КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (30), 2025
Спеціальний випуск ISSN 2663 – 4023
Special issue
DOI 10.28925/2663-4023.2025.30.909
УДК 355.4

Паламарчук Світлана Анатоліївна
головна наукова співробітниця науково-дослідного управління
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID: 0000-0001-7483-9165
svitlana.palamarchuk@viti.edu.ua

Паламарчук Наталія Анатоліївна
начальниця науково-дослідної лабораторії
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID: 0000-0001-8818-7794
nataliia.palamarchuk@viti.edu.ua

Штонда Роман Михайлович
доктор філософії, начальник науково-дослідного відділу
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID: 0000-0001-5986-0847
roman.shtonda@viti.edu.ua

Побережець Тетяна Василівна
наукова співробітниця науково-дослідної лабораторії
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID: 0000-0001-8007-8614
tetiana.poberezhets@viti.edu.ua

СУТНІСТЬ КІБЕРОБОРОНИ УКРАЇНИ: ВИЗНАЧЕННЯ ТА ПРОТИРІЧЧЯ ПРАВОВИХ ТА ТЕОРЕТИЧНИХ ЗАСАД

Анотація. З початком гібридної агресії рф у 2014 році, а особливо після повномасштабного вторгнення 2022 року, Україна стала об'єктом масштабних кібератак, спрямованих на критичну інфраструктуру та інформаційні системи державних інституцій. Наявна статистика кібератак підтверджує наміри рф будь-якими методами "захопити" кіберпростір України з метою досягнення стратегічної переваги у збройному конфлікті. Відповідно, завданнями України є захист власного кіберпростору та створення умов для здійснення активних дій у кіберпросторі противника. У статті досліджено сутність кібероборони України в розрізі фундаментальних визначень згідно Законів України "Про основні засади забезпечення кібербезпеки України", "Про оборону України" та відповідних нормативно-правових актів. За результатами аналізу виокремлено протиріччя теоретичних та правових засад кібероборони, наголошується на відсутності чіткого законодавчого визначення терміну "кібероборона". Підкреслюється, що жодним нормативно-правовим актом не визначені структура системи кібероборони держави, склад та завдання суб'єктів її забезпечення, а також об'єкти кібероборони. Деякі питання частково окреслено у проєкті Закону про Кіберсили Збройних Сил України, однак його положення містять розбіжності із чинним законодавством та розглядають кібероборону у "вузькому" значенні. Все зазначене ускладнює формування державної політики у сфері кібероборони, та відповідно, реалізації системи кібероборони. Акцентовано увагу на необхідності гармонізації законних та підзаконних дефініцій з позицій системного підходу, виокремлення кібероборони в окрему сферу з прийняттям базового закону "Про кібероборону України", який визначатиме засади державної політики, забезпечить гармонізацію правового поля та сприятиме реалізації стратегічних цілей держави у сфері кібероборони.

Ключові слова: захист інформації; інформаційна інфраструктура; інформаційно-комунікаційна система; кібербезпека, кіберзахист; кібероборона; кіберпростір; критична інфраструктура.

ВСТУП

В 2016 році члени Організації Північноатлантичного договору (далі – НАТО) підтвердили оборонний мандат і визнали кіберпростір операційним середовищем, в якому НАТО має захищатися так само ефективно, як у повітрі, на землі та на морі [1]. Стратегією кібербезпеки України 2021 року [2], кіберпростір, разом з іншими фізичними просторами також визнаний одним з можливих театрів воєнних дій, а "кібербезпека" – однією з найбільш актуальних та чутливих складових національної безпеки держави. Крім цього, протягом останнього десятиліття почав вживатися термін "кібероборона" з позиції, що це складова оборони держави, тоді як вона більш за все розглядається у законодавстві України про кібербезпеку.

Постановка проблеми. Системне застосування кіберзброї та наслідки кібератак Україна відчула на собі в повній мірі. Фактично з 2014 року, російська федерація вела гібридну війну проти України, з початком повномасштабного вторгнення кількість кібератак постійно росла, і більшість з них стосувалася поширення шкідливого програмного забезпечення. Сучасний досвід показав, що особливо під час збройних конфліктів, реалізуються різноманітні концепції кібератак, які призводять як до появи нових загроз витоку інформації так і порушення функціонування систем в цілому. Наявна статистика підтверджує факт того, що рф намагається будь-якими методами "захопити" кіберпростір України, коли традиційні військові дії поєднуються з цифровими атаками на військову і критичну інфраструктуру (енергетика, транспорт, системи управління, тощо), виводяться з ладу інформаційні системи, знищуються та викрадаються дані. Крім цього, деякі атаки на портали державних послуг та реєстри, перешкоджають доступу громадян до них, чим "паралізують" роботу державних інституцій на невизначений термін. При цьому, кіберпростір виступає як базована платформа забезпечення реалізації цих гібридних воєнних дій.

Створення умов для безпечного функціонування власного кіберпростору, захисту кіберпростору, формування дієвої системи кіберзахисту та в подальшому, національної системи кібероборони як ніколи є актуальними. Наразі, створення системи кібероборони України знаходиться на початковому етапі, а саме, етапі становлення нормативно-правового забезпечення та наукових дискусій, які визначають пріоритетні цілі та напрями реалізації. Досягнення належного рівня кіберборони, здатного задовольнити інтереси держави, безпосередньо і первинно залежить від якості її правових засад.

Аналіз останніх досліджень і публікацій. Питання кібероборони України є відносно новим розділом знань (вперше кібероборона згадується в Стратегії кібербезпеки України 2016 року як здійснення заходів з підготовки держави до відбиття воєнної агресії у кіберпросторі), відповідно має небагато наукових публікацій, в яких фрагментарно висвітлюються різні бачення кібероборони.

О. Скіцько та Р. Ширшов розглядали сучасний стан правового забезпечення кібероборони в Україні [3]. В. Тютюнник детально проаналізував стан, проблеми та актуальні заходи щодо забезпечення кібероборони [4]. А. Давидюк [5] порівнює компоненти кібероборони та кіберзахисту відповідно до визначень цих термінів у законодавстві та пропонує введення додаткового терміну "система активного кіберзахисту (кібероборони)". У роботах В. Савченка [6] та Ю. Даника, П. Воробієнка, В. Чернеги [7] приділено увагу загальним підходам до організації системи кібероборони держави, але лише з позиції законодавства України про кібербезпеку. О. Терновий, О. Шкуренко, Л Міненко розглядають проблемні аспекти кібероборони, а також місце та роль кіберзахисту в Збройних Силах України [8]. Також, серед існуючих праць, увагу

привертають результати П. Сніцаренко [9], [10], в яких детально розглянуто сутність кібероборони як виду воєнних дій з позиції законодавства України з питань оборони, запропонована загальнодержавна система із структурно-логічною схемою її організації, намічено основні етапи реалізації. Очевидно, що питання правових та теоретичних засад кібероборони України сьогодні є дискусійним та потребує подальших досліджень для їх становлення, а нормативно-правові акти потребують узгодженості.

Мета статті. Метою даної статті є аналіз нормативно-правових актів з кібероборони України та узагальнення правових та теоретичних засад.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Правову основу забезпечення кібероборони України становить низка нормативних документів (закони України, укази Президента України, постанови Кабінету Міністрів України), які визначають основні засади державної політики та задають напрями та цілі забезпечення оборони держави, національної безпеки, кібербезпеки, захисту інформації, тощо.

Розглянемо основні з них та деякі міркування науковців щодо сутності та інших питань кібероборони:

1) Базовим законом щодо кібероборони України є Закон України “Про основні засади забезпечення кібербезпеки України” від 05.10.2017 № 2163-VIII (зі змінами) (далі – Закон про кібербезпеку) [11]. Він визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки та ін.

Згідно Закону про кібербезпеку [11], кібероборона – сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії (рис. 1).

Рис. 1. Сутність кібероборони

Тобто кібероборона знаходить свій вираз у системі певних заходів у кіберпросторі, спрямованих на захист національної безпеки України. Водночас таке визначення не дає

чіткого розуміння щодо механізмів реалізації вказаних заходів (процесів) з кібероборони [3], [5], [6]. Більше того, на думку П. Сніцаренко [9], якщо розглядати одночасно всі варіанти визначень, що містяться в законах України, сутність кібероборони зрозуміти неможливо, а тому слід визнати, що поняття "кібероборона" в законодавстві України виписане недосконало. Це є системним недоліком, проблемою, яка перешкоджає гармонізувати практичну діяльність на шляхах побудови (створення) дієвої системи кібероборони держави.

Таке визначення, по-перше, настільки узагальнене, що не дає реального уявлення про саму сутність кібероборони в її специфічних ознакових характеристиках, а по-друге, неможливо уявити, яким чином реалізувати зазначені заходи "виключно в кіберпросторі" [9].

Разом з цим, на думку А. Давидюка [5], оскільки термін "кібероборона" почав вживатися як частина національної системи оборони, актуальним стає питання співвідношення між "кіберзахистом" та "кібероборoною" або їх поєднання (рис. 1). З метою уникнення невизначеності у цьому питанні порівняємо компоненти кібероборони та кіберзахисту відповідно до визначень цих термінів у законодавстві (рис. 2) [5].

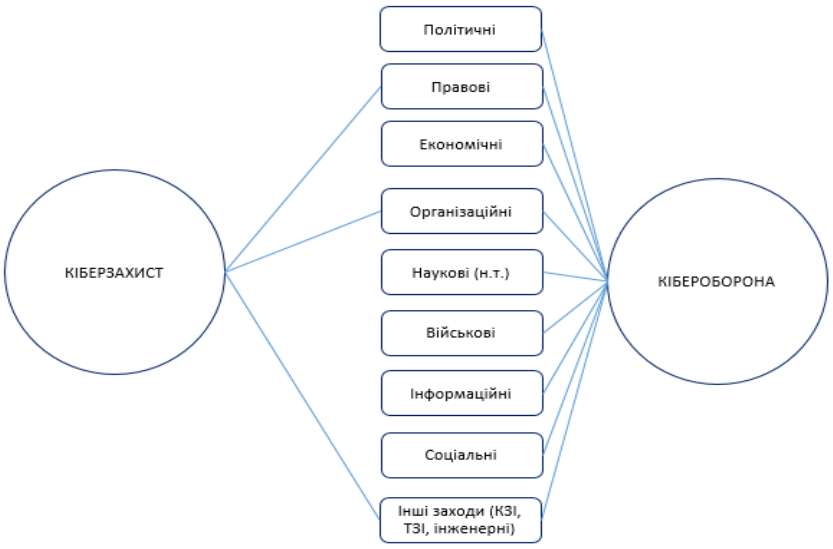

Рис. 2. Порівняння "кібероборони" та "кіберзахисту" відповідно до їх визначень

Особливістю кібероборони на відміну від кіберзахисту є наявність активної фази, де знайдені вразливості у власній системі повинні стати проекцією цілей у подібних системах противника. Таким чином, в системах критичного призначення під час війни важливою є наявність процедур моніторингу стану системи, сканування мереж на вразливості, розгортання інфраструктури хибних цілей, постійного обміну інформацією з активними силами кібероборони. Основним завданням кібероборони є забезпечення безперервності функціонування систем критичного призначення об'єктів критичної інфраструктури (далі – ОКІ) з використанням активних заходів протидії противнику.

Таке порівняння сприяє введенню додаткового терміну "система активного кіберзахисту (кібероборони)" з таким визначенням "сукупність апаратних та програмних засобів, заходів, методів та компетенцій обслуговуючого персоналу, що можуть бути задіяні як ресурс в активному кіберзахисті (кібероборoні)" [5].

Повертаючись до Закону про кібербезпеку [11], оборонні заходи входять до національної системи кібербезпеки. Національна система кібербезпеки є сукупністю

суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури (далі – ОКІ).

Основними суб'єктами національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України (далі – Міноборони) та Генеральний штаб Збройних Сил України (далі – Генштаб ЗС України) та ін., які виконують визначені завдання з кіберзахисту.

Цим же Законом про кібербезпеку [11] визначено, що Міноборони та Генштаб ЗС України "відповідно до компетенції здійснюють заходи (лише!) з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони)", що на думку П.М. Сніцаренко [9], принципово відрізняється за сутністю від наведеного вище визначення кібероборони.

2) У жовтні 2017 року до Закону України "Про оборону України" від 06.12.1991 №1932-XII (далі – Закон про оборону) [12] внесено зміни (доповнено новим абзацом) згідно Закону про кібербезпеку [11], якими встановлено, що підготовка держави до оборони в мирний час крім іншого включає обов'язковість *"здійснення заходів з кібероборони (активного кіберзахисту) для захисту суверенітету держави та забезпечення її обороноздатності, запобігання збройному конфлікту та відсічі збройній агресії (передостанній абзац статті 3), у тому числі проведення спеціальних операцій (розвідувальних, інформаційно-психологічних тощо) у кіберпросторі"*.

Звідси випливає: кібероборона – це активний кіберзахист, що є іншим варіантом розуміння сутності кібероборони [9].

Таким чином, завдання щодо здійснення заходів з кібероборони (активного кіберзахисту) з'являються в Законі про оборону в 2017 році, і покладаються на Міноборони та Генштаб ЗС України. Останній здійснює планування оборони держави, відповідно і планування кібероборони та координацію завдань між іншими суб'єктами (хоча наразі визначені лише суб'єкти кібербезпеки). Визначено, що обов'язковість здійснення таких заходів передбачена в мирний час в ході підготовки держави до оборони, проте безпосередні кроки, які необхідно робити під час протистояння збройній агресії не відображені [3].

3) Стратегія кібербезпеки України затверджена Указом Президента України від 26 серпня 2021 року № 447/2021 "Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"" (далі – Стратегія) [2]. У Стратегії визначено, що забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України, тоді як одним із пріоритетів забезпечення кібербезпеки України є убезпечення кіберпростору задля захисту суверенітету держави та розвитку суспільства.

Щодо реалізації попередньої Стратегії (затвердженої Указом Президента України від 15 березня 2016 року № 96), зазначено, що діяльність суб'єктів національної системи кібербезпеки залишається недостатньо скоординованою і такою, що спрямована на виконання лише поточних завдань. Реалізація була ускладнена відсутністю цілісного бачення (програми) розвитку спроможностей основних суб'єктів системи кібербезпеки, обмеженістю ресурсного забезпечення, відсутністю належної державної підтримки розвитку її інституційного забезпечення. Стан її реалізації за визначеними показниками не перевищує 40 відсотків.

Стратегія 2021 року визначає стратегічні цілі, що мають бути досягнуті протягом періоду її реалізації. Першою з них є стратегічна ціль С.1. Дієва кібероборона, її необхідно досягнути для формування потенціалу стримування, тобто спроможності національної системи кібербезпеки для унеможливлення збройної агресії проти України у кіберпросторі або з його використанням та ін. Для досягнення стратегічної цілі С.1 Україна сформує систему дієвої кібероборони шляхом (зокрема):

утворення у системі Міноборони кібервійськ та забезпечення їх належними фінансовими, кадровими та технічними ресурсами для стримування збройної агресії у кіберпросторі та надання відсічі агресору;

запровадження ефективних механізмів взаємодії основних суб'єктів національної системи кібербезпеки та сил оборони в частині спільного виконання завдань кібероборони;

розроблення та виконання плану кібероборони як складової частини плану оборони України;

забезпечення оцінки спроможностей суб'єктів сектору безпеки і оборони в частині спільного виконання завдань кібероборони.

Реалізація Стратегії безпосередньо здійснюється основними суб'єктами національної системи кібербезпеки, Міністерством закордонних справ України, Міністерством цифрової трансформації України, Міністерством освіти і науки України та іншими суб'єктами забезпечення кібербезпеки в межах їх компетенції.

З початком повномасштабного вторгнення рф відмічені у Стратегії виклики та загрози у сфері кібербезпеки лише збільшилися, з різних причин зберігається проблематика щодо реалізації положень Стратегії, в т.ч., і з утворенням кібервійськ, яке започатковано з 2021 року.

4) Рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про невідкладні заходи з кібероборони держави" введено в дію Указом Президента України від 26 серпня 2021 року №446/2021 (далі – Указ про невідкладні заходи з кібероборони) [13].

Згідно цього Указу, Кабінету Міністрів України доручено невідкладно здійснити розрахунки потреб щодо обсягу матеріально-технічних і фінансових ресурсів, необхідних для створення й забезпечення належного функціонування кібервійськ; їх комплектування та ін., а також у двомісячний термін розробити та внести на розгляд Верховної Ради України (далі – ВРУ) законопроект щодо створення та функціонування у системі Міноборони кібервійськ.

При цьому, проект Закону "Про Кіберсили Збройних Сил України" (далі – проект Закону про Кіберсили) [14] було зареєстровано у ВРУ у грудні 2024 року (див. п. 6).

5) Рішення Ради національної безпеки і оборони України від 20 серпня 2021 року "Про Стратегічний оборонний бюлетень України", введене в дію Указом Президента України від 17 вересня 2021 року № 473/2021 (далі – СОБ) [15].

Новий цикл оборонного планування в Україні розпочато у 2019 році. При цьому, у зазначеному СОБ відмічається, що "*…під час реалізації оборонної реформи та оборонного огляду визначено низку проблем функціонування сил оборони в умовах існуючих та потенційних загроз, зокрема:" "неспроможність ефективно реагувати на зростаючу кількість загроз у кіберпросторі*". Тому, передбачається що: "*створення системи кібероборони буде орієнтовано на набуття необхідних спроможностей суб'єктами підготовки та здійснення заходів кібероборони, створення і розвиток сил, засобів та інструментів протиборства в кіберпросторі та через кіберпростір, які*

забезпечать створення необхідного потенціалу сил оборони для відбиття воєнної агресії в кіберпросторі".

В цілому, у СОБ значна увага надавалася питанням забезпечення кібероборони держави. Даний документ оборонного планування унормував поняття воєнної агресії в кіберпросторі, дій у кіберпросторі, кіберзагроз воєнного характеру, кіберборотьби, кібердій, кібердорозвідки, кіберзброї та кіберінфраструктури. Зроблено акцент на тому, що для протидії силам і засобам противника мають бути поєднані дії, спрямовані на радіоелектронну боротьбу і протистояння в кібер- та інформаційному просторах [8].

6) Проект Закону про Кіберсили [14], Закон визначатиме правовий статус та засади діяльності Кіберсил ЗС України, на які покладається планування та проведення військових заходів кібероборони України, захист суверенітету та недоторканості України в кіберпросторі або з його використанням.

Кіберсили ЗС України є органом військового управління та головним органом з підготовки та проведення у встановленому порядку військових заходів кібероборони України. Військовими заходами кібероборони України є військові кібероперації, які плануються та проводяться в кіберпросторі або з його використанням (пункт 1 та 3 статті 1). Стримування агресії в кіберпросторі або з його використанням в мирний час та надання відсічі агресору в особливий період здійснюється Кіберсилами ЗС України згідно з планами військових кібероперацій, які затверджує Головнокомандувач ЗС України (пункт 4 статті 1).

Суттєвим у проекті Закону є те, що згідно пункту 3 статті 6 планується внести зміни до Закону про оборону" [12], а саме, доповнити новою статтею 41 такого змісту:

"Стаття 41. Національна система кібероборони

Національна система кібероборони є сукупністю суб'єктів забезпечення кібероборони та взаємопов'язаних заходів політичного, міжнародного, економічного, соціального, військового, наукового, науково-технічного, інформаційного, правового та іншого характеру, кібердипломатії, які спрямовані на запобігання виникненню збройного конфлікту та відсіч збройній агресії проти України.

Основними суб'єктами національної системи кібероборони є Міноборони, ЗС України, Державна служба спеціального транспорту, Міністерство закордонних справ України, Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Національна гвардія України, Державна прикордонна служба України, розвідувальні органи, інші центральні органи виконавчої влади відповідно до визначених повноважень.

Міноборони формує та забезпечує реалізацію державної політики у сфері кібероборони, встановлює вимоги до захисту інформації та кіберзахисту систем оборонного та військового призначення з урахуванням стандартів НАТО; у взаємодії з Генштабом ЗС України та основними суб'єктами національної системи кібероборони здійснює планування заходів щодо підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборона України)". Що привертає увагу у цьому проекті:

1) У пункті 1 статті 1 зазначено що Кіберсили ЗС України готують та проводять лише "військові заходи кібероборони України". Військовими заходами кібероборони України є військові кібероперації. Якщо звернутися до визначення "кібероборони" (див. рис. 2), то хто проводить всі інші зазначені заходи кібероборони в державі, наразі не визначено.

2) Згідно Закону про оборону [12] (щодо відсічі збройній агресії проти України) діє положення, що:

"...у разі збройної агресії проти України або загрози нападу... на підставі відповідного рішення Президента України ЗС України разом з іншими військовими формуваннями розпочинають воєнні дії, у тому числі проведення спеціальних операцій (розвідувальних, інформаційно-психологічних тощо) у кіберпросторі".

Із цього положення випливає, що ЗС України розпочинають воєнні дії (операції) в кіберпросторі лише (виключно!) в разі збройної агресії проти України або загрози нападу. Це означає, що за Законом, ведення воєнних дій (операцій) ЗС України в кіберпросторі в умовах мирного часу не передбачається [9].

3) Запропоновано внесення доповнення до Закону України "Про оборону України" (стаття 41), а саме, визначення національної системи кібероборони та суб'єктів національної системи кібероборони, що буде вперше на законодавчому рівні. Однак, у проекті Закону визначаються лише основні завдання Кіберсил ЗС України, які стосуються (лише!) планування та проведення військових заходів кібероборони. Завдання решти суб'єктів національної системи кібероборони (стаття 41) відсутні, як і відсутні в будь-яких інших нормативно-правових актах України.

4) У абзаці 3 статті 41 доповнення до Закону України "Про оборону України" зазначено що: "Міністерство оборони України формує та забезпечує реалізацію державної політики у сфері кібероборони, встановлює вимоги до захисту інформації та кіберзахисту систем оборонного та військового призначення з урахуванням стандартів НАТО; у взаємодії з Генеральним штабом Збройних Сил України та основними суб'єктами національної системи кібероборони здійснює планування заходів щодо підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборона України)".

Тоді як, у пункті 4 частини другої статті 8 Закону про кібербезпеку [11] визначено інші завдання Міноборони та Генштабу ЗС України (щодо кібероборони), це:

"здійснення заходів з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони); здійснення військової співпраці з НАТО та іншими суб'єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз".

Звідси спостерігаються розбіжності, різні тлумачення щодо завдань та компетенцій Міноборони та Генштабу ЗС України, що потребує узгодження та приведення до відповідності на законодавчому рівні, оскільки цим проектом Міноборони надаються повноваження щодо формування державної політики у сфері кібероборони, а не лише здійснення заходів з підготовки до відбиття….

5) Згідно пункту 4 статті 6 проекту Закону планується внести зміни до Закону України "Про розвідку" від 17 вересня 2020 року № 912-IX, а саме, надати Кіберсилам ЗС України повноваження на здійснення спеціальної розвідки та проведення інших спеціальних заходів в кіберпросторі або з його використанням, що є цілком логічним.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Правову основу забезпечення кібероборони становить низка нормативно-правових актів України, в статті розглянуто основні з них. Однак, наразі, більшість питань кібероборони визначені законодавством з кібербезпеки, тоді як кібероборона належить до сфери оборони держави, і державна політика мала б формуватися виходячи з цієї позиції.

За результатами аналізу правових засад, а також досліджень та публікацій на тему кібероборони, можливо зазначити, що існує ряд проблемних питань, починаючи із законодавства, самого визначення терміну "кібероборона" та її сутності), які потребують

вирішення на рівні держави. Так, згідно визначення, кібероборона знаходить свій вираз у системі певних заходів у кіберпросторі... Таке визначення, по-перше, настільки узагальнене, що не дає реального уявлення про саму сутність кібероборони в її специфічних ознакових характеристиках, а по-друге, неможливо уявити, яким чином реалізувати зазначені заходи "виключно в кіберпросторі". Слід визнати, що поняття "кібероборона" в законодавстві України виписане недосконало, що перешкоджає гармонізувати практичну діяльність на шляхах створення дієвої системи кібероборони.

Невизначеними залишаються структура системи кібероборони держави, склад та завдання суб'єктів її забезпечення, а також об'єкти кібероборони. Деякі питання частково окреслено у проєкті Закону про Кіберсили, однак його положення містять розбіжності із чинним законодавством та розглядають кібероборону у "вузькому" значенні. Загалом, проект Закону про Кіберсили не вирішує в повній мірі тих завдань, які мають бути вирішені в межах створення системи кібероборони, формування державної політики кібероборони та в подальшому, її реалізації. Відповідно, під загрозою реалізація стратегічних цілей України щодо створення дієвої кібероборони.

Тому, доцільним було б врегулювання нормативно-правового поля кібероборони держави та кібербезпеки, як окремих сфер діяльності, та в подальшому, створення системи кібероборони починаючи із ухвалення Закону України "Про кібероборону України" як базового (у якості прикладу, як то сфери кібербезпеки, захисту інформації та ін.). Більше того, поряд із наявним законодавчим забезпеченням кібероборони (нормативного та організаційного рівня), решта завдань щодо формування національної системи кібероборони знаходяться на довготривалій реалізації, наприклад, як то створення кібервійськ.

Подальші дослідження будуть направлені на аналіз міжнародних документів з кібероборони та можливості їх гармонізації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Організація Північноатлантичного договору. (2016, 8–9 липня). *Заява за результатами саміту у Варшаві.* URL: https://www.nato.int/cps/uk/natohq/official_texts_133169.htm (дата звернення: 27.08.2025)
2. Президент України. (2021, 26 серпня). *Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України № 447/2021*. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 27.08.2025)
3. Скіцько, О., & Ширшов, Р. (2024). Нормативно-правове забезпечення кібероборони України: сучасний стан. *Юридичний вісник, (3),* 244–250. https://doi.org/10.32782/yuv.v3.2024.29
4. Тютюнник, В. (2025). Кібероборона України: стан, проблеми та актуальні заходи щодо її забезпечення. *Оборонно-промисловий кур'єр.* URL: https://surl.li/tcqxwm (дата звернення: 27.08.2025)
5. Давидюк, А. В. (2022). Кіберзахист та кібероборона критичної інфраструктури. *Кібербезпека енергетики: матеріали науково-практичної конференції* (м. Київ, 27 травня 2022 р.) (с. 50–52). Київ. URL: https://is.gd/yd2rQK (дата звернення: 27.08.2025)
6. Савченко, В. А. (2023). Забезпечення стійкості кібероборони держави в умовах збройного конфлікту. *Сучасний захист інформації, 55(3),* 6–11. https://doi.org/10.31673/2409-7292.2023.030001
7. Даник, Ю., Воробієнко, П., & Чернега, В. (2019). *Основи кібербезпеки та кібероборони* (2-ге вид.). Одеса: ОНАЗ ім. О. С. Попова.
8. Терновий, О., Шкуренко, О., & Міненко, Л. (2023). Проблемні аспекти кібероборони: місце та роль кіберзахисту в Збройних силах України. *Сучасні інформаційні технології у сфері безпеки та оборони, 46(1),* 23–31. https://doi.org/10.33099/2311-7249/2023-46-1-23-31
9. Сніцаренко, П. М. (2024). Про сутність кібероборони як виду воєнних дій. *Наука і оборона, (3),* 45–54. https://doi.org/10.33099/2618-1614-2024-26-3-45-54

10. Сніцаренко, П. М. (2024). Кібероборона України як складова оборони держави. *Наука і оборона, (4),* 40–48. https://doi.org/10.33099/2618-1614-2024-27-4-40-48
11. Верховна Рада України. (2017, 5 жовтня). *Про основні засади забезпечення кібербезпеки України: Закон України № 2163-VIII (станом на 20 квітня 2025 р.).* URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 27.08.2025)
12. Верховна Рада України. (1991, 6 грудня). *Про оборону України: Закон України № 1932-XII (станом на 9 липня 2025 р.).* URL: https://zakon.rada.gov.ua/laws/show/1932-12#Text (дата звернення: 27.08.2025)
13. Рада національної безпеки і оборони України. (2021, 14 травня). *Про невідкладні заходи з кібероборони держави: Рішення Ради нац. безпеки і оборони України (станом на 28 серпня 2021 р.).* URL: https://zakon.rada.gov.ua/laws/show/n0053525-21#Text (дата звернення: 27.08.2025)
14. Верховна Рада України. (2024, 19 грудня). *Про Кіберсили Збройних Сил України: Проєкт Закону України № 12349.* URL: https://itd.rada.gov.ua/billinfo/Bills/Card/45453 (дата звернення: 27.08.2025)
15. Президент України. (2021, 17 вересня). *Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року «Про Стратегічний оборонний бюлетень України»: Указ Президента України № 473/2021.* URL: https://zakon.rada.gov.ua/laws/show/473/2021#Text (дата звернення: 27.08.2025)

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (30), 2025
Спеціальний випуск ISSN 2663 – 4023
Special issue

Svitlana Palamarchuk
Chief Research Fellow of Research Department
Heroes of Kruty Military Institute of Information and Telecommunication Technologies, Kyiv, Ukraine
ORCID: 0000-0001-7483-9165
svitlana.palamarchuk@viti.edu.ua

Nataliia A. Palamarchuk
Head of the Research Laboratory
Heroes of Kruty Military Institute of Information and Telecommunication Technologies, Kyiv, Ukraine
ORCID: 0000-0001-8818-7794
nataliia.palamarchuk@viti.edu.ua

Roman M. Shtonda
PhD, Head of Research Department
Heroes of Kruty Military Institute of Information and Telecommunication Technologies, Kyiv, Ukraine
ORCID: 0000-0001-5986-0847
roman.shtonda@viti.edu.ua

Tetiana V. Poberezhets
Researcher of the Research Laboratory
Heroes of Kruty Military Institute of Information and Telecommunication Technologies, Kyiv, Ukraine
ORCID: 0000-0001-8007-8614
tetiana.poberezhets@viti.edu.ua

THE ESSENCE OF UKRAINE'S CYBER DEFENSE: DEFINITION AND CONTRADICTIONS OF LEGAL AND THEORETICAL PRINCIPLES

Abstract. Since the beginning of the Russian Federation's hybrid aggression in 2014, and especially after the full-scale invasion in 2022, Ukraine has become the target of large-scale cyberattacks aimed at critical infrastructure and information systems of state institutions. The available statistics of cyberattacks confirm the Russian Federation's intentions to "capture" Ukraine's cyberspace by any means in order to achieve a strategic advantage in an armed conflict. Accordingly, Ukraine's tasks are to protect its own cyberspace and create conditions for active actions in the enemy's cyberspace. The article examines the essence of Ukraine's cyber defense in terms of fundamental definitions according to the Laws of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine", "On the Defense of Ukraine" and relevant regulatory legal acts. The analysis identifies contradictions in the theoretical and legal foundations of cyber defense, and emphasizes the lack of a clear legislative definition of the term "cyber defense". It is emphasized that no regulatory legal act defines the structure of the state cyber defense system, the composition and tasks of the entities providing it, as well as the objects of cyber defense. Some issues are partially outlined in the draft Law on the Cyber Forces of the Armed Forces of Ukraine, however, its provisions contain discrepancies with the current legislation and consider cyber defense in a "narrow" sense. All of the above complicates the formation of state policy in the field of cyber defense, and accordingly, the implementation of the cyber defense system. Attention is focused on the need to harmonize legal and regulatory definitions from the standpoint of a systemic approach, to separate cyber defense into a separate sphere with the adoption of the basic law "On Cyber Defense of Ukraine", which will determine the principles of state policy, ensure the harmonization of the legal field and contribute to the implementation of the state's strategic goals in the field of cyber defense.

Key words: information protection; information infrastructure; information and communication system; cybersecurity, cyber protection; cyber defense; cyberspace; critical infrastructure.

REFERENCES

1. North Atlantic Treaty Organization. (2016, July 8–9). *Statement following the Warsaw Summit.* Retrieved August 27, 2025, from https://www.nato.int/cps/uk/natohq/official_texts_133169.htm

2. President of Ukraine. (2021, August 26). *On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine" (Decree No. 447/2021).* Retrieved August 27, 2025, from https://zakon.rada.gov.ua/laws/show/447/2021#Text
3. Skitsko, O., & Shirshov, R. (2024). Regulatory and legal support for cyber defense of Ukraine: Current state. *Legal Bulletin, (3),* 244–250. https://doi.org/10.32782/yuv.v3.2024.29
4. Tyutyunnyk, V. (2025). Cyber defense of Ukraine: State, problems, and current measures to ensure it. *Defense-Industrial Courier.* Retrieved August 27, 2025, from https://surl.li/tcqxwm
5. Davydyuk, A. V. (2022). Cybersecurity and cyber defense of critical infrastructure. In *Cybersecurity of Energy: Proceedings of the Scientific and Practical Conference* (Kyiv, May 27, 2022) (pp. 50–52). Kyiv. Retrieved August 27, 2025, from https://is.gd/yd2rQK
6. Savchenko, V. A. (2023). Ensuring the stability of the state's cyber defense under conditions of armed conflict. *Modern Information Protection, 55(3),* 6–11. https://doi.org/10.31673/2409-7292.2023.030001
7. Danyk, Y., Vorobiienko, P., & Chernega, V. (2019). *Fundamentals of cybersecurity and cyber defense* (2nd ed.). Odesa: ONAZ named after O. S. Popov.
8. Ternovy, O., Shkurenko, O., & Minenko, L. (2023). Problematic aspects of cyber defense: The place and role of cyber protection in the Armed Forces of Ukraine. *Modern Information Technologies in the Field of Security and Defense, 46(1),* 23–31. https://doi.org/10.33099/2311-7249/2023-46-1-23-31
9. Snitsarenko, P. M. (2024). On the essence of cyber defense as a type of military action. *Science and Defense, (3),* 45–54. https://doi.org/10.33099/2618-1614-2024-26-3-45-54
10. Snitsarenko, P. M. (2024). Cyber defense of Ukraine as a component of state defense. *Science and Defense, (4),* 40–48. https://doi.org/10.33099/2618-1614-2024-27-4-40-48
11. Verkhovna Rada of Ukraine. (2017, October 5). *On the basic principles of ensuring cybersecurity in Ukraine (Law No. 2163-VIII, as of April 20, 2025).* Retrieved August 27, 2025, from https://zakon.rada.gov.ua/laws/show/2163-19#Text
12. Verkhovna Rada of Ukraine. (1991, December 6). *On the defense of Ukraine (Law No. 1932-XII, as of July 9, 2025).* Retrieved August 27, 2025, from https://zakon.rada.gov.ua/laws/show/1932-12#Text
13. National Security and Defense Council of Ukraine. (2021, May 14). *On urgent measures for the cyber defense of the state (Resolution as of August 28, 2021).* Retrieved August 27, 2025, from https://zakon.rada.gov.ua/laws/show/n0053525-21#Text
14. Verkhovna Rada of Ukraine. (2024, December 19). *On the Cyber Forces of the Armed Forces of Ukraine (Draft Law No. 12349).* Retrieved August 27, 2025, from https://itd.rada.gov.ua/billinfo/Bills/Card/45453
15. President of Ukraine. (2021, September 17). *On the decision of the National Security and Defense Council of Ukraine dated August 20, 2021 "On the Strategic Defense Bulletin of Ukraine" (Decree No. 473/2021).* Retrieved August 27, 2025, from https://zakon.rada.gov.ua/laws/show/473/2021#Text