no 3, pp. 82-90, 2022, doi: https://doi.org/10.26693/ahpsxxi2021-2022.03.082.

[36] V. Horlynskyi, and B. Horlynskyi, "Educational priorities of training of cyber security specialists under the conditions of the state of martial state in the state", *Information Technology and Security*, vol. 12, iss. 2 (23), pp. 268-282, 2024, doi: https://doi.org/10.20535/2411-1031.2024.12.2.31574.

Стаття надійшла до редакції 18.02.2025

REFERENCES

[1] Verkhovna Rada of Ukraine. (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, 2025.

[2] 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.

[3] O. Potii, "Cybersecurity remains a crucial battleground, just like other domains", *SSSCIP. News*. [Online]. Available: https://cip.gov.ua/en/news/oleksandr-potii-kiberbezpeka-zalishayetsya-takoyu-samoyu-arenoyu-boiovikh-dii-yak-i-inshi-domeni. Accessed on: Jan. 10, 2025.

[4] NSDC of Ukraine. (2025, Jan. 09). Annual Analytical Review: Key Events, Trends, and Challenges in Cybersecurity in 2024. [Online]. Available: https://www.rnbo.gov.ua/ua/Diialnist/7095.html. Accessed on: Jan. 10, 2025.

[5] J. Arcvilly, and D. Rothfeldt, "Cyberwar is Coming*", In Athena's Camp: Preparing for Conflict in the Information Age, RAND/MR-880-OSD/RC*, 1997. [Online]. Available: https://www.rand.org/pubs/reprints/RP223.html. Accessed on: Jan. 10, 2025.

[6] M. Libicki, "Cyber Deterrence and Cyber Warfare", *RAND Corporation*, 2009. [Online]. Available: https://www.rand.org/pubs/monographs/MG877.html#document-details. Accessed on: Jan. 10, 2025.

[7] R. Clarke, and R. Knake, *Cyber War: The Next Threat to National Security and What to Do*. Glasgow, UK: Harper Collins, 2010. [Online]. Available: https://books.google.com.ua/books/about/Cyber_War.html?id=rNRlR4RGkecC&redir_esc=y Accessed on: Jan. 10, 2025.

[8] J. Carr, *Inside Cyber Warfare*, Sebastopol, CA, USA: O'Reilly Media, Inc., 2012. [Online]. Available: https://books.google.com.ua/books/about/Inside_Cyber_Warfare.html?id=nFP9wrNmGhcC&redir_esc=y. Accessed on: Jan. 10, 2025.

[9] E. Filiol, "Operational Aspects of a Cyberattack: Intelligence, Planning and Conduct", in *Cyberwar and Information Warfare*, D. Ventre, Ed. London, UK: Wiley Online Library, pp. 245-284, 2013, doi: https://doi.org/10.1002/9781118603482.ch5.

[10] B. Raboin, "Corresponding Evolution: International Law and the Emergence of Cyber Warfare", *Journal of the National Association of Administrative Law Judiciary*, pp. 81-99, 2011. [Online]. Available: https://digitalcommons.pepperdine.edu/naalj/vol31/iss2/5. Accessed on: Jan. 10, 2025.

[11] O. Buxton, "Cyber Warfare: Types, Examples, and How to Stay Safe", *Academy*, 2023. [Online]. Available: https://www.avast.com/c-cyber-warfare. Accessed on: Jan. 10, 2025.

[12] Y. Kohut, "*Cyberwarfare and the Security of Critical Infrastructure Facilities*", Kyiv, Ukraine: Sidcon, 2024. [Online]. Available: https://nashformat.ua/products/ebook-kibervijna-ta-bezpeka-ob-ektiv-krytychnoi-infrastruktury-629032?srsltid=AfmBOor0cXRP2XUE4VrxwfkTvPik5wBBsMQxUkOhI_njh9RS1zUjUw9c. Accessed on: Jan. 10, 2025..

[13] M. Buchyn, and Y. Kurus, "Information war and its particularities at the contemporary stage", *Humanitarian visions*, vol. 4, iss. 2, pp. 1-6, 2018, doi: https://doi.org/10.23939/shv2018.02.001.

[14] V. Horlynskyi, and B. Horlynskyi, "Constitution of national cyber space and its educational significance for cyber security professionals", *Information Technology and Security*, vol. 11, iss. 1, pp. 69-83, 2023, doi: https://doi.org/10.20535/2411-1031.2023.11.1.283710.

[15] United Nations, (2018, Dec. 22). Resolution adopted by the General Assembly 73/266 "*Advancing responsible State behaviour in cyberspace in the context of international security*". [Online]. Available: https://ccdcoe.org/uploads/2019/10/UN-190102-GA-Resolution-A_RES_73_266.pdf. Accessed on: Jan. 10, 2025.

[16] "Cyber Warfare", *ICRC*. [Online]. Available: https://casebook.icrc.org/highlight/cyber-warfare. Accessed on: Feb. 26, 2025.

[17] ICRC. (2019, Nov. 28). ICRC position paper. "*International Humanitarian Law and Cyber Operations during Armed Conflicts*". [Online]. Available: https://www.icrc.org/en/download/file/108983/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf. Accessed on: Jan. 10, 2025.

[18] European Treaty Series. (2001, Nov. 23). "*Convention on Cybercrime*". Budapest, no. 185. [Online]. Available: https://rm.coe.int/1680080f0b. Accessed on: Jan. 10, 2025.

[19] M. Kamchatniy, "The main features of the concept of cyberwar in contemporary international law", *Almanac of International Law*, vol. 15, pp. 12-22, 2017. [Online]. Available: http://nbuv.gov.ua/UJRN/amp_2017_15_4. Accessed on: Jan. 10, 2025.

[20] President of Ukraine. (2021, Aug. 26). *Decree № 446/2021, On the Decision of the National Security and Defense Council of Ukraine "On urgent measures for the state's cyber defense"*. [Online]. Available: https://www.president.gov.ua/documents/4462021-40009. Accessed on: Jan. 10, 2025.

[21] Yu. Razmietaieva, "Cyberwar: General Theoretical Aspects", *Bulletin of the Academy of the Customs Service of Ukraine. Series: Law*, no. 1, pp. 12-22, 2015. [Online]. Available: http://nbuv.gov.ua/UJRN/vamsup_2015_1_4. Accessed on: Jan. 15, 2025.

[22] M. Yatsyshyn, "Use of force in cyberspace within the framework of international law", *Information and law*, no. 4 (27), pp. 22-32, 2018. [Online]. Available: https://www.researchgate.net/publication/332849607_Vikoristanna_sili_u_kiberprostori_v_ramkah_miznarodnogo_prava. Accessed on: Jan. 22, 2025.

[23] Yu. Zavhorodnya, "The history of the formation of cyber war as a component of the political process", *Current issues of politics*, iss. 72, pp. 42-46, 2023. doi: https://doi.org/10.32782/app.v72.2023.6.

[24] United States. Department of State. (2024, May 6). United States International Cyberspace & Digital Policy Strategy, *U.S. Department of State, An official website of the United States Government*. [Online]. Available: https://www.state.gov/united-states-international-cyberspace-and-digital-policy-strategy. Accessed on: Jan. 10, 2025.

[25] D. Dubov, *Cyberspace as a new dimension of geopolitical rivalry: monograph*. Kyiv, Ukraine: NSRI, 2014. [Online]. Available: https://shron1.chtyvo.org.ua/Dubov_Dmytro/Kiberprostir_iak_novyi_vymir_heopolitychnoho_supernytstva.pdf. Accessed on: Jan. 10, 2025.

[26] "CERT-UA. (2025, Jan. 08). CERT-UA processed 4,315 cyber incidents last year", *St. Serv. of Spec. Com. and Inf. Prot. of Ukraine (SSSCIP). News*. [Online]. Available: https://cip.gov.ua/en/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv. Accessed on: Jan. 10, 2025.

[27] H. Bondar, "Cyber War in Ukraine and National Security Challenges: Cyber Attacks on Digital Infrastructure (Government Agencies, Critical Infrastructure and Third Sector Organizations)", *Public Administration and Regional Development*, no. 1, pp. 30-67, 2022, doi: https://doi.org/10.34132/pard2022.15.02.

[28] A. Bilyuga, "Cyberweapons: Modern Threats to National Security and Ways to Counteract", *Science and Defense*, no. 2, pp. 42-49, 2021, doi: https://doi.org/10.33099/2618-1614-2021-15-2-42-49.

[29] Y. Mikhieiev, M. Pavlenko, V. Loboda, and T. Voitko, "Requirements for advanced cyber weapons of the Armed Forces of Ukraine", *Systems and technologies of communication, informatization and cybersecurity*, no. 6, pp. 146-152, 2024, doi: https://doi.org/10.58254/viti.6.2024.11.146.

[30] N. Tkachuk, "US Experience in Creating and Developing Cyber Command: Lessons for Ukraine", *Information and Law*, no. 1 (48), pp. 139-149, 2024. doi: https://doi.org/10.37750/2616-6798.2024.1(48).300798.

[31] Ya. Manuilov, "Ensuring Cybersecurity of Critical Infrastructure Facilities in Cyberwar", *Information and Law*, no. 1 (44), pp. 154-157, 2023. [Online]. Available: https://ippi.org.ua/sites/default/files/15_25.pdf. Accessed on: Jan. 10, 2025.

[32] M. Kuleshov, "Critical infrastructure facilities as an object of ensuring cybersecurity in conditions of armed aggression", *Bulletin of the Penitentiary Association of Ukraine*, no. 4 (22), pp. 50-58, 2022. doi: https://doi.org/10.34015/2523-4552.2022.4.05.

[33] Verkhovna Rada of Ukraine. (2021, Nov. 16), *Law no. 1882. About critical infrastructure.* [Online]. Available: https://ips.ligazakon.net/document/T211882. Accessed on: Jan. 22, 2025.

[34] Verkhovna Rada of Ukraine. (2022, Okt. 18), *Law no. 2684-IX. On amendments to certain laws of Ukraine regarding the powers of the authorized body in the field of protection of critical infrastructure of Ukraine.* [Online]. Available: https://zakon.rada.gov.ua/laws/show/2684-20#Text. Accessed on: Jan. 15, 2025.

[35] O. Zvezdova, and A. Vakalyuk, "Cyber security strategy in hybrid war", *Acta De Historia & Politica: Saeculum XXI*, no 3, pp. 82-90, 2022, doi: https://doi.org/10.26693/ahpsxxi2021-2022.03.082.

[36] V. Horlynskyi, and B. Horlynskyi, "Educational priorities of training of cyber security specialists under the conditions of the state of martial state in the state", *Information Technology*

and Security, vol. 12, iss. 2 (23), pp. 268-282, 2024, doi: https://doi.org/10.20535/2411-1031.2024.12.2.31574.

VICTOR HORLYNSKYI,
BORIS HORLYNSKYI

CYBERWAR AS A SYSTEMIC CHALLENGE TO UKRAINE'S CYBERSECURITY

Based on the analysis of scientific sources and generalization of knowledge about the confrontation in global cyberspace, the basic characteristics of cyberwar have been identified, namely: the parties to cyberwar can be states, coalitions or other subjects of international relations; the main targets in cyberwar are state strategic and military facilities, financial institutions, and the country's critical infrastructure; the main means of cyberwar is the complex, coordinated in time and space, use of various types of cyberweapons; the basic form of using cyberweapons as an element of a cyberoperation is a cyberattack; the involvement of cyber troops and cyber units in preventive cyberoperations; the organization of preventive cyberdefense as a counteraction to the destructive impact on cyberspace in the forms of cyberespionage, cybersabotage, cyberterrorism, and cybercrime. The proposed understanding of the essence of cyberwar as a way of resolving geopolitical and socio-economic contradictions between subjects of international relations with the complex use of cyberweapons and other forms of destructive influence on cyberspace is revealed. The substantive side of cyberwar, which is determined by the composition and functions of the structural components of the organization of preventive active counteraction in cyberwar, is revealed. The factors of the functioning of the national segment of cyberspace in the conditions of cyberwar are substantiated, namely:

– the presence of cyber potential for confrontation in cyberspace, deterrence of cybercrime, cyberterrorism and other cyberthreats;

– effective cyber defense based on the use of cyber units with the authority to conduct confrontation in cyberspace and effective interaction of the main subjects of the national cybersecurity system and defense forces;

– cyber resilience, security and cyber readiness of national critical infrastructure;

– national cyber sovereignty – legal security of the established functioning of cyberspace on national and international legal principles;

– the presence of the state's professional and educational potential – ensuring the personnel needs of cyber troops with cybersecurity specialists.

Keywords: cybersecurity, cyberwar, cyberdefense, cyberweapons, cyberspace, cyberpotential, cyberdefense, cyberforces.

Горлинський Віктор Вікторович, кандидат філософських наук, доцент, провідний науковий співробітник Науково-дослідного центру, 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, заступник начальника Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації, Київ, Україна, ORCID 0000-0002-9993-2427, vjzgoxnf@gmail.com.

Horlynskyi Viktor, candidate of philosophical sciences (Ph.D), associate professor, a leading researcher of the Scientific Research Center, Institute of special communications and information protection, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.

Horlynskyi Borys, candidate of technical sciences, deputy head of the State scientific and research institute of cybersecurity technologies and information protection, Kyiv, Ukraine.