УДК 342.951

КРАСНІКОВ С.А., провідний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0001-6548-5457.

ОРГАНІЗАЦІЙНО-ПРАВОВІ ЗАСАДИ ПОСИЛЕННЯ СПРОМОЖНОСТЕЙ ДЕРЖАВИ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРОБОРОНИ

Анотація. *Досліджено питання забезпечення кібероборони. Розглянуто вітчизняні стратегічні документи, присвячені питанням кібербезпеки та кібероборони. Деталізовано засади реалізації державної військової політики з метою розвитку кібероборонного потенціалу. Окреслено перспективи утворення в Україні кібервійськ. Розкрито підхід НАТО до поняття та особливостей кібероборони. Висвітлено турецький досвід забезпечення кібероборони держави. Узагальнено перспективи удосконалення кібероборонного потенціалу з урахуванням результативних здобутків зарубіжного досвіду.*

Ключові слова: *національна система кібербезпеки, кібероборона, кіберпростір, кібервійська, військова політика, інформаційно-телекомунікаційні системи, державне оборонне планування.*

Summary. *The issue of providing cyber defense has been detailed. Domestic strategic documents on cyber security and cyber defense are considered. The principles of implementation of the state military policy for the purpose of development of cyber defense potential are fixed. Prospects for the formation of cyber troops in Ukraine are outlined. NATO's approach to the concept and features of cyber defense is revealed. The Turkish experience of providing state cyber defense is highlighted. The prospects of improving the cyber defense potential of our country are identified, taking into account the effective achievements of foreign experience.*

Keywords: *national cyber security system, cyber defense, cyberspace, cyber troops, military policy, information and telecommunication systems, state defense planning.*

Аннотация. *Исследованы вопросы обеспечения кибероборонны. Рассмотрены отечественные стратегические документы, посвященные вопросам кибербезопасности и кибероборонне. Детализированы основы реализации государственной военной политики с целью развития кибероборонительного потенциала. Определены перспективы создания в Украине кибервойск. Раскрыт подход НАТО касаемо понятия и особенностей кибероборонны. Освещен турецкий опыт обеспечения кибероборонны государства. Обобщены перспективы усовершенствования кибероборонительного потенциала с учетом результативных достижений зарубежного опыта.*

Ключевые слова: *национальная система кибербезопасности, кибероборона, киберпространство, кибервойска, военная политика, информационно-телекомуникационные системы, государственное оборонное планирование.*

Постановка проблеми. Останнім часом прискіплива увага держави сконцентрована на питаннях забезпечення кібербезпеки і особливо кібероборони. Саме кібероборона стає невід'ємною частиною безпекового потенціалу будь-якої держави. Ця вимога пов'язана із реаліями сьогодення, враховує всесвітній технологічний прогрес та появу нових гібридних загроз у цьому сегменті. Беззаперечно, на перманентній основі зростає небезпека використання кіберпростору для завдання шкоди національним інтересам України, включаючи виведення з ладу критично важливих об'єктів інфраструктури. Фактор поширення CoVID-19 переконливо довів, що епідемії здатні вражати держави

та суспільства одразу в багатьох вимірах. Заходи протидії CoVID-19 порушують усталені практики міжнародного спілкування, передбачають обмеження основних прав і свобод та при цьому все одно можуть бути недостатніми для захисту життя і здоров'я людей. Така ситуація провокує необхідність пошуку шляхів посилення кібероборони держави.

Агресивна політика РФ, яка проявляється в проекції її силового потенціалу в Азово-Чорноморському регіоні, на Південному Кавказі, у Східній і Південно-Східній Європі та у Середземномор'ї, спричинює ерозію регіональної безпекової архітектури. Саме держава-агресор залишається одним з основних джерел загроз національній та міжнародній кібербезпеці, активно реалізує концепцію інформаційного протиборства, яка базується на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно застосовуються у гібридній війні проти України. Така деструктивна активність створює реальну загрозу вчинення актів кібертероризму та кібердиверсій стосовно національної інформаційної інфраструктури.

Враховуючи виклики та загрози, які провокує РФ, серед важелів та засобів гібридної війни, які держава-агресор застосовує, у першу чергу, проти України – це масштабні кібератаки на критично важливі об'єкти інфраструктури. На цьому фоні важливим меседжем держави стало схвалення на державному рівні у серпні 2021 року низки важливих рішень РНБО України, якими затверджені актуальні для держави стратегічні документи (Стратегія кібербезпеки України, Стратегічний оборонний бюлетень), які змістовно та безпосередньо присвячені, у тому числі, й питанням посилення кібероборони в умовах ескалації збройного конфлікту на Донбасі. Тому висвітлення останніх здобутків організаційно-правового характеру нашої держави за напрямом посилення стану кібероборони є своєчасним та актуальним.

Результати аналізу наукових публікацій. Деякі проблемні питання забезпечення кібероборони держави досліджували у своїх наукових працях такі фахівці: О. Вітер [5], С. Вдовенко [6], В. Роллер [7], К. Соколов [8] тощо. На дисертаційному рівні засади державної політики у сфері розбудови вітчизняної системи кібероборони розглядали: І. Діордиця [9], О. Островий [10]. Проте жоден із зазначених авторів не розглядав питання забезпечення кібероборони в контексті схвалення в Україні оновленої Стратегії кібербезпеки України на 2021 – 2025 роки та Стратегічного оборонного бюлетеня України.

Метою статті є визначення на підставі контент-аналізу схвалених стратегічних документів, присвячених питанням посилення стану кібероборони, перспективних шляхів удосконалення кібероборонного потенціалу нашої держави з врахуванням позитивного зарубіжного досвіду у цій сфері.

Виклад основного матеріалу. Важливим завданням державного стратегічного планування є раціональний розподіл державою потенційних можливостей та наявних ресурсів (людських, інформаційних, фінансових, телекомунікаційних, технічних, технологічних), завдяки яким держава гарантує забезпечення національної безпеки та стабільний соціально-економічний і цифровий розвиток громадянського суспільства в цілому. Для досягнення цієї мети необхідно мати досить високий рівень управлінської культури державного апарату, що зумовлює застосування методів системного аналізу й прогнозування, а також спеціальних методів забезпечення безпеки в кіберпросторі тощо. Важливим завданням концептуального проектування системи забезпечення кібербезпеки є її методологічне забезпечення, в основі якого перебуває розуміння природи цього виду діяльності. Важливою складовою кібербезпеки є саме кібероборона. У вітчизняному законодавстві кібероборона визначається як 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 [1].

Таким чином, кібероборона об'єднує усі можливі оборонні заходи та потужності держави на фоні яких інформаційно-комунікаційні технології цілеспрямовано застосовуються у якості оборонних технологій, а кіберпростір виступає "театром військових дій". Проте, тривалий час питання забезпечення кібероборони на державному рівні не розвивалося. Розуміючи актуалізацію питань забезпечення кібероборони, 26 серпня 2021 року Президент України увів в дію рішення РНБО України "Про невідкладні заходи з кібероборони держави" від 14.05.21 р. [2]. Цим актом підкреслюється необхідність термінового вжиття невідкладних заходів щодо створення передумов для формування у системі Міністерства оборони України кібервійськ для захисту суверенітету держави, забезпечення її обороноздатності, запобігання збройному конфлікту та відсічі збройній агресії у кіберпросторі. Задекларовано, що Кабінет Міністрів України має розробити та внести на розгляд Верховної Ради України законопроект щодо створення та функціонування у системі Міністерства оборони України підрозділу кібервійськ. Тобто важливою складовою побудови вітчизняної системи кібероборони є саме інституційне утворення кібервійськ. Адже це є лише однією із важливих композитних складових розбудови системи кібероборони.

На жаль, у 2016 – 2019 роках законодавчо визначені завдання щодо здійснення Міністерством оборони України та Генеральним штабом Збройних Сил України заходів із забезпечення кібероборони держави, нарощування її кібероборонних спроможностей не були належним чином імплементовані у документах оборонного планування, що призвело до гальмування процесів у сфері розбудови національної кібероборони. У зв'язку з чим з 2019 року в Україні (після зміни політичного керівництва країни) розпочато новий цикл оборонного планування.

Революційним здобутком сучасності стало схвалення нової Стратегії кібербезпеки України на 2021 – 2025 роки [3]. Оновлена редакція Стратегії кібербезпеки містить перелік викликів і загроз, які стоять перед Україною в сфері кібербезпеки, визначає засади розбудови національної системи захисту від кіберзагроз, деталізує основні пріоритети та стратегічні цілі забезпечення кібербезпеки України, а також напрями зовнішньополітичної діяльності і стратегічні завдання, які стоять перед державою в зазначеній сфері. Згідно з оприлюдненим текстом Стратегії, забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України, а реалізація зазначеного пріоритету очікувано здійснюватиметься шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі.

Досконалий аналіз положень Стратегії кібербезпеки України на 2021 – 2025 роки дає змогу визначити пріоритетні цілі та стратегічні завдання щодо розвитку та побудови власної системи надійної кібероборони. Формування нової сучасної якості національної системи кібербезпеки потребує чіткого та зрозумілого визначення стратегічних цілей, важливою з яких виступає дієва кібероборона. З метою її забезпечення Україна має консолідувати зусилля на таких напрямах, як: створення та забезпечення динамічного розвитку підрозділів з повноваженнями ведення збройного протиборства в кіберпросторі, формування організаційно-правової та технологічної моделі їх функціонування та застосування, забезпечення ефективної взаємодії основних суб'єктів національної системи кібербезпеки та сил оборони під час проведення заходів з кібероборони, належне навчання та фінансове забезпечення таких структур, систематичне проведення

кібернавчань, здійснення оцінки спроможностей та ефективності підрозділів, розроблення та імплементацію індикаторів оцінки їх діяльності.

Важливим завданням для нашої держави на стратегічному рівні є формування системи кібероборони шляхом: 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; 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; проведення щонайменше двічі на рік спільних тематичних навчань із відповідними підрозділами держав-членів НАТО задля досягнення оперативної сумісності; створення MIL.CERT-UA в інтересах Міністерства оборони України та Збройних Сил України, налагодивши на постійній основі співпрацю із європейською військовою CERT-мережею; забезпечення оцінки спроможностей суб'єктів сектору безпеки і оборони в частині спільного виконання завдань кібероборони, зокрема під час проведення оборонних оглядів, оглядів національної системи кібербезпеки, оглядів стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури; запровадження у системі військово-патріотичного виховання та системі територіальної оборони навчальних програм підготовки та проведення практичних навчань у сфері кібербезпеки.

Таким чином, кібероборона є важливим чинником сучасної оборони держави. Забезпечення кібероборони України відповідно до чинного законодавства покладено на Міноборони та Генштаб ЗСУ, які у рамках своєї компетенції повинні вживати заходи із забезпечення кібероборони з метою захисту суверенітету держави та забезпечення її обороноздатності, відсічі збройної агресії.

Президент України своїм Указом від 17 вересня 2021 року № 473/2021 увів у дію рішення РНБО України від 20 серпня 2021 року [4], яким затвердив концептуальний документ – оновлений Стратегічний оборонний бюлетень України, в якому відображається стратегія воєнної безпеки України, її засади, чинники й складові компоненти. Згідно із положеннями цього документа, військова політика України реалізується за кількома основними напрямами, один із яких – це забезпечення відсічі і стримування збройної агресії РФ, відновлення суверенітету і територіальної цілісності України, запобігання військових конфліктів з будь-якими іноземними державами. Зокрема, достатня увага приділяється побудові ефективних механізмів забезпечення кібероборони. Нормативно акцентовано, що створення національної системи кібероборони має бути орієнтовано на набуття необхідних спроможностей суб'єктами підготовки та здійснення заходів кібероборони, створення і розвиток сил, засобів та інструментів протиборства в кіберпросторі, які забезпечать створення необхідного потенціалу сил оборони для відбиття воєнної агресії в кіберпросторі.

У Стратегічному оборонному бюлетені України, зокрема п. 5.6, присвячений питанням утворення системи кібероборони. При цьому кінцева мета такої діяльності – використання силами оборони кіберпростору та створення системи кібероборони, які забезпечують запобігання виникненню воєнного конфлікту та загрози з використанням кіберпростору, підготовку та ведення кібероборони.

На виконання цієї мети мають бути вжиті такі заходи: розвиток спроможностей щодо ведення протиборства в інформаційному просторі (включаючи кіберпростір) Збройними Силами України та іншими складовими сил оборони; створення системи кібероборони як основного засобу стримування та відбиття воєнної агресії в кіберпросторі; створення та розвиток у складі Збройних Сил України необхідних військових організаційних структур

для дій у кіберпросторі, їх комплектування, підготовка та всебічне забезпечення; створення системи управління підготовкою та веденням кібероборони, її інтеграція в системи управління (керівництва) обороною держави та забезпеченням кібербезпеки, включаючи створення в системі Міністерства оборони України ситуаційного центру кібербезпеки; розвиток спроможностей системи захисту інформації та кіберзахисту в інформаційно-телекомунікаційних системах Міністерства оборони України та Збройних Сил України; нормативне визначення та включення до системи операцій Збройних Сил України сучасних форм і способів дій військ (сил) у кіберпросторі, ведення ними кібероборони; впровадження сучасних апаратно-програмних комплексів кібербезпеки, засобів з кіберзахисту, інших систем (зразків) кіберзброї у Збройних Силах України та інших складових сил оборони; розвиток спроможностей сил оборони щодо забезпечення кіберзахисту критичної інформаційної інфраструктури держави в умовах надзвичайного і воєнного стану; розширення військової співпраці з НАТО щодо забезпечення безпеки кіберпростору та спільних дій у кіберпросторі тощо.

Таким чином, кібероборона України базується на готовності та здатності сил оборони виконувати завдання кібероборони в будь-який час та в складних умовах функціонування кіберпростору. При цьому сили оборони для досягнення військового та стратегічного паритету в кіберпросторі мають застосовувати належні можливості реагування на зовнішні та внутрішні кіберзагрози воєнного характеру [11, с. 33].

На початку серпня 2021 року Україна у рамках посилення співпраці з НАТО у кіберпросторі подала офіційний запит на приєднання до Об'єднаного центру передових технологій з кібероборони НАТО (CCDCOE), який базується в м. Таллінні (Естонія). Унікальність центру НАТО з кібербезпеки полягає в тому, що там спільно працюють військові, цивільні, представники уряду. Робота центру сфокусована на трьох основних напрямках: дослідження, тренування та навчання. Зокрема, делегація Національного координаційного центру кібербезпеки при РНБО України здійснила робочий візит до Естонської Республіки, в межах якого було проведено низку двосторонніх зустрічей з метою розвитку паритетної співпраці між Україною та Естонією у сфері посилення кібербезпеки. Сторони дійшли згоди, що ефективним кроком на шляху до приєднання України до кібербезпеки НАТО є залучення українських експертів до роботи в рамках тематичних груп CCDCOE [12].

Для НАТО протидія кіберзагрозам визначена поняттям "кібероборона", яка входить до переліку головних цілей колективної оборони, що підкреслює його безпеково-оборонну спрямованість. Вперше кібероборона була включена в політичний порядок денний Альянсу на Празькому саміті ще у 2002 році. На Уельському саміті 2014 року НАТО схвалено посилену політику з кібероборони і відповідний план дій з її імплементації. На Варшавському саміті 2016 року Альянс вже зосереджував увагу на посиленні кібероборони національних мереж та промисловості. Тоді ж був підтверджений мандат НАТО на проведення операцій у кіберпросторі, який прирівняли до інших сфер проведення операцій – суші, повітря і моря. На Брюссельському саміті НАТО 2018 року кібератаки віднесені до головних гібридних загроз. НАТО погодило необхідність доведення операцій з кібероборони до рівня операцій в інших трьох сферах як за загальної координації Альянсу, так і в межах окремих груп союзників. На саміті НАТО у 2021 році було наголошено на необхідності постійно модернізувати та удосконалювати кібероборону, а кіберпростір визначено як окрему сферу військових операцій.

За таких умов забезпечення кібероборони є важливою складовою забезпечення кібербезпеки держави. Як переконливо засвічує зарубіжний досвід функціонування кібервійськ, чималі витрати на утримання відповідних підрозділів у арміях передбачені у

переважній більшості держав світу. Наприклад, у США щорічний бюджет на утримання штату у кількості 9 тис. кібервійськових складає $7 млрд. США, у Великій Британії $450 млн. США на 2 тис. персоналу, у Франції – $220 млн. на 800 осіб. Держава-агресор щорічно витрачає $300 млн. США при загальній чисельності 1 тис. вояків, у тому числі й "білих" хакерів, Ізраїль – $150 млн. США на утримання 1 тис. штату. Тобто функціонування кібервійськ передбачає й належний обсяг фінансування.

17 вересня 2021 року під головуванням Президента України відбулося засідання РНБО України, на якому було розглянуто бюджет сектору безпеки й оборони на 2022 рік. За результатами розгляду РНБО ухвалила рішення рекомендувати уряду при підготовці проекту державного бюджету на наступний рік збільшити фінансування сектору безпеки та оборони до 5,95 % ВВП, або 319,4 млрд. грн. (з 5,93 % ВВП у 2021 році). У бюджеті закладено витрати на забезпечення кібербезпеки та зокрема утримання кібервійськ.

На початку 2020 року Естонія, Хорватія, Литва, Нідерланди, Румунія, Польща підписали меморандум, відповідно до положень якого у перелічених країнах будуть утворені спільні міжнародні команди реагування на кіберзагрози. Зокрема, меморандумом передбачено практичні механізми роботи команд, їхній правовий статус та компетенція. До складу вказаних команд увійдуть цивільні та військові експерти вказаних країн, а їхня діяльність буде спрямована на нейтралізацію та розслідування будь-яких кіберінцидентів. Таким чином, на виконання політичної волі військових структур вказаних країн була утворена міжнародна група швидкого реагування з метою протистояння будь-яких кібератакам. Новоутворена структура буде опікуватися не тільки віртуальними питаннями, але й при необхідності і фізично брати участь під час розслідування потужних кіберінцидентів.

Одночасно у 2020 році в Туреччині з'явилися власні кібервійська (Türk Siber Ordusu) у кількості орієнтовно 13 тис. осіб. До складу кібервійськ Туреччини входять військові та цивільні особи, які є фахівцями у сфері кібербезпеки, переважну більшість складають хакери, які перейшли на роботу до державного сектора. Ядро турецької кіберармії складається з 5 тактичних груп (правоохоронна, морська, космічна, комплексної оборони та група "армія"). В авангарді турецької кіберармії перебувають великі хакерські спільноти, на кшталт "Ayyıldız Tim" та "Anka Neferler" які діють автономно від національних кіберсил. Як правило, лояльні угруповання використовуються для проведення відволікаючих маневрів у кіберпросторі. Залучаються також й хакери-одинаки. Доктрина кібербезпеки Туреччини має комплексний (оборонно-наступальний) характер та передбачає не тільки захисні, але й розвідувальні заходи, а також проведення кібератак на упередження. Таким чином, Туреччина як стратегічний сусід України має робочу військово-цивільну структуру, яка забезпечує стабільний захист національного сегменту кіберпростору, гарантує кібероборону. При цьому в її арсеналі активно та відкрито використовуються хакери для захисту державних інтересів у кіберпросторі, проведення наступальних кібероперацій.

Висновки.

Забезпечення кібероборони неможливе без прийняття управлінських рішень на планових засадах, що передбачає розробку та вжиття необхідних заходів, визначення алгоритму спільних дій з боку державних органів та інших суб'єктів забезпечення кібербезпеки, встановлення конкретних строків та відповідальних за їх виконання. В сучасних умовах перед державою постає важливе та актуальне завдання щодо створення та функціонування підрозділу кібервійськ, розробки власних напрацювань та зразків кіберзброї, прискорення розробки проекту Стратегії кібероборони України, де прискіпливу увагу слід приділити не лише кібероборонним (кіберзахисним) діям

об’єднаних сил/військ кібероборони, а й їхнім проактивним упереджувальним, кіберрозвідувальним та кібернаступальним діям. Також доцільно визначити у відповідних нормативно-правових актах структуру системи кібероборони держави, склад, функції та завдання суб’єктів її забезпечення, а також об’єкти кібероборони, деталізувати заходи, практичне впровадження яких надасть змогу значно посилити кібероборону та підвищити кібероборонні спроможності держави.

Використана література

1. Про основні засади забезпечення кібербезпеки України: Закон України від 5.10.17 р. № 2163. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403.

2. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року “Про невідкладні заходи з кібероборони держави”: Указ Президента України від 26.08.21 р. № 446/2021. URL: https://www.president.gov.ua/documents/4462021-40009

3. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року “Про Стратегію кібербезпеки України”: Указ Президента України від 26.08.21 р. № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013

4. Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року “Про Стратегічний оборонний бюлетень України”: Указ Президента України від 17.09.21 р. № 473/2021. URL: https://www.president.gov.ua/documents/4732021-40121

5. Вітер О. Законодавче забезпечення у сфері оборони та безпеки: підсумки та перспективи. *Голос України*. 2019. № 3. – (5 січня 2019 р.).

6. Вдовенко С.Г., Даник Ю.Г. Проблеми та перспективи забезпечення кібероборони держави: збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. Київ: ВІКНУ, 2020. Вип. № 66. С. 75-89.

7. Роллер В.М. Правове регулювання здійснення кібероборони. *Право і суспільство*. 2018. № 5. Ч. 2. С. 137-141.

8. Соколов К.О., Гудима О. П. Підхід до розробки елементів структури системи виявлення деструктивного впливу у кіберпросторі. *Наукоємні технології*. 2019. № 4(44). С. 426-432.

9. Діордиця І.В. Адміністративно-правове регулювання кібербезпеки України: автореф. дис. …д-ра юрид. наук: спеціальність 12.00.07. Запоріжжя. 2018. 40 с.

10. Островий О.В. Формування державної політики забезпечення кібернетичної безпеки в Україні: автореф. дис. ...канд. наук з держ. упр.: спеціальність 25.00.02; Донец. держ. ун-т упр. Маріуполь, 2019. 20 с.

11. Живило Є.О., Черноног О.О. Стратегія кібероборони України: збірник наукових праць ВІТІ. 2017. № 4. С. 30-37.

12. Україна подала запит на приєднання до центру НАТО з кібероборони. URL: https://ua.interfax.com.ua/news/general/759797.html

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~