Інформаційна і національна безпека

УДК 342.951

ФИЦА В.М., старший науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0002-6590-8082.

ІНСТИТУЦІЙНЕ ЗАБЕЗПЕЧЕННЯ СТВОРЕННЯ КІБЕРВІЙСЬК В УКРАЇНІ

Анотація. *Розглянуто питання інституційного забезпечення створення та функціонування кібервійськ. Визначено завдання та цілі кібервійськ. Висвітлено кращі практики зарубіжного досвіду у сфері розбудови кібервійськ та кіберкомандування. Акцентована увага на сучасних загрозах поширення мілітаризації кіберпростору. Визначено шляхи удосконалення державної політики у військовій сфері щодо утворення кібервійськ в структурі Міністерства оборони України.*

Ключові слова: *кібервійська, кіберкомандування, кібербезпека, кібероборона, спеціальні інформаційні операції, кіберпростір, кібератака, мілітаризація кіберпростору.*

Summary. *The issue of institutional support for the creation and functioning of cyber forces is considered. The tasks and goals of cyber forces have been defined. The best practices of foreign experience in the field of building cyber forces and cybercommand are highlighted. Emphasis is placed on current threats to the spread of cyber space militarization. The directions of the improvement of the state policy in the military sphere on the formation of cyber forces in the structure of the Ministry of Defense of Ukraine have been identified.*

Keywords: *cyber forces, cybercommand, cybersecurity, special information operations, cyberspace, cyber attack, militarization of cyberspace.*

Аннотация. *Рассмотрены вопросы институционального обеспечения создания и функционирования кибервойск. Определены задачи и цели кибервойск. Освещены лучшие практики зарубежного опыта в сфере создания кибервойск и киберкомандования. Акцентировано внимание на современных угрозах распространения милитаризации киберпространства. Определены направления усовершенствования государственной политики в военной сфере касаемо создания кибервойск в структуре Министерства обороны Украины.*

Ключевые слова: *кибервойска, киберкомандование, кибербезопасность, кибероборона, специальные информационные операции, киберпространство, кибератака, милитаризация киберпространства.*

Постановка проблеми. Останнім часом колосального масштабу у світі набула проблема захисту кіберпростору та елементів системи стратегічних комунікацій сектору безпеки і оборони від загроз несанкціонованого втручання. Практично безмежні можливості використання Інтернету підкреслюють глобальну загрозу кіберзлочинів, кібертероризму та ведення кібервійни. Анонімність глобальних інформаційних мереж, швидкість передачі інформації та простота їх використання одночасно дозволяють використовувати всі ці переваги для здійснення протиправних діянь. Інформаційно-комунікаційні технології впроваджуються і розвиваються набагато швидше, ніж законодавці та правоохоронні органи можуть реагувати на це зростання. У багатьох країнах світу проголошено мілітаризацію кіберпростору. Таким чином, розбудова дієвої

системи кібербезпеки України вимагає чіткого визначення засад державної політики у цій сфері та випереджального організаційно-правового та техніко-технологічного реагування на динамічні зміни, що відбуваються у кіберпросторі. Сучасна війна неможлива без кіберзахисту і, на превеликий жаль, без кібератак. Так, власні кібервійська вже мають у своєму потенціалі США, Китай, Великобританія, Франція, Німеччина, Ізраїль, Південна Корея, Японія та інші провідні держави світу. Протиборство в кіберпросторі стає принципово новою сферою та фазою вирішення конфліктних ситуацій між державами, а терміни та визначення з префіксом "кібер" знайшли своє відображення у положеннях стратегій, доктрин та концепцій переважної більшості держав світу, а також міжнародних організацій, у т.ч. НАТО. Стрімкий зростаючий у світі інтерес до проблематики кіберпростору пов'язаний, у першу чергу, з питаннями забезпечення кібербезпеки та ведення сучасних кібервійн. За таких умов визначення інституційних засад створення вітчизняних кібервійськ набуває актуальності в умовах масштабного поширення гібридних загроз, особливо з боку інформаційної експансії РФ.

Результати аналізу наукових публікацій. Питання інституційно-функціонального створення та розбудови кібервійськ досліджували у своїх працях такі науковці як: Г. Красноступ [1], О. Косогов [2], Р. Лук'янчук [3], С. Паламарчук [4] та інші. Аналіз праць вказаних авторів дає змогу визначити, що інституційні засади створення кібервійськ недостатньо розглянуті, що зумовлює необхідність дослідження зазначених процесів з урахуванням позитивного зарубіжного досвіду. Особливо це питання актуально на фоні анонсованих у травні 2021 року ініціатив Секретаря РНБО України О. Данилова щодо прискорення створення кібервійськ в Україні.

Метою статті є визначення інституційних засад у сфері забезпечення створення кібервійськ з урахуванням кращих практик зарубіжного досвіду у цій сфері в умовах глобального геополітичного протиборства.

Виклад основного матеріалу. Розуміючи необхідність та доцільність мілітаризації кіберпростору, у багатьох країнах світу створено та функціонують спеціальні підрозділи – кібервійська, які використовуються як для військових, так і розвідувальних цілей. Спеціалізовані підрозділи з кібербезпеки офіційно використовуються у десятках країн, а неофіційно – вже майже у сотні іноземних держав. Найбільш потужну армію у кіберпросторі має США, а державне фінансування на її утримання складає понад $7 млдр. США на рік. Комплектування цих підрозділів здійснюється переважно за рахунок хакерів, які поповнюють ряди військових у кіберпросторі. Надійний захист кіберпростору та домінування у світовому масштабі – стратегічне завдання уряду США, що не виключає військових дій у кіберпросторі з урахуванням національних інтересів. Політичний вектор, закладений у стратегії національної кібербезпеки США, аргументовано декларує систему кіберзагроз, настання яких провокує необхідність проведення спеціальних інформаційних операцій, спрямованих на запобігання їм та недопущення будь-яких кібератак з боку інших держав. Основними напрямками діяльності кібервійськ є шпіонаж, у тому числі й промисловий, кібератаки, спеціальні інформаційні операції та навіть ведення війни у кіберпросторі. У військових структурах передових країн світу є навіть кіберкомандування та відокремлено персонал, який залучається для захисту інфраструктури військових кіберсистем. Перемога над супротивником у цифровій війні вважається більш пріоритетною, аніж перемога у класичному військовому протистоянні.

Цікавим видається у цій площині передовий досвід Естонії. На початку серпня 2018 року в естонській армії з'явився підрозділ, що відповідає за кібербезпеку країни. Поява власного підрозділу кіберкомандування в Естонії демонструє не тільки відданість

приписам НАТО, який у 2016 році визнав кіберпростір полем проведення військових операцій на рівні з повітрям, сушею та морем. І не тільки поширення тенденції до створення власних кібервійськ, як у Франції, де їх заснували у 2016 році, або у Німеччині, де вони діють з 2017 року. Проте у цій країні процес створення оперативного кіберкомандування має закінчитися у 2023 році, оскільки повинні бути виконані нормативно визначені завдання у повному обсязі. Основна ідея підрозділу кіберкомандування Естонії полягає в тому, щоб об'єднати в єдине ціле різні частини усієї оборонної системи, які використовуються для підтримання життєдіяльності кіберсфери, для більш ефективного використання наявних людських, технологічних та фінансових ресурсів. Об'єднаний центр кіберкомандування допоможе краще використовувати здібності захищати об'єкти критичної інфраструктури від потенційних комп'ютерних загроз.

Кібернетичне командування має наступальні спроможності і може завдавати удари у відповідь на будь-які атаки. Також у цій структурі окремо було створено волонтерський підрозділ з кібербезпеки, до якого входять цивільні особи з комп'ютерними навичками. Добровольці захищають естонський кіберпростір у вільний від роботи час. Мета наступальних операцій у кіберпросторі полягає в тому, щоб вразити ворога у кіберпросторі для збереження власної свободи пересування. Незалежно від розвинених наступальних можливостей кіберкомандування, основним завданням нового підрозділу є підтримка командування оборонних сил Естонії через надання та захист інформації. Наступальні кіберспроможності використовуються, у тому числі, для перевірки безпеки власних інформаційно-комунікаційних систем і створення реалістичного середовища для навчань оборонних підрозділів. Кіберкомандування виконує свої повноваження лише в межах завдань Міністерства оборони цієї країни. Головна місія кіберкомандування – проводити спеціальні операції у кіберпросторі і надавати підтримку міністерству оборони. Тож кіберкомандування не несе відповідальності за підтримку та захист національних електронних послуг, але тісно співпрацює з організаціями, які цим займаються. Чисельно в Естонії кібервійська складають усього 300 осіб персоналу. У свою чергу, німецьке кіберкомандування у 2021 році налічує 13,5 тисячі військовослужбовців, в американському спецпідрозділі 19 тисяч, а в російській кіберармії – щонайменше 1 тис. військовослужбовців. За таких умов, пошук та підбір кваліфікованих кадрів – важливе завдання комплектування підрозділу кібервійськ. Волонтерська ліга оборони, резервні служби та призовники є основним резервом кадрів для пошуку кваліфікованого персоналу. Модель національної оборони Естонії ґрунтується на військовому обов'язку призовної служби, а також резервній службі. ІТ-навички, яким навчають у загальноосвітніх школах, можуть бути застосовані в силах оборони. Тому використовуються призовники з конкретними навичками під час виконання ними військового обов'язку. Наразі у кібервійськах Естонії проходять службу приблизно 30 призовників, які підтримують щоденні кібероперації. Якщо майбутні призовники матимуть відповідні вміння та навички, вони теж зможуть проходити службу у підрозділі кіберкомандування.

Держава-агресор ще у 2014 році створила у складі Міністерства оборони війська інформаційних операцій. РФ входить до топ п'ятірки держав світу, які мають власні кібервійська, які активно використовуються для проведення наступальних спеціальних інформаційних операцій та проведення інформаційних війн. Орієнтовно чисельність російських кібервійськ складає 1 тис. осіб, а обсяг щорічного фінансування дорівнює $300 млн. Об'єктами посягань з боку РФ залишається, у першу чергу, Україна та її інформаційний простір.

В Україні, особливо в умовах російської агресії, питання забезпечення безпеки кіберпростору гостро стоять перед політичним керівництвом нашої держави. Починаючи з 2018 року РНБО України опрацьовує питання створення кібервійськ, тобто вивчаються кращі практики зарубіжного досвіду з метою його адаптації в українських реаліях для створення власних кібервійськ у складі Збройних Сил України. Це надасть змогу значно посилити спроможності держави у сфері забезпечення оборони в кіберпросторі. Необхідно також зазначити, що відповідно до Указу Президента України "Про рішення Ради національної безпеки і оборони України від 20 травня 2016 року "Про Стратегічний оборонний бюлетень України" від 06.06.16 р. № 240/2016 [5], в нашій країні прийнято Стратегічний оборонний бюлетень, який слугуватиме дорожньою картою оборонної реформи із визначенням шляхів її впровадження відповідно до стандартів НАТО.

Зокрема передбачається, в рамках оборонного реформування, досягнення таких стратегічних цілей, як: удосконалення системи управління силами оборони; створення ефективної системи оперативного (бойового) управління, зв'язку, розвідки та спостереження (C4ISR); удосконалення системи кібербезпеки та захисту інформації; становлення та розбудова спроможностей сил оборони у сфері стратегічних комунікацій, спрямованих на підтримку формування та реалізації політики у сфері безпеки і оборони України, а також досягнення цілей оборони держави; впровадження ефективної політики, системи планування і управління ресурсами в секторі оборони з використанням сучасних євроатлантичних підходів тощо. У свою чергу, Стратегічний бюлетень охоплював довгостроковий період до кінця 2020 року. Тобто в рамках оборонного реформування передбачається: створення в Міністерстві оборони та Генеральному штабі Збройних Сил підрозділів із забезпечення кібербезпеки та кіберзахисту, протидії технічним розвідкам; впровадження заходів із захисту інформації відповідно до вимог нормативно-правових актів України та з урахуванням стандартів НАТО і ISO/IEC; створення воєнної команди реагування на комп'ютерні надзвичайні події (*milCert*); здійснення міжвідомчої координації з цих питань в інтересах забезпечення обороноздатності держави, оскільки забезпечення максимальної ефективності Збройних Сил України в кіберпросторі та їх здатність надавати адекватну відповідь реальним та потенційним кіберзагрозам залишаються важливими завданнями сучасності; створення єдиного підрозділу із забезпечення кібербезпеки та кіберзахисту Збройних Сил України на стратегічному, оперативному та тактичному рівнях. У цьому контексті нормативно було встановлено, що до кінця 2020 року Міністерством оборони України спільно з Держспецзв'язку заплановано: створення відділу безпеки інформації та відділу кібербезпеки в Головному управлінні зв'язку та інформаційних систем (*J6*); забезпечення розвитку підрозділів захисту інформації та кібербезпеки інформаційно-телекомунікаційної системи Збройних Сил України; створення регіональних центрів захисту інформації та кібербезпеки в містах Вінниця, Чернігів, Миколаїв; посилення спроможності Збройних Сил України в напрямі створення системи захисту інформації та кібербезпеки з урахуванням базових стандартів НАТО; забезпечення виконання вимог нормативних документів у сфері захисту інформації та протидії технічним розвідкам тощо.

Таким чином, Міністерство оборони України, Генеральний штаб Збройних Сил України на виконання політичних рішень і нормативно-правових актів у рамках реформування сектору безпеки і оборони України поступово впроваджують заходи, спрямовані на повномасштабне забезпечення безпеки в кіберпросторі, здійснюючи це на планових засадах у військовій сфері. При цьому державна політика у сфері забезпечення

кібербезпеки також повинна враховувати заходи розвитку ринку сучасних інформаційних технологій та інновацій у контексті взаємодії ІТ-сектору та держави. Проте цей процес триває у нашій країні дуже повільно. Тільки у травні 2021 року питання щодо створення в Україні кібервійськ стало предметом розгляду на черговому засіданні РНБО України. Адже створення кібервійськ стосується не тільки закупівлі комп'ютерів та відповідного обладнання, а також побудови захищеного *data*-центру, пошуку кваліфікованих фахівців та формування відповідного людського ресурсу професіоналів.

Висновки.

Виклики та загрози у кіберпросторі сьогодні набагато небезпечніші, ніж поширення ядерної зброї. Головним безпековим аспектом у воєнній сфері на національному рівні залишається розв'язана Російською Федерацією гібридна війна проти України, яка ведеться у формі комбінації різноманітних дій прихованого застосування регулярних військ (сил), незаконних збройних формувань і терористичних організацій, використання пропаганди, саботажу, тероризму, вчинення диверсій, навмисного завдавання шкоди громадянам, юридичним особам та об'єктам критичної інфраструктури в Україні. Метою цих дій є посягання на територіальну цілісність, дестабілізація соціально-політичної ситуації, гальмування соціально-економічного розвитку, європейської та євроатлантичної інтеграції, відновлення свого впливу в Україні, зміна її територіального устрою, зокрема шляхом повномасштабного застосування воєнної сили проти України. На цьому фоні важливим напрямком залишається розвиток інституційних спроможностей Міністерства оборони України та інших складових сил оборони з метою посилення кібербезпеки. У зв'язку з цим Україна максимально підтримує ідею створення кібервійськ у НАТО, які можуть стати одним із найпотужніших альянсів, враховуючи рівень проникнення інформаційних технологій в усі сфери життєдіяльності держави.

В умовах потенційної ескалації Російською Федерацією збройної агресії проти України, можуть застосовуватися методи воєнної сили проти України шляхом проведення військових операцій з рішучими діями, що може супроводжуватись інформаційними кампаніями, інформаційно-психологічними операціями, кібероперераціями та спеціальними операціями проти України тощо. Зокрема, Російська Федерація активно реалізує концепцію інформаційного протиборства, базовану на симбіозі бойових дій у кіберпросторі та інформаційних операцій, механізми якої активно застосовуються в процесі гібридної війни проти України. Країни ЄС, НАТО, провідні міжнародні компанії та експерти одностайно визнають Російську Федерацію та її дії у кіберпросторі головною загрозою міжнародній кібербезпеці. Її розвідувально-підривна діяльність у кіберпросторі є частиною гібридної війни, яку вона веде проти України. Така деструктивна активність створює реальну загрозу вчинення актів кібертероризму та кібердиверсій стосовно об'єктів національної інформаційної інфраструктури.

Таким чином, кіберпростір визнано одним з можливих театрів воєнних дій. Тому спроможність держави захищати національні інтереси в ньому розглядається як важлива складова кібербезпеки. Набирає сили загальносвітова тенденція зі створення нового роду військ – кібервійськ, до завдань яких належить не лише забезпечення захисту критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі, спрямованих на знищення обчислювальних мереж та інформаційних систем збройних сил противника, а також виведення з ладу критично важливих об'єктів противника шляхом руйнування інформаційних систем, які управляють такими об'єктами.

За таких умов для України надзвичайно важливим є прискорення створення підрозділу кібервійськ. Тобто розвиток спроможностей щодо забезпечення кібербезпеки, кіберзахисту та кібероборони під час підготовки та ведення всеохоплюючої оборони України є важливим та актуальним завданням політичного керівництва держави, що неможливе без досягнення Міністерством оборони України необхідних інституційних спроможностей з метою забезпечення формування та реалізації державної політики у воєнній сфері [6].

Використана література

1. Красноступ Г.М. Організаційно-правове забезпечення протидії інформаційній агресії іноземних держав. *Правова інформатика*. № 2(42)/2014. С. 129-131.

2. Косогов О.М. Сірик А.О. Сучасна політика безпеки кіберпростору в умовах його мілітаризації. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2015. №3. С. 181-186.

3. Лук'янчук Р.В. Міжнародне співробітництво у сфері забезпечення кібернетичної безпеки: державні пріоритети. *Вісник Національної академії державного управління при Президентові України*. 2015. № 4. С. 50-56;

4. Паламарчук С.А. Шемендюк О.В., Ляшенко Г.Т., Ткач В.О. Забезпечення захисту кіберпростору в провідних країнах світу. *Збірник наукових праць ВІТІ*. 2020. № 1. С. 58-64.

5. Про рішення Ради національної безпеки і оборони України від 20 травня 2016 року "Про Стратегічний оборонний бюлетень України": Указ Президента України від 06.06.16 р. № 240/2016. URL: https://zakon.rada.gov.ua/laws/show/240/2016#Text (дата звернення: 20.05.2021).

6. Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року "Про Стратегію воєнної безпеки України": Указ Президента України від 25.03.21 р. № 121/2021. URL: https://www.president.gov.ua/documents/1212021-37661(дата звернення: 20.05.2021).

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