DOI: **10.33099/2311-7249/2024-51-3-41-50**

УДК: [004.01/.08+004.49+004.62+004.78]:001.4

Горгуленко Владислав Андрійович

Центральний науково-дослідний інститут Збройних Сил України, Київ, Україна

ВІЙСЬКОВО-ТЕОРЕТИЧНЕ ОБҐРУНТУВАННЯ РЕКОМЕНДАЦІЙ СТОСОВНО РОЗВИТКУ ТЕРМІНОЛОГІЧНОГО АПАРАТУ В СФЕРІ КІБЕРБОРОТЬБИ

Метою статті є розроблення рекомендацій стосовно розвитку термінологічного апарату у сфері кіберборотьби у напрямі його уніфікації, систематизації, ієрархізації, а також забезпечення єдності теорії та практики для врегулювання й унормування положень низки нормативно-правових актів і профільних керівних документів. Під час проведення дослідження було використано наукові методи аналізу документації, критичного аналізу, порівняння та систематизації. Методом аналізу документації було досліджено основні положення нормативно-правових актів у сфері кіберборотьби. За допомогою методу критичного аналізу було виявлено низку системних невідповідностей термінологічного апарату у сфері кіберборотьби, які не дають змоги однозначно трактувати, описувати та класифікувати дії у кіберпросторі, та, як наслідок, і оцінювати їх ефективність. Користуючись методом порівняння – отримано суперечності термінологічного апарату. Відповідно, методом систематизації було розроблено рекомендації стосовно розвитку термінологічного апарату у сфері кіберборотьби. Зміст запропонованих рекомендацій зводиться до введення понять «кібердомен» та «кіберпротиборство» із відповідними дефініціями, а також уточнення визначень термінів «кіберборотьба», «кібердії», «кібервплив» та «кіберрозвідка». У статті було вперше окреслено межі застосування кіберпростору для ведення воєнних дій (протиборства) у ньому шляхом введення у науковий обіг поняття терміну «кібердомен» та розкриття його фізичного змісту, а також термінологічно розмежовано кіберборотьбу, що ведеться державами постійно як у мирний час, так і під час воєнного конфлікту завдяки запропонованому терміну «кіберпротиборство». Удосконалення та подальшого розвитку набули дефініції термінів «кіберборотьба», «кібердії», «кібервплив» та «кіберрозвідка». Теоретичною значущістю результатів дослідження є те, що удосконалений термінологічний апарат у сфері кіберборотьби відкриває шлях до оцінювання ефективності її ведення із достатнім рівнем адекватності, так як необхідною є відповідність показників та критеріїв ефективності положенням термінологічного апарату. Практична значущість результатів дослідження полягає у можливості внесення необхідних змін у низку нормативно-правових актів та профільних керівних документів на основі запропонованих рекомендацій стосовно розвитку термінологічного апарату у сфері кіберборотьби. Адже саме усталена та, головне, обґрунтована термінологія дає змогу чітко окреслити межі об'єкта та предмета досліджень, відкриває шлях до системного їх проведення, а також унеможливлює підміну понять термінів у нормативно-правових актах та галузевих керівних документах. Особливої актуальності отримані результати дослідження набувають в умовах реальної можливості утворення Кіберсил як окремого роду сил Збройних Сил України. Чіткість у формулюванні (визначенні) завдань і повноважень цього військового формування є надзвичайно важливою для забезпечення його ефективності.

Ключові слова: *кібербезпека, кіберпростір, кіберборотьба, кібердомен, кіберпротиборство, кіберзахист, кіберрозвідка, кібервплив.*

Вступ

Постановка проблеми. Кожна сфера суспільних відносин передбачає оперування певним набором понять термінів об'єктивної дійсності, які притаманні саме для неї або знаходяться на перетині з іншими сферами. Наукові поняття позначаються (іменуються) термінами, а їхня сутність розкривається у дефініціях (визначеннях). У своїй сукупності терміни та дефініції наукових понять формують термінологічний апарат (терміносистему, термінологію) у відповідній сфері. Одним із ключових та основоположних індикаторів ступеня розвитку та розробленості певної наукової сфери є інтегральний рівень термінологізації її понять, адже саме усталена та, головне, обґрунтована термінологія дає змогу чітко окреслити межі об'єкта та предмета досліджень, відкриває шлях до системного їх проведення, а також унеможливлює підміну понять термінів у нормативно-правових актах та галузевих керівних документах. Серед часткових, здебільшого якісних, показників рівня термінологізації можна виокремити: повноту (відсутність не позначених термінами наукових понять у сфері); точність (чіткість та однозначність дефініцій наукових понять, неможливість їх подвійного трактування); необхідність і достатність (дефініція має повною мірою передавати сутність наукового поняття, і водночас бути не надлишковою); не має існувати декількох

термінів, що позначають одне і те ж поняття; ієрархічність (нормативно-правові акти нижчого рівня можуть доповнювати, але не заперечувати термінології вищого рівня) та ін. За цими показниками можливо визначити актуальний стан термінологічного апарату конкретної наукової сфери й ті його елементи, які потребують розвитку (уточнення, уніфікації, оновлення тощо), у випадку їх наявності.

Під час проведення авторського наукового дослідження спрямованого на підвищення ефективності кіберборотьби в інтересах застосування угруповань військ (сил), а саме в ході узагальнення досвіду її ведення у воєнних конфліктах сучасності, керуючись вище наведеними показниками, було виявлено низку системних невідповідностей у термінологічному апараті цієї сфери, які не дають змогу однозначно трактувати, описувати та класифікувати дії у кіберпросторі, а як наслідок і оцінювати їх ефективність [1]. Сьогодні є не виділеними межі застосування кіберпростору у воєнних цілях [2]. Всупереч провідному методологічному науковому доробку у сфері кібербезпеки [3], який доводить, що складовими елементами кіберборотьби є кіберзахист, кіберрозвідка та кібервплив, сформований системою нормативно-правових актів і керівних документів термінологічний апарат не дає змогу так стверджувати в офіційних документах. Взаємозв'язок понять кібероборони, ведення якої відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» від 05 жовтня 2017 року № 2163-VIII [4] покладається на Міністерство оборони України (далі – МО України) та Генеральний штаб Збройних Сил України (далі – ГШ ЗС України) і кіберборотьби, для підготовки та планування якої, у структурі останнього функціонує відповідний орган військового управління (далі – ОВУ), також не знайшов свого місця у терміносистемі, що досліджується. Окрім цього, враховуючи постійний характер ведення кіберборотьби [1; 5; 6], питання розмежування понять та категоріювання воєнних дій у кіберпросторі, що відбуваються в мирний час від тих, що проводяться за єдиним замислом та планом під час воєнного конфлікту теж залишається відкритим. Суперечливість термінології кіберборотьби є одним із ключових факторів, що впливають на набуття та підтримання ЗС України спроможностей із ведення протиборства у кіберпросторі [7]. Отже, невідповідність наявного термінологічного апарату вимогам сьогодення потребує науково обґрунтованого нормативно-правового врегулювання. Слід зазначити, що особливої актуальності дослідженню анонсоване створення Кіберсил як окремого роду сил ЗС України. Чіткість у формулюванні (визначенні) завдань і повноважень цього військового формування є надзвичайно важливою для забезпечення його ефективності.

Аналіз останніх досліджень і публікацій. Сьогодні питання нормативно-правового, понятійно-категоріального та термінологічного унормування кіберпростору і дій у ньому, зокрема кіберборотьби, привертають значну увагу як вітчизняних, так і зарубіжних науковців та активно досліджуються у різних галузях знань. З огляду на те, що кожна країна має власне законодавство, більшість із таких наукових праць спрямовані на розвиток та удосконалення термінологічного апарату відповідного політичного утворення. У розрізі цього, актуальними публікаціями можна вважати ті, що опубліковані після набрання чинності Законом України «Про основні засади забезпечення кібербезпеки України» [4] у 2017 році, а особливо актуальними – після введення в дію Стратегії воєнної безпеки України [8], Стратегії кібербезпеки України [9] та Стратегічного оборонного бюлетеня України (далі – СОБ України) [10] у 2021 році.

Працю [11] можна виділити як таку, що є однією із основоположних за напрямом розвитку термінології у кібер сфері. Автори підійшли системно до з'ясування дефініційних проблем кібербезпеки та кібероборони: влучно відмітили, що наразі відсутній перелік вичерпних заходів щодо підготовки до відбиття та відбиття воєнної агресії у кіберпросторі; вказали на необхідність корегування законодавчо визначеної дефініції кібероборони та низки інших понять; запропонували алгоритм формування множини семантичних аналітичних і синтетичних визначень термінологічної системи сфери кібербезпеки та кібероборони.

У дослідженні [2] вперше означено досі не вирішену проблему ототожнення завдань з кібербезпеки, кіберзахисту та кібероборони, що є неправомірним ні по суті, ні по змісту. Підмічено розмивання відповідальності між складовими Сектору безпеки і оборони України за кібероборону в умовах наявної парадигми. Цілковито погоджуємося із запропонованим автором підходом, за яким завдання як з підготовки до відбиття воєнної агресії у кіберпросторі, так і ведення воєнних дій у ньому мають бути покладені саме на ЗС України. Подібного висновку щодо різного змісту понять кібероборони, кібербезпеки та кіберзахисту отримано і в [12]. Окрім цього, колектив авторів констатував нормативно-правову невизначеність структури, складу, об'єктів, а також функцій і завдань суб'єктів системи кібероборони України.

Питання сутності кіберпростору та його взаємозв'язку з кібернетичним простором було піднято в [13]. Долучаємося до твердження автора про неоднозначність дефініцій понять, що позначаються термінами із префіксом «кібер», яка призводить їх до вільного та, іноді, недоречного використання. Висновок щодо концептуальної розбіжності сутностей понять кіберпростору та кібернетичного простору є обґрунтованим та беззаперечним, підтверджує необхідність зміни в керівних документах ЗС України низки термінів, таких як «кібернетичні дії», «кібернетична операція» тощо на відповідні з коренем «кібер». Враховуючи безпосередній вплив якості підготовки персоналу на спроможності ЗС України із ведення протиборства у кіберпросторі [7], актуальним є дослідження [14], в

якому розкрито особливості сучасного понятійно-термінологічного апарату у сфері підготовки фахівців з кібербезпеки.

Нагальність нормативно-правового та термінологічного унормування кібероборони та, зокрема сутності процесу ведення воєнних дій у кіберпросторі, у контексті ймовірного формування Кіберсил як окремого роду сил ЗС України підтверджується і результатами дослідження [15]. Окремим завданням, яке потребує детального розгляду в подальших дослідженнях є термінологічне та нормативно-правове врегулювання поняття кіберзброї, вивченню проявів якої у сьогоденні присвячено статтю [16].

Окремими недоліками деяких наукових праць за тематикою дослідження є те, що вони хоч і торкаються проблематики нормативно-правового та термінологічного врегулювання сфер кібербезпеки, кібероборони та кіберборотьби, втім несуть здебільшого констатуючий характер, містять надто багато прямих цитувань з офіційних державних актів та/або галузевих керівних документів, не надаючи водночас, дієвих пропозицій до покращення (удосконалення, розвитку) ситуації, що склалася. До прикладу, заключна частина [17] висвітлює загальновідомі стратегічні завдання зі Стратегії кібербезпеки України [9].

Отже, питання нормативно-правового, понятійно-категоріального та термінологічного унормування кіберпростору і дій у ньому активно досліджується науковцями в технічній, військовій і правничій наукових сферах. Втім, питанню розвитку термінологічного апарату у сфері кіберборотьби у напрямі його уніфікації, систематизації, ієрархізації, а також забезпечення єдності теорії та практики, наразі, достатньої уваги не надається.

Мета статті. Розробити рекомендації щодо розвитку термінологічного апарату у сфері кіберборотьби.

Виклад основного матеріалу дослідження

Існуючий термінологічний апарат у сфері кіберборотьби сформувався в результаті синтезу термінів та дефініцій понять з низки профільних нормативно-правових актів державного рівня та керівних документів ЗС України, як основного носія спроможностей із ведення протиборства у кіберпросторі.

Основним законодавчим актом у сфері забезпечення кібербезпеки держави є Закон України «Про основні засади забезпечення кібербезпеки України». У ньому змістовно надано визначення таким ключовим термінам як «кібербезпека», «кіберпростір», «кібероборона», «кіберінцидент», «кібератака», «об'єкт критичної інформаційної інфраструктури», «кіберзагроза», «активна протидія агресії у кіберпросторі», «кіберзахист», «кіберрозвідка» та іншим, втім не вказано на їх ієрархічність, не наділено визначену термінологію ознаками системності, а поняття «кібервплив», яке усталено використовується у науковому обігу галузі кібербезпеки на одному рівні з двома останніми із перелічених, у документі не фігурує. Цей нормативно-правовий акт детермінує основні цілі, напрями та принципи державної політики у сфері кібербезпеки, правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі [4]. Таке формулювання преамбули слабко корелюється із положеннями Закону України «Про національну безпеку України» від 21 червня 2018 р. №2469-VIII, згідно з яким «національні інтереси України» визначаються як життєво важливі інтереси людини, суспільства і держави. Відтак, національні інтереси України у кіберпросторі є поняттям вищого рівня, яке агрегує в собі життєво важливі інтереси людини і громадянина у цифровій сфері. Відповідно, це виключає потребу в додатковому перерахуванні інтересів людини та громадянина окремо, оскільки вони включені до дефініції ширшого терміну «національні інтереси у кіберпросторі».

Склад, повноваження (завдання) та координація діяльності суб'єктів національної системи забезпечення кібербезпеки також є прерогативою Закону України «Про основні засади забезпечення кібербезпеки України» [4]. Згідно з ним, підготовка держави до відбиття воєнної агресії у кіберпросторі (кібероборона) покладена саме на МО України та ГШ ЗС України (відповідно до компетенції). Водночас, поняття відбиття воєнної агресії у кіберпросторі є нормативно невизначеним, а кібероборона розглядається як сукупність заходів, зокрема і військових, які здійснюються в кіберпросторі з метою захисту суверенітету та обороноздатності держави, відсічі збройній агресії. Визначеним є поняття активної протидії агресії у кіберпросторі, втім це завдання покладається на Державну службу спеціального зв'язку та захисту інформації України. Така парадигма продукує низку взаємозалежних запитань. А саме, чи мав законодавець під відбиттям воєнної агресії у кіберпросторі на увазі виконання військових заходів з кібероборони? Якщо так, то МО України та ГШ ЗС України несуть відповідальність лише за військові заходи з кібероборони держави (перелік яких також не визначено). Якщо ж ні, то виникає наступне запитання: чи мають МО України та ГШ ЗС України спроможності з реалізації, наприклад, політичних, економічних, соціальних та правових заходів із кібероборони? Відповідей на ці запитання наразі не існує.

Стратегія воєнної безпеки України одним із заходів всеохоплюючої оборони України, з-поміж інших, виділяє «протидію в кіберпросторі» [8]. Втім такий термін дослівно не підпадає ні під «активну протидію агресії у кіберпросторі», ні під «відбиття воєнної агресії у кіберпросторі», які розглядалися вище. Зазначений нормативно-правовий акт ототожнює поняття кібербезпеки, кіберзахисту та кібероборони, ставлячи заданням «розвиток спроможностей щодо забезпечення кібербезпеки, кіберзахисту та кібероборони», адже законодавчий акт вищого рівня [4] чітко встановлює, що кібербезпека це, в першу чергу, стан захищеності, тоді

як кібероборона та кіберзахист є процесами. До того ж, у Стратегії [8] одним із завдань є «відбиття агресії в кіберпросторі» (не воєнної, як у Законі України [4]).

Іншим вкрай важливим для сфери кіберборотьби нормативно-правовим актом Президента України є Указ, яким введено в дію СОБ України [10]. На відміну від Стратегії воєнної безпеки України, невідповідності якої аналізувалися вище, СОБ України дає визначення низці понять у сфері кіберборотьби, а також визначає перелік необхідних для набуття та підтримання спроможностей із ведення протиборства в інформаційному та кіберпросторі. Повертаючись до попередньо піднятої проблеми невизначеності сутності поняття «відбиття воєнної агресії у кіберпросторі», СОБ України надає дефініцію поняття «воєнної агресії у кіберпросторі», зміст якого несе в собі виключно військові заходи: масштабні дій проти України в кіберпросторі, залучення кіберпідрозділів військових формувань, використання кіберозброєння та ін. Можна припустити, що для відбиття такої агресії необхідними є також військові заходи (оборонного характеру), які з огляду на своє призначення, повинні виконувати ЗС України. Таке припущення підтверджується і визначеною у СОБ України спроможністю зі стримування та відсічі збройної агресії в кіберпросторі, одним із носіїв якої є ЗС України. Саме цей нормативно-правовий акт містить в собі поняття кіберборотьби та визначає її як сукупність взаємоузгоджених за метою, завданнями, місцем та часом заходів визначених військ (сил), спрямованих на здобуття інформації про кіберінфраструктуру противника, її знищення всіма видами зброї або захоплення (виведення з ладу, отримання контролю), заподіяння їй шкоди шляхом здійснення кібердій, проведення кібероперацій та радіоелектронного подавлення, захист своєї кіберінфраструктури від кіберрозвідки та кібердій противника. На одному рівні із поняттям кіберборотьби в документі надано визначення термінам «дії в кіберпросторі» та «кібердії», втім їх взаємозв'язку із поняттям кіберборотьби не сформовано: «дії в кіберпросторі» є сукупністю заходів із захисту власного кіберпростору, впливу на кіберпросторі та дії противника, а «кібердії» – організованим застосуванням визначених сил і засобів для здійснення впливу на кіберпростір противника або на захист власного кіберпростору. Окрім цього, формулювання деяких спроможностей щодо ведення протиборства у кіберпросторі містять в собі термін «кібервплив», втім дефініції йому як СОБ України, так і Закон України [4] не надають.

Стратегія кібербезпеки України [9] констатує визнання кіберпростору одним із можливих театрів воєнних дій, а одним із завдань покладає утворення у системі Міністерства оборони України кібервійськ та забезпечення їх належними фінансовими, кадровими та технічними ресурсами для стримування збройної агресії у кіберпросторі та надання відсічі агресору. Зазначений документ свідчить про недосконаліть нормативно-правового забезпечення кібербезпеки, усувати яку пропонує шляхом розроблення проєктів нормативно-правових актів, нормативних документів та стандартів у цій сфері із залучення на регулярній основі представників, зокрема з наукових установ, чим додатково підкреслює актуальність цього дослідження.

Профільними керівними документами ЗС України у сфері кіберборотьби також надано терміни та визначення цілої низки понять. Причому, деякі з них доповнюють, певні дублюють, а кілька – суперечать положенням нормативно-правових актів державного рівня, які розглядалися вище. А саме,

надано дефініції таких понять, як «кібервплив», «кіберзасіб», «кіберконтрзаходи», «кіберпротидія», «кіберудар»;

практично повністю продубльовано визначення понять «кібердії» та «кіберборотьба»;

дефініції понять кібератаки, кібердорозвідки, кіберзброї та кіберпростору різняться (суперечать) нормативно-правовим актам вищого рівня.

Дефініція поняття кібервпливу, як одного з основних складових елементів кіберборотьби, яка надана керівними документами ЗС України, на наш погляд, не відповідає сутності. Визначене формулювання більшою мірою стосується результатів кібервпливу (ефекту дії), а не суті, мети та способів його нанесення. «Кіберзасіб» та «кіберзброя», відповідно до наданих визначень, можуть застосовуватися лише під час здійснення кібератаки.

Разючу суперечність термінологічного апарату створює поняття кібератаки, яка в керівних документах ЗС України трактується як несанкціоновані дії, а визначена Законом України [4] дефініція цього поняття чітко класифікує його як спрямовані (навмисні) дії в кіберпросторі.

Аналогічним чином, у СОБ України «кібердорозвідка» є діяльністю щодо виявлення вразливостей, а керівні документи ЗС України стверджують, що це збір інформації щодо вразливостей. Тобто, згідно нормативно-правового акту вищого рівня результати кібердорозвідки мають характер першоджерела про вразливості кіберінфраструктури противника, а згідно керівного документу нижчого рівня – лише узагальнення інформації про неї, отриманої на одному із попередніх кроків. Втім, найбільш значну та системну невідповідність термінологічного апарату у сфері кіберборотьби провокує неоднозначність поняття кіберпростору як середовища її ведення, нормативно-правове врегулювання якого, на наше переконання, є ключем до цілісного вирішення проблеми за означеною темою дослідження.

Кіберпростір (згідно з Законом України [4]) – це 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. Така дефініція описує кіберпростір та його використання, в більшій мірі, у цивільних цілях. Водночас, СОБ

України визначає перелік необхідних для набуття спроможностей складових сил оборони із ведення протиборства у кіберпросторі. Втім, жодним законодавчим актом України кіберпростір не визначений, як середовище ведення оборонних дій для забезпечення захисту суверенітету держави [11].

Керівні ж документи ЗС України у сфері кіберборотьби дають цілком іншу дефініцію поняття кіберпростору – глобальний домен, що складається з усіх взаємопов'язаних комунікацій, інформаційних технологій та інших електронних систем, мереж та їх даних, у тому числі відокремлених або незалежних, які обробляються, зберігаються або передаються. Таке визначення середовища ведення кіберборотьби, хоча і дещо відрізняється, проте корелюється із доктриною «Cyberspace Operations» США [18], яка також стверджує, що кіберпростір є глобальним доменом. Цей доктринальний документ США також свідчить про те, що кіберпростір входить до складу інформаційного середовища (простору). Водночас, профільний керівний документ ЗС України за сферою кіберборотьби у дефініції кіберпростору оперує поняттями, які не відповідають основоположному Закону України з кібербезпеки [4]. Так, у визначенні використовуються словосполучення «взаємопов'язані комунікації» та «електронні системи» замість усталеного поняття «систем електронних комунікацій (комунікаційних систем)», замість «мереж передачі даних» – «мереж та їх даних» тощо.

Для нормативно-правового поля України, в якому положення нормативно-правового акту вищого рівня є переважаючими одночасне існування двох дефініцій терміну «кіберпростір» є неприпустимим.

Як керівні документи у сфері кіберборотьби ЗС України, так і доктринальна база США стверджують, що кіберпростір є глобальним доменом. Концепція мультидоменних операцій (МДО) передбачає об'єднане застосування спроможностей збройних сил та інших складових сил оборони з метою завоювання переваги, її утримання та створення сприятливих умов для досягнення поставлених цілей та мети операції, розгрому противника, консолідації здобутків. МДО військ (сил) базуються на раціональному застосуванні сил та засобів з усіх доменів для досягнення мети операції з найменшими втратами особового складу, озброєння та військової техніки, а також витратами ресурсів в кожному з них [19]. Сама сутність доменів бойового простору (середовища), зокрема домену ведення кіберборотьби, є вужчою наданої в [4] дефініції поняття кіберпростору. Доменом є сфера операційного середовища, яка має фізичні характеристики, що вимагають унікальних доктрин, організацій та обладнання для ефективного застосування збройних сил під час проведення військових операцій [20]. Тому необхідною є конкретизація та виділення середовища ведення протиборства у кіберпросторі на нормативно-правовому рівні. Це поняття пропонуємо іменувати як «кібердомен».

Як феномен, кібердомен виник у результаті розвитку комп'ютерних інформаційних технологій до рівня, за якого останні стали підґрунтям та основою сталого функціонування об'єктів критичної інформаційної інфраструктури, національних електронних інформаційних ресурсів, систем управління технологічними процесами, систем електронних комунікацій, інформаційних систем військового призначення та автоматизованих систем управління військами (зброєю). Фізичний зміст кібердомену схематично зображений автором (зображення у схему взято із мережі Інтернет) на рис. 1.

Рисунок 1 – Фізичний зміст поняття кібердомену

Кібердомен існує в межах кіберпростору. Кібербезпека, як стан захисщеності життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якого забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища (інформаційного простору), досягається у взаємодії та зусиллями суб'єктів національної системи кібербезпеки України. Умовою такого стану захищеності є підготовка та ведення кібероборони кіберпростору України, як складової інформаційного простору [10], а безпосереднє відбиття воєнної агресії у кіберпросторі (виконання військових заходів з кібероборони) у формі ведення протиборства у кіберпросторі (кіберборотьби) здійснюється у кібердомені – сегменті кіберпростору, середовищі ведення воєнних дій у ньому.

Як було попередньо зазначено, для ЗС України та інших складових сил оборони визначені необхідні для набуття та підтримання спроможності із ведення протиборства у кіберпросторі, а в структурі ГШ ЗС України функціонує ОВУ (Головне управління радіоелектронної та кіберборотьби) призначений, зокрема, для організації виконання завдань щодо планування кібероборони України, планування та ведення кіберборотьби. Взаємозв'язку, співвідношення та ієрархічності понять кібероборони та кіберборотьби в жодному з розглянутих попередньо нормативно-правових актів та керівних документів не сформульовано. Можемо лише припустити, що визначене Законом України [4] завдання щодо відбиття воєнної агресії у кіберпросторі, яке покладено на МО України та ГШ ЗС України означає виконання виключно військових заходів із кібероборони. На основі детального аналізу сучасного стану термінологічного апарату було отримано логічного висновку, що саме поняття кіберборотьби повинно бути зафіксовано нормативно-правовим чином як безпосереднє виконання ЗС України військових заходів із кібероборони держави у кібердомені. Як наслідок, врегулювання також потребують дефініції таких термінів, як «дії у кіберпросторі» та «кібердії», які сьогодні де-факто позначають одне і те ж поняття.

Сутність кіберборотьби включає в себе: по-перше, постійний захист власної кіберінфраструктури, який проводиться постійно, а також активний захист – у разі нанесення противником кібервпливу; розвідку кіберінфраструктури противника на наявність її вразливостей; вплив (ураження, знищення) кіберінфраструктури противника. Втім, дефініції понять кіберзахисту, кіберрозвіки та кібервпливу не вказують на їх приналежність до кіберборотьби. До того ж, визначення кіберрозвідки [4] детермінує її ведення виключно розвідувальними органами України.Як було попередньо зазначено, для ЗС України та інших складових сил оборони визначені необхідні для набуття та підтримання спроможності із ведення протиборства у кіберпросторі, а в структурі ГШ ЗС України функціонує ОВУ (Головне управління радіоелектронної та кіберборотьби) призначений, зокрема, для організації виконання завдань щодо планування кібероборони України, планування та ведення кіберборотьби. Взаємозв'язку, співвідношення та ієрархічності понять кібероборони та кіберборотьби в жодному з розглянутих попередньо нормативно-правових актів та керівних документів не сформульовано. Можемо лише припустити, що визначене Законом України [4] завдання щодо відбиття воєнної агресії у кіберпросторі, яке покладено на МО України та ГШ ЗС України означає виконання виключно військових заходів із кібероборони. На основі детального аналізу сучасного стану термінологічного апарату було отримано логічного висновку, що саме поняття кіберборотьби повинно бути зафіксовано нормативно-правовим чином як безпосереднє виконання ЗС України військових заходів із кібероборони держави у кібердомені. Як наслідок, врегулювання також потребують дефініції таких термінів, як «дії у кіберпросторі» та «кібердії», які сьогодні де-факто позначають одне і те ж поняття.

Сутність кіберборотьби включає в себе: по-перше, постійний захист власної кіберінфраструктури, який проводиться постійно, а також активний захист – у разі нанесення противником кібервпливу; розвідку кіберінфраструктури противника на наявність її вразливостей; вплив (ураження, знищення) кіберінфраструктури противника. Втім, дефініції понять кіберзахисту, кіберрозвіки та кібервпливу не вказують на їх приналежність до кіберборотьби. До того ж, визначення кіберрозвідки [4] детермінує її ведення виключно розвідувальними органами України. Окрім цього, результати аналізу та узагальнення передового досвіду ведення кіберборотьби у воєнних конфліктах сучасності та російсько-української війни зокрема свідчать про те, що кіберборотьба ведеться державами постійно як у мирний час, так і під час вирішення непереборних міждержавних суперечностей збройним шляхом [1]. Кіберборотьба, що ведеться державами (блоками держав) під час війни чи збройного конфлікту переростає у кіберпротиборство, якому притаманна двосторонність, послідовність, зв'язок із операціями військ (сил) в інших доменах та ін.

Отже, пропонуються такі рекомендації щодо розвитку термінологічного апарату у сфері кіберборотьби в напрямі його структуризації, уніфікації, ієрархізації, а також забезпечення єдності теорії та практики:

1. Ввести термін «кібердомен», і надати йому дефініцію – домен бойового простору, який фізично сегментом кіберпростору, середовищем ведення в ньому та/або через нього воєнних дій силами та засобами кіберборотьби, сфера розповсюдження якого охоплює системи електронних комунікацій військового призначення, системи управління технологічними процесами та інші інформаційні системи об'єктів критичної інфраструктури держави.

2. Внести зміни до визначення терміну «кіберборотьба» на основі того, що кіберборотьба, враховуючи фізичну сутність середовища її ведення, не може бути узгодженою за місцем у класичному значенні цього слова – вона може узгоджуватися за місцем у кібердомені; ведення кіберборотьби може здійснюватися силами та засобами кіберборотьби (не усіма видами зброї, як визначено у [10]); кіберборотьба містить заходи з кіберзахисту, кіберрозвідки та кібервпливу; радіоелектронне

подавлення здійснюється силами та засобами радіоелектронної боротьби, тобто не є елементом кіберборотьби; також, досвід кіберборотьби свідчить, що вона ведеться державами постійно як у мирний час, так і під час дії воєнного стану (війни). Тому, пропонується надати терміну «кіберборотьба» визначення такого змісту – процес виконання ЗС України військових заходів з кібероборони як сукупності взаємоузгоджених і пов'язаних за метою, завданнями, місцем у кібердомені та часом дій з кіберрозвідки інформаційної та кіберінфраструктури противника, її ураження та/або знищення шляхом нанесення кібервпливу, кіберзахисту власної інформаційної та кіберінфраструктури, а також інших кібердій призначених для відбиття (відсічі) воєнної агресії у кіберпросторі, які здійснюються силами та засобами кіберборотьби як у мирний час, так і під час воєнного конфлікту в операціях або окремо. Тобто, поняття кібероборони та кіберборотьби, на наше переконання, мають співвідноситися між собою як загальне та часткове.

3. Для створення ієрархічності понять дій в кіберпросторі, кіберборотьби та кібердій, пропонуємо викласти визначення терміну «кібердії» у такому вигляді – організоване ведення дій у кібердомені (як сегменті кіберпростору) визначеними силами і засобами у межах операції сил оборони або окремо для здійснення впливу на кіберпростір противника, розвідки його кіберінфраструктури або захисту власного кіберпростору.

4. Кібервплив – це сукупність взаємоузгоджених і пов'язаних за метою, завданнями, місцем у кібердомені та часом кібердій (кібератак, кіберударів, демонстраційних та превентивних кібердій), які проводяться силами та засобами кіберборотьби для ураження, виведення з ладу та знищення інформаційної та кіберінфраструктури противника або окремих її елементів.

5. Згідно із Законом України [4] «кіберрозвідка» є діяльністю, що здійснюється розвідувальними органами у кіберпросторі або з його використанням. Така дефініція дає змогу класифікувати будь-яку діяльність розвідувальних органів у кіберпросторі як кіберрозвідку, що з досвіду ведення російсько-українського кіберпротиборства не відповідає дійсності. Також, таке визначення породжує невідповідність із СОБ України [10], згідно з яким завдання щодо кіберрозвідки покладаються не лише на розвідувальні органи, а й на ЗС України та інші складові сил оборони. Керівні документи ЗС України надають таке визначення цьому терміну: кіберрозвідка – це збір оперативної розвідувальної інформації за допомогою комп'ютерних мереж з метою отримання даних про цілі в автоматизованих системах управління, системах зв'язку і управління зброєю, інформаційно-телекомунікаційних мережах і системах противника.

Пропонуємо доопрацювати обидва варіанти визначення терміну «кіберрозвідка», узагальнити їх, звести до одного та викласти у такій редакції: кіберрозвідка – це сукупність взаємоузгоджених і пов'язаних за метою, завданнями, місцем у кібердомені та часом кібердій, які проводяться силами та засобами кіберборотьби для перехоплення даних, отримання несанкціонованого доступу до систем електронних комунікацій противника, виявлення вразливостей його інформаційної та кіберінфраструктури, заволодіння розвідувальною інформацією в інтересах застосування сил оборони держави, а також виявлення і визначення ступеня зовнішніх загроз національній безпеці України у кіберпросторі.

6. Ввести термін «кіберпротиборство» та надати йому таке визначення – процес двостороннього ведення кіберборотьби між державами (блоками держав), які перебувають у стані війни або збройного конфлікту.

Питання пов'язані з нормативно-правовим врегулюванням понять кіберзброї, кіберозброєння та загалом кіберзасобів, терміни та дефініції яких сьогодні вже існують у термінологічному апараті потребують детального розгляду під час подальших досліджень, сфокусованих саме на цьому напрямі. Розроблені рекомендації щодо розвитку термінологічного апарату у сфері кіберборотьби (ведення воєнних дій у кібердомені) відображено автором на рис. 2.

Висновки й перспективи подальших досліджень

Отже, у статті за допомогою критичного аналізу, порівняння та узагальнення положень низки нормативно-правових актів та профільних керівних документів ЗС України було детально вивчено сучасний стан термінологічного апарату у сфері кіберборотьби, виявлено низку його системних невідповідностей, які не дають змоги однозначно трактувати, описувати та класифікувати дії у кіберпросторі, а, як наслідок, і оцінювати їх ефективність. Для вирішення цієї проблемної ситуації автором розроблено рекомендації стосовно розвитку термінологічного апарату у сфері кіберборотьби у напрямі його систематизації ієрархізації, уніфікації, а також забезпечення єдності (відповідності) теорії практиці. Зміст запропонованих рекомендацій зводиться до введення понять «кібердомен» та «кіберпротиборство», а також видозміні дефініцій понять «кіберборотьби», «кібердій», «кібервпливу» та «кіберрозвідки». Окрім цього, вважаємо, що саме кіберборотьба (не кібернетичні / кібер дії) має стати однією з форм воєнних (бойових) дій у системі застосування сил оборони держави.

Водночас, погоджуємося з тим, що надані рекомендації не є останньою інстанцією, а запропоновані автором терміни та їхні дефініції можуть не бути остаточною версією, однак вони передають те змістовне навантаження, обґрунтування якого і було основним завданням цього дослідження. Приведення останніх до стану, за якого вони будуть придатними до внесення у відповідні нормативно-правові акти та профільні керівні документи вимагає спільної діяльності науковців за військовою, технічною та правничою галузями у межах, принаймні, науково-дослідної роботи. Унормування термінологічного апарату у сфері кіберборотьби відкриває шлях до адекватного оцінювання ефективності її ведення в операціях або окремо, адже необхідною є відповідність показників та критеріїв ефективності положенням термінологічного апарату.

ISSN 2311-7249 (Print) / ISSN 2410-7336 (Online) Сучасні інформаційні технології у сфері безпеки та оборони № 3(51)/2024

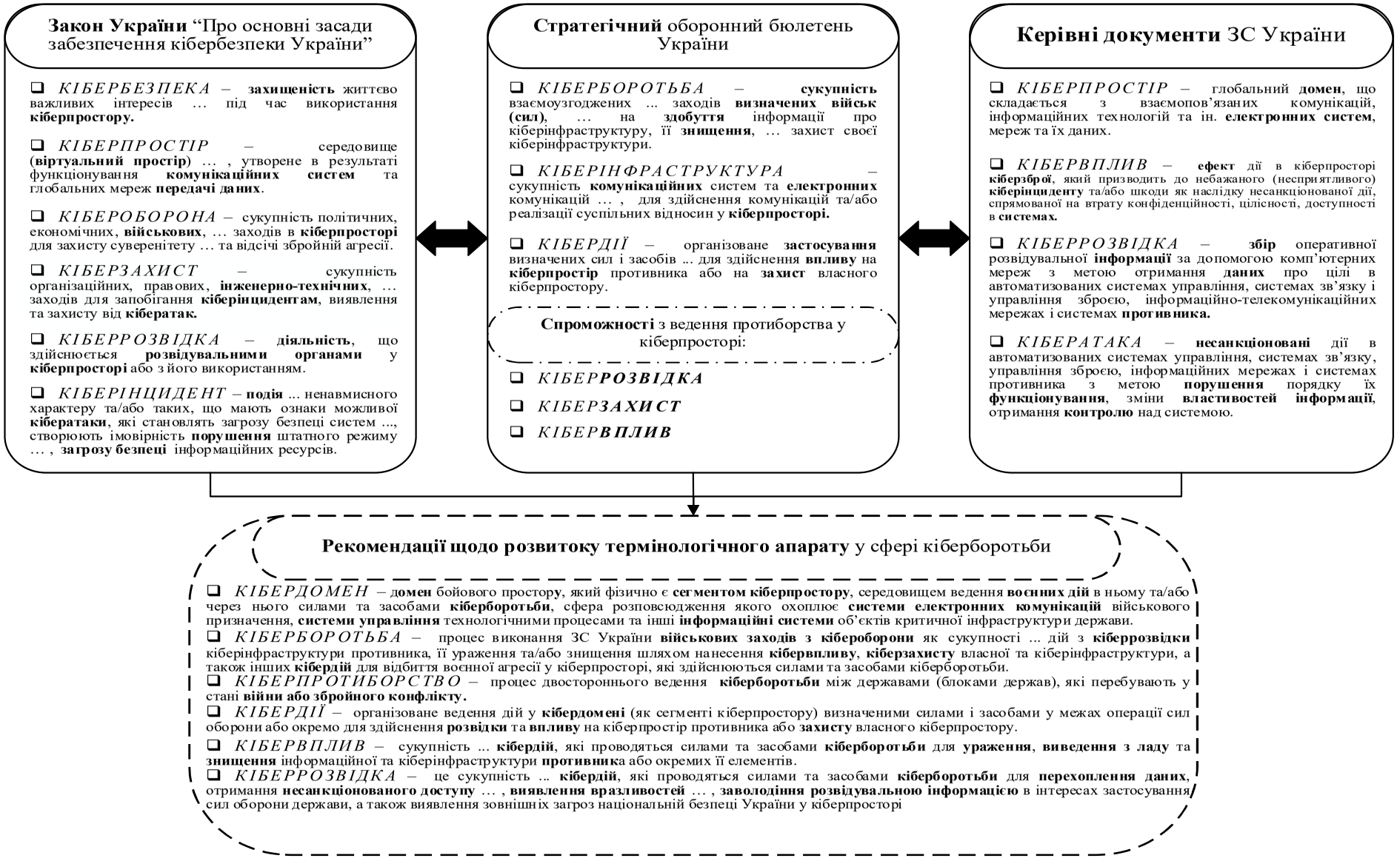

Рисунок 2 – Рекомендації щодо розвитку термінологічного апарату у сфері кіберборотьби (ведення воєнних дій у кібердомені)

Розроблення системи показників та критеріїв оцінювання ефективності кіберборотьби, а також математичної моделі її ведення і є перспективами подальших досліджень за цим напрямом. Питання нормативно-правового унормування термінологічного апарату за напрямом кіберзброї, а також врегулювання розподілу завдань і повноважень сил оборони держави із ведення протиборства у кіберпросторі потребують проведення окремих досліджень.

Список бібліографічних посилань

1. Горгуленко В. А. Кіберборотьба у воєнних конфліктах сучасності: передовий досвід, тенденції та закономірності розвитку. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2024. № 2 (50). С. 11–28. DOI: 10.33099/2311-7249/2024-50-2-11-28. **2. Грищук Р. В.** Дії в кіберпросторі як асиметрична відповідь на «гібридну» агресію росії. *Уроки збройної агресії росії проти України – воєнно-стратегічні аспекти* : зб. матеріалів міжв. наук-практ. конф., м. Київ, 29 квітня 2021 р. Київ : Національний університет оборони України імені Івана Черняховського, 2021. С. 204–209. **3. Грищук Р. В., Даник Ю. Г.** Основи кібернетичної безпеки: монографія. Житомир: ЖНАЕУ, 2016. 636 с. **4. Про основні засади забезпечення кібербезпеки України** : Закон України від 05.10.2017 № 2163-VIII : станом на 28 черв. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 12.11.2024). **5. Машталір В. В., Гук О. М., Мурасов Р. К., Фараон С. І., Лоза В. В.** Кіберборотьба в умовах збройного протистояння: аналіз, стратегії та виклики. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2024. № 1 (49). С. 93–104. DOI: 10.33099/2311-7249/2024-49-1-93-104. **6. Машталір В. В., Гук О. М., Толмачов В. І., Фараон С. І.** Прогнозування ступеню кібервпливу на гетерогенні інформаційні системи військового призначення з урахуванням його еволюції. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2023. № 3 (48). С. 147–156. DOI: 10.33099/2311-7249/2023-48-3-147-156. **7. Горгуленко В. А.** Фактори, що впливають на спроможності Збройних Сил України у кібердомені. *Військові інновації у сучасних війнах*. Зб. тез доповідей міжнародного академічного форуму. (Київ, 18–19 квіт. 2024 р.). Київ. 7БЦ. 2024. С. 157–158. **8. Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року "Про Стратегію воєнної безпеки України"** : Указ Президента України від 25.03.2021 №121/2021. URL: https://zakon.rada.gov.ua/laws/ show/121/2021#Text (дата звернення: 17.11.2024). **9. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»** : Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/ 2021#Text (дата звернення: 17.11.2024). **10. Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року «Про Стратегічний оборонний бюлетень України»** : Указ Президента України від 17.09.2021 № 473/2021. URL: https://zakon.rada.gov.ua/laws/show/ 473/2021#Text (дата звернення: 17.11.2024). **11. Вдовенко С. Г, Даник Ю. Г, Фараон С. І.** Дефініційні проблеми термінології у сфері кібербезпеки і кібероборони та шляхи їх вирішення. *Комп'ютерні науки та кібербезпека.* 2019. № 1 (13). С. 17–29. DOI: 10.26565/2519-2310-2019-1-02. **12. Терновий О. В., Шкуренко О. М., Міненко Л. М.** Проблемні аспекти кібероборони: місце та роль кіберзахисту в Збройних силах України. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2023. № 1 (46). С. 23–31. DOI: 10.33099/2311-7249/2023-46-1-23-31. **13. Сніцаренко П. М., Саричев Ю. О., Гордійчук В. В.** Сутність кіберпростору та його взаємозв'язок із кібернетичним простором. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2024. № 2 (50). С. 5–10. DOI: 10.33099/2311-7249/2024-50-2-5-10. **14. Горліченко С. О.** Особливості сучасного понятійно-термінологічного апарату у сфері підготовки фахівців з кібербезпеки. *Кібербезпека: освіта, наука, техніка*. 2024. № 3 (24). С. 171–181. DOI: 10.28925/2663-4023.2024.23.171181. **15. Федієнко О. П.** Сучасні тенденції нормативного забезпечення інституційного формування кібервійськ (кіберсил): досвід деяких країн НАТО. *Інформація і право*. 2024. № 1 (48). С. 150–161. DOI: 10.37750/2616-6798.2024.1(48).300800. **16. Алексєєва О. А.** Кіберзброя: поняття, її прояви та заходи протидії. *Інформація і право*. 2024. № 3 (50). С. 162–169. DOI: 10.37750/2616-6798.2024.3(50).311720. **17. Скіцько О. І., Ширшов Р. А.** Нормативно-правове забезпечення кібероборони України: сучасний стан. *Юридичний вісник*. 2024. № 3. С. 244–250. DOI: 10.32782/yuv.v3.2024.29. **18. Joint Publication 3-12 "Cyberspace Operations".** J7 Directorate for Joint Force Development. 2018. URL: https://irp.fas.org/doddir/dod/jp3_12.pdf (дата звернення: 15.11.2024). **19. Defense Primer: Army Multi-Domain Operations (MDO).** Congressional research service. 2024. URL: https://sgp.fas.org/crs/natsec/IF11409.pdf (дата звернення: 16.11.2024). **20. Michael P. Kreuzer**. Cyberspace is an Analogy, Not a Domain: Rethinking Domains and Layers of Warfare for the Information Age. The Strategy Bridge. 2021. URL: https://thestrategybridge.org/the-bridge/2021/7/8/cyberspace-is-an-analogy-not-a-domain-rethinking-domains-and-layers-of-warfare-for-the-information-age (дата звернення: 16.11.2024).

MILITARY-THEORETICAL JUSTIFICATION OF RECOMMENDATIONS FOR THE DEVELOPMENT OF TERMINOLOGICAL APPARATUS IN THE SPHERE OF CYBER WARFARE

Horhulenko Vladyslav

Central Research Institute of the Armed Forces of Ukraine, Kyiv, Ukraine

Formulation of the problem in general. *One of the key and fundamental indicators of the degree of a certain scientific field development is the integral level of its concepts terminologization, because it is the established and, most importantly, well-founded terminology that allows to clearly outline the boundaries of the object and subject of research, opens the way to their systematic conduction, and also makes impossible the replacement of concepts in normative legal acts and industry guidance documents. During the author's scientific research aimed at increasing the effectiveness of cyber warfare, namely during the generalization of the experience of conducting it in modern military conflicts, a number of systemic inconsistencies in the terminological apparatus of this sphere were revealed, which do not allow to unambiguously interpret, describe and classify actions in cyberspace, and as a result, to evaluate their effectiveness. The main aim of the article is to formulate the recommendations for the development of the terminological apparatus in the sphere of cyber warfare.*

Research methods. *Scientific methods of documentation analysis, critical analysis, comparison and systematization were used during the research. The main provisions of normative legal acts in the field of cyber warfare were studied by the method of documentation analysis. Using the method of critical analysis, a number of systemic inconsistencies in the terminological apparatus in the field of cyber warfare were revealed, which do not allow to unambiguously interpret, describe and classify actions in cyberspace, and as a result, to evaluate their effectiveness. Using the method of comparison, the contradictions of the terminological apparatus were obtained. Accordingly, the systematization method was used to formulate recommendations for the development of the terminological apparatus in the field of cyber warfare.*

Analysis of the latest research findings. *The issue of improving and developing the terminological apparatus directly in the field of cyber warfare, despite the challenges of modern times, is currently not given enough attention.*

Presenting the main results. *The content of the proposed recommendations consists in the introduction of the concepts of «cyber domain» and «cyber opposition» with the corresponding definitions, as well as changes in the definitions of the concepts of «cyber warfare», «cyber action», «cyber influence» and «cyber intelligence».*

An element of scientific novelty. *The article outlined for the first time the limits of the use of cyberspace for the conduct of military operations (hostilities) in it by introducing the concept of «cyber domain» into scientific use and revealing its physical content, as well as terminologically separated cyber warfare, which is constantly waged by states both in peacetime and under the time of military conflict due to the proposed term «cyber opposition». Definitions of the concepts of «cyber warfare», «cyber action», «cyber influence» and «cyber intelligence» have been improved and further developed.*

Theoretical and practical significance of the article. *The theoretical significance of the research results is that the improved terminological apparatus in the field of cyber warfare opens the way to evaluating the effectiveness of its conduct with a sufficient level of adequacy, as it is necessary to match the performance indicators and criteria with the provisions of the terminological apparatus. The practical significance of the research results lies in the possibility of making the necessary changes in a number of normative legal acts and profile guidance documents based on the proposed recommendations for the development of the terminological apparatus in the field of cyber warfare. The obtained results of the research acquire particular relevance in the conditions of the real possibility of the formation of Cyber Forces as a separate branch of the Armed Forces of Ukraine in the near future, the accuracy of the formulation (definition) of tasks and powers of which must be absolute.*

Conclusion and the perspectives of future research. *We agree that the given recommendations are not the last resort, and the terms and definitions proposed by the author may not be the final version, but they convey the content load, the justification of which was the main task of this study. Bringing the latter to a state in which they will be suitable for inclusion in the relevant normative legal acts and profile guidance documents requires the joint activity of scientists in the military, technical and legal fields within, at least, research and development work. The development of a system of indicators and effectiveness evaluation criteria of cyber warfare, as well as it's mathematical model, are the prospects of further research in this direction.*

Keywords: *cybersecurity, cyber space, cyber warfare, cyber domain, cyber opposition, cyber defense, cyber intelligence, cyber influence.*

References

1. Horhulenko, V. A., (2024). Cyber warfare in modern military conflicts: experience, trends and regularities of development. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony*. 50 (2), 11-28. DOI: 10.33099/2311-7249/2024-50-2-11-28. **2. Hryschuk, R. V.,** (2021). Actions in cyberspace as an asymmetric response to Russia's «hybrid» aggression. In: *Uroky zbrojnoi ahresii rosii proty Ukrainy – voienno-stratehichni aspekty: zb. materialiv mizhv. nauk-prakt. konf*. Kyiv, Ukraina, 29 kvitnia 2021. Kyiv: Natsional'nyj universytet oborony Ukrainy imeni Ivana Cherniakhovs'koho. **3. Hryschuk, R. V., Danyk, Yu. H.,** (2016). Fundamentals of cyber security: a monograph. Zhytomyr: ZhNAEU. **4. The official site of Verkhovna Rada of Ukraine** (2017). A law of Ukraine is «On the basic principles of cybersecurity in Ukraine" from Oct., 05. No 2163-VIII» Available at: https://zakon.rada.gov.ua/laws/show/2163-19 [Accessed: 10 November 2024]. **5. Mashtalir, V. V., Huk, O. M., Murasov, R. K., Faraon, S. I., Loza, V. V.,** (2024). Cyber warfare in armed confrontation conditions: analysis, strategies and challenges. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony*. 49 (1). 93–104. DOI: 10.33099/2311-7249/2024-49-1-93-104. **6. Mashtalir, V. V., Huk, O. M., Tolmachov, V. I., Faraon, S. I.,** (2023). Prognostication the degree of cyber influence on heterogeneous military information systems taking into account its evolution. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony*. 48 (3). 147–156. DOI: 10.33099/2311-7249/2023-48-3-147-156. **7. Horhulenko, V. A.,** (2024). Factors affecting on the capabilities of the Armed Forces of Ukraine in a cyber domain. In: *Military innovations in the contemporary warfare: zb. tez dop. mizhnar. akad. forumu*. Kyiv, Ukraina, 18–19 kvitnia 2024. Kyiv: 7BC. **8. The official site of Verkhovna Rada of Ukraine** (2021). «Decree of the President of Ukraine is "On the Military Security Strategy of Ukraine" from March, 25, 2021. 121/2021» Available at: https://zakon.rada.gov.ua/laws/show/121/2021#Text [Accessed: 05 November 2024]. **9. The official site of Verkhovna Rada of Ukraine** (2021). «Decree of the President of Ukraine is "On the Cyber Security Strategy of Ukraine" from Aug., 26, 2021. 447/2021» Available at: https://zakon.rada.gov.ua/laws/show/ 447/2021#Text [Accessed: 06 November 2024]. **10. The official site of Verkhovna Rada of Ukraine** (2021). «Decree of the President of Ukraine is "On the Strategic Defense Bulletin of Ukraine" from Sep., 17, 2021. 473/2021» Available at: https://zakon.rada.gov.ua/laws/show/473/2021#Text [Accessed: 07 November 2024]. **11. Vdovenko, S. H, Danyk, Yu. H, Faraon, S. I.,** (2019). Definitive problems of the Terms of the Sphere of Cyber security and Cyber Defense and the Ways of their solution. *Kompiuterni nauky ta kiberbezpeka*. 13 (1). 17–29. DOI: 10.26565/2519-2310-2019-1-02. **12. Ternovyi, O. V., Shkurenko, O. M., Minenko, L. M.,** (2023). Problematic aspects of cyber defense: place and role of cyber defense in the armed forces of Ukraine. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony*. 46 (1). 23–31. DOI: 10.33099/2311-7249/2023-46-1-23-31. **13. Snitsarenko, P. M., Sarychev, Yu. O., Hordiichuk, V. V.,** (2024). On the essence of cyber space and its relationship with cybernetic space. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony*. 50 (2). 5–10. DOI: 10.33099/2311-7249/2024-50-2-5-10. **14. Horlichenko, S. O.,** (2024). Features of modern conceptual and terminological apparatus in the field of training of cyber security specialists. *Kiberbezpeka: osvita, nauka, tekhnika*. 24 (3). 171–181. DOI: 10.28925/2663-4023.2024.23.171181. **15. Fediienko, O. P.,** (2024). Modern trends in regulatory support for the institutional formation of cyber forces (cyber forces): the experience of some NATO countries. *Informatsiia i pravo*. 48 (1). 150–161. DOI: 10.37750/2616-6798.2024.1(48).300800. **16. Alekseieva, O. A.,** (2024). Cyber weapon: concepts, their manifestations and countermeasures. *Informatsiia i pravo*. 50 (3). 162–169. DOI: 10.37750/2616-6798.2024.3(50).311720. **17. Skitsko, O. I., Shyrshov, R. A.,** (2024). Regulatory and legal provision of cyber defense of Ukraine: current state. *Yurydychnyi visnyk*. 3. 244–250. DOI: 10.32782/yuv.v3.2024.29. **18. Joint Publication 3-12 «Cyberspace Operations»** [online], (2018). *J7 Directorate for Joint Force Development*. Available at: https://irp.fas.org/doddir/dod/jp3_12.pdf [Accessed: 08 November 2024]. **19. Defense Primer: Army Multi-Domain Operations (MDO)** [online], (2024). *Congressional research service*. Available at: https://sgp.fas.org/crs/natsec/IF11409.pdf (Accessed: 09 November 2024). **20. Michael P. Kreuzer** [online], (2021). Cyberspace is an Analogy, Not a Domain: Rethinking Domains and Layers of Warfare for the Information Age. *The Strategy Bridge*. Available at: https://thestrategybridge.org/the-bridge/2021/7/8/cyberspace-is-an-analogy-not-a-domain-rethinking-domains-and-layers-of-warfare-for-the-information-age (Accessed: 11 November 2024).