DOI:**10.33099/2311-7249/2023-46-1-23-31**

УДК: 338.242(477)

Олександр Васильович Терновий
Олексій Миколайович Шкуренко
Людмила Миколаївна Міненко ***(доктор філософії)***

Національний університет оборони України імені Івана Черняховського, Київ, Україна

ПРОБЛЕМНІ АСПЕКТИ КІБЕРОБОРОНИ: МІСЦЕ ТА РОЛЬ КІБЕРЗАХИСТУ В ЗБРОЙНИХ СИЛАХ УКРАЇНИ

У статті розглянуто проблемні аспекти кібероборони нашої держави, а також місце та роль кіберзахисту в Збройних Силах України. Акцентовано зосередженість на тому, що формування інформаційного суспільства зумовило численні кібернетичні загрози. Показано, що кіберпростір не лише надає ресурси і можливості, а несе певні проблеми, що мають руйнівний характер, спричиняють небезпеку існуванню держави, її функціонуванню та розвитку. Звернуто увагу, що Україна не є в числі передових у сфері інформаційно-комунікаційних технологій і кібероборони серед цивілізованих країн світу. Аргументовано, що саме такі напрями наукових досліджень є надзвичайно актуальними тому, що кібернетичний захист є стратегічно важливим як у цивільній царині, так і в сфері військової діяльності. Доведено, що в умовах війни Україна є однією з країн, яка найбільше потерпає від кіберзагроз. Головну небезпеку, в цьому сенсі, становить російська федерація, як військовий агресор. Підкреслено, що саме тому одним із основних завдань сьогодення є забезпечення кібернетичної безпеки. Проаналізовано наукові праці за темою статті, систематизовано та охарактеризовано зміст нормативно-правових актів України в сфері кібербезпеки, висвітлено заходи, що передбачено для підготовки до протистояння інформаційній агресії й кібернетичним атакам. Означено, що вже сьогодні є ряд проблемних питань стосовно кібероборони держави, що потребують нагального вирішення. Згруповано і представлено низку практичних рекомендацій для Міністерства оборони України і Збройних Сил України, щодо доцільності виконання нормативно-правових й адміністративно виважених кроків та використання алгоритму їх реалізації.

Ключові слова: *кіберпростір; інтерактивне інформаційне середовище; кібероборона; кібербезпека; кіберзагрози; кіберзахист; рекомендації стосовно кібероборони держави.*

Вступ

Постановка проблеми. Швидкий розвиток інформаційних технологій і комп'ютеризації зумовили формування інформаційного суспільства та, водночас, виникнення глобального кібернетичного простору, що відзначається невичерпним потенціалом поєднання можливостей отримання інформації і знань й відіграє провідну роль в економічному та соціальному розвитку передових країн світу. Фактично, кіберпростір виступає середовищем, де виробляється і поширюється різнопланова інформація, що створена та працює на основі принципів і методів кібернетики. По суті, сьогодні він є абсолютно новим двигуном зростання економіки, сучасною основою соціального управління, інноваційним способом міжнародного співробітництва та інтерактивною інформаційною сферою, що прямо впливає на безпеку державного суверенітету країни, спонукає займатися питаннями кібероборони. Реально, тотальна цифровізація та інфокомунікаційний зв'язок збільшили ризики кібербезпеки (комплексу заходів, що допомагають мінімізувати негативні наслідки від кібератак), зробивши суспільство вразливішим до кіберзагроз і розширивши коло специфічних проблем, з якими стикаються люди. Саме тому, протидія загрозам, у першу чергу національній безпеці, що надходять з кіберпростору, набула абсолютно нового сенсу. Варто зазначити, що кіберзагрози дедалі почастішали, стали більш організованими і збитковими для державної економіки в цілому та об'єктів критичної інфраструктури зокрема. Вони здатні досягти небезпечного рівня і негативно вплинути на національний розвиток та євроатлантичні прагнення нашої держави, безпеку і стабільність європейської спільноти. Джерелами таких загроз можуть бути іноземні військові й розвідувальні служби, організовані злочинні угруповання, терористичні та екстремістські групи тощо. За сформованих умов, основним завданням державних органів безпеки та оборони України, є застосування заходів, спроможних зменшити, а іноді, й цілком унеможливити негативні наслідки кіберзагроз. Значну роль у виробленні загальновизнаних підходів стосовно забезпечення кібербезпеки відіграє Організація

Північноатлантичного договору (або Північноатлантичний альянс) (далі – НАТО) як складова національної безпеки країн-членів договору. Сукупність способів потенційного застосування кіберзасобів висуває перед НАТО одне з головних завдань щодо розуміння її власної ролі в створенні умов для функціонування необхідних процесів кібербезпеки країн-членів і країн-партнерів Альянсу. Отже, актуальність нашого дослідження полягає у розгляді практичних питань кібероборони, у першу чергу місця і ролі кібернетичного захисту інформаціїї, зокрема, у Збройних Силах України (далі – ЗС України), в співпраці з НАТО.

Аналіз останніх досліджень і публікацій. Вивчення наукових праць вітчизняних вчених та аналіз нормативно-правових актів України і НАТО дозволило сформувати виклад основного матеріалу статті. Зокрема, В. Ліпкан та О. Ліпкан опрацювали понятійний апарат у сфері національної і міжнародної безпеки [7]. Основи кібернетичної безпеки і світові тенденції та виклики для України у цій сфері виклали Р. Грищук, Ю. Даник, В. Бурячок, В. Толубко, В. Хорошко, С. Толюпа , Д. Дубов, М. Ожеван [2; 3; 4]. Проблеми і перспективи подолання кіберінтервенції та кібербезпеки визначив і дослідив Ю. І. Грицюк [1]. Огляд практичних питань організації створення кібервійськ України і рекомендації щодо визначення їхніх завдань визначили і розробили Р. Кирилюк та Є. Шелест [5]. Правове забезпечення системи кібернетичної безпеки України, основні напрями її вдосконалення, а також деякі практичні питання в сфері попередження правопорушень у кіберпросторі роз'яснили О. Климчик, С. Мельник, В. Кащук, В. Шеломенцев [6; 8; 9]. Науковці В. Дідик, А. Гончарук., І. Сімоненкова висвітлили основні проблеми кіберзахисту в ЗС України у ході протидії можливим варіантам кіберзлочинності [11]. Кібербезпеку як напрям євроатлантичної інтеграції України розглянув А. Войціховський [12]. Крім того, питання підготовки фахівців у сфері кібербезпеки, в частині забезпечення дистанційного навчання, авторами статті розглядалося з точки зору дотримання норм Стратегії програми НАТО з удосконалення військової освіти (DEEP) [10]. Головним чином, з'ясуванню теми сприяло вивчення національних нормативно-правових актів, а саме:

Указів Президента України: «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про Доктрину інформаційної безпеки України"» від 25.02.2017 р. №47/2017; «Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки України"» від 14.09.2020 р. №392/2020; «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України"» від 15.03.2016 р. №96/2016; «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"» 26 серпня 2021 року № 447/2021; «Про Положення про Генеральний штаб Збройних Сил України» від 30.01.2019 р. № 23/2019; «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про невідкладні заходи з кібероборони держави"» від 26.08.2021 р. № 446/2021; «Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року "Про Стратегічний оборонний бюлетень України"» від 17.09.2021 р. № 473/2021, а також:

Законів України: «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. № 2163-VIII; «Про національну безпеку України» від 21.06.2018 р. № 2469-VIII; «Про оборону України» від 06.12.1991 р. № 1932-XII.

Мета статті. Окреслити проблемні аспекти кібероборони нашої держави, кокретизувати місце та роль кіберзахисту в Збройних Силах України, розробити практичні рекомендації.

Виклад основного матеріалу дослідження

В Указі Президента України «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про Доктрину інформаційної безпеки України"» від 25.02.2017 р. №47/2017 вказується, що важливою загрозою національним інтересам та національній безпеці України в інформаційній сфері є здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу ЗС України та інших військових формувань, а також провокування екстремістських проявів, підживлення панічних настроїв, загострення й дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання в Україні міжетнічних і міжконфесійних конфліктів. Так, дійсно, як показує практика, проблематика захисту від кібернетичних загроз є одним із головних пріоритетів для збройних сил будь-якої країни. Україна не стала винятком. Починаючи з 2014 року наша держава була змушена давати відсіч гібридній російській збройній агресії, включаючи кіберпростір. Однак, офіційне визнання необхідності кібероборони відбулось лише у березні 2016 року завдяки Указу Президента України «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України"» від 15.03.2016 р. №96/2016. Зміни і доповнення до нього були введені Указом Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"» від 26 серпня 2021 року № 447/2021.

Відповідно до цієї Стратегії, національна система кібербезпеки перебуває у віданні Міністерства оборони України (далі – МО України), Державної служби спеціального зв'язку

та захисту інформації України (далі – ДССЗЗІ України), Служби безпеки України (далі – СБ України), Національної поліції України та Національного банку України. Через це, вперше, для МО України і Генерального штабу Збройних Сил України (далі – ГШ ЗС України) було визначено додаткові завдання: здійснення заходів щодо підготовки держави до відбиття воєнної агресії в кіберпросторі (кібероборони); здійснення військової співпраці з НАТО у поєднанні із забезпеченням безпеки кіберпростору та спільного захисту від кіберзагроз; забезпечення за допомогою тісної взаємодії з ДССЗЗІ України України і СБ України кіберзахисту інформаційної інфраструктури. З цією метою утворено Національний координаційний центр кібербезпеки, що став робочим органом Ради національної безпеки і оборони України (далі – РНБО України). Основними завданнями цього органу затверджено розроблення і внесення до РНБО України та подання її Голові пропозицій стосовно: здійснення заходів, спрямованих на державну підтримку стратегічно вагомих для кібероборони держави наукових установ і організацій; зростання рівня дієвості реалізації військово-технічної політики й політики військово-технічної співпраці в сфері кібероборони; гарантування належного стану кібероборонних можливостей країни [9, 311]. Водночас, Указ Президента України «Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки України"» від 14.09.2020 р. №392/2020 провідними загрозами національній безпеці України в інформаційній сфері визначив ведення інформаційної війни проти України й відсутність структурованої комунікативної політики держави та належний рівень медіа-культури суспільства.

Крім того, варто зазначити, що ще у 2015 році науковці В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко , С. В. Толюпа виокремили основні напрями державної політики стосовно забезпечення інформаційної безпеки, що були враховані у процесі розроблення вищезгаданої Стратегії національної безпеки України, а саме: реалізація політики інформаційної безпеки на основі асиметричних дій проти всіх форм та проявів інформаційної агресії; розробка інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них; протидія інформаційним операціям проти України, маніпуляціям свідомістю населення та поширенню спотвореної інформації, захист національних цінностей та зміцнення єдності українського суспільства; впровадження регульованої інформаційної політики органів державної влади та ін. [4]. Зі свого боку, зустріч голів держав і голів урядів країн-членів НАТО, що відбулась у Варшаві у 2016 році, підтвердила важливість кіберзахисту для функціонування органів державної влади України та її Збройних Сил. На зустрічі вперше було підписано Договір між Європейським союзом (далі – ЄС) і НАТО про співробітництво в сфері безпеки, зокрема, це стосувалось питань гібридних війн і кібератак. Тож було окреслено такі пріоритетні сфери діяльності, як: протистояння гібридним загрозам; оперативне реагування й співробітництво у військово-морській сфері; кібербезпека та оборона; потенційні можливості захисту, оборонні промислові й відповідні наукові дослідження; тренування та узгодження дій партнерів. МО України підтримало проєкт НАТО, що спрямовувався на підготовку фахівців у сфері кібербезпеки. Так, фахівці Альянсу розробили Стратегію програми НАТО з удосконалення військової освіти (DEEP), до якої долучились не лише країни-члени НАТО, а й партнери, серед яких – Україна [10].

Саме тому, в Законі України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. № 2163-VIII (далі – Закон про кібербезпеку) було вперше визначено необхідні терміни цієї проблеми, а саме: *кібербезпека* – належний стан захисту життєво вагомих інтересів людини та громадянина, суспільства і держави під час використання кіберпростору, за якої забезпечений стабільний розвиток інформаційного суспільства та цифрового комунікативного середовища, вчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національній безпеці України у кіберпросторі; *кіберзахист* – сукупність організаційних, нормативно-правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, що спрямовуються на запобігання кібервипадкам, протидії кібератакам, ліквідацію їх наслідків, відновлення стабільності та надійності функціонального існування комунікаційних та технологічних систем; *кібероборона* – комбінація, що включає політичні, економічні, соціальні, військові, наукові, науково-технічні, інформаційні, правові, організаційні та ряд інших заходів, що здійснюються у кіберпросторі та спрямованих на захист суверенітету та обороноздатності держави, запобігання збройним конфліктам і відсіч збройним агресіям. Підсумково, Законом про кібербезпеку для МО України та ГШ ЗС України визначено те, що вони мають: здійснюватися заходи із забезпечення готовності держави до відбиття воєнної агресії у кіберпросторі (кібероборони); організовувати і проводити військову співпрацю з НАТО та різними суб'єктами оборонної сфери стосовно забезпечення безпеки кіберпростору й спільного захисту від кіберзагроз. Окремо передбачається те, що повинні впроваджуватись заходи із забезпечення кіберзахисту критичної інформаційної інфраструктури у випадках надзвичайного і воєнного стану [13].

Разом із тим, для посилення уваги до кібероборони, у жовтні 2017 року до Закону України «Про оборону України» від 06.12.1991 р.

№ 1932-XII було внесено зміни, що передбачають підготовку держави до оборони в мирний час, під час якої мають бути реалізовані заходи стосовно кібероборони (активний кіберзахист) з метою захисту суверенітету держави, забезпечення її обороноздатності, запобігання збройним конфліктам і відсічі збройним агресіям [14]. У подальшому, не менше важливим національним нормативно-правовим актом для гарантування кібербезпеки став Закон України «Про національну безпеку України» від 21.06.2018 р. № 2469-VIII. Його засади частково розкрили особливості Стратегії кібербезпеки України. В Законі викладено винятково загальні положення, що не містять конкретних заходів. Це призвело до недоліків у сфері безпеки та оборони України, наслідком чого продовжилися збої в роботі органів державної влади, приватного бізнесу та ін.

Тому, з метою конкретизації заходів з оборони нашої держави і, зокрема, кібероборони, Указом Президента України «Про Положення про Генеральний штаб Збройних Сил України» від 30.01.2019 р. № 23/2019 (далі – Положення про ГШ ЗС України) було затверджено відповідне Положення. Серед основних його завдань визначено: організовувати розгортання, здійснювати управління та забезпечувати функціональне існування системи захисту інформації та кіберзахисту в інформаційно-телекомунікаційних системах МО України і ЗС України; брати участь у створенні національної системи кібербезпеки та проведенні її огляду на періодичній основі; організовувати планування та виконання у межах компетенції заходів з підготовки держави до відбиття воєнних агресій в кіберпросторі (кібероборони); координувати виконання завдань щодо підготовки до кібероборони органами виконавчої влади, органами місцевого самоврядування та іншими складовими сил оборони; забезпечувати інформаційну безпеку в ЗС України і протидіяти системним та масштабним діям проти інтересів України в кіберпросторі. Фактично, це дії з боку іноземних держав (груп держав) із одночасним залученням кіберпідрозділів збройних сил іноземних держав з одночасним використанням спеціальних засобів (кіберозброєнь) [15].

Згодом, для покращення вирішення стратегічно важливих національних питань оборонного характеру, у тому числі й заходів з кібербезпеки, на початку лютого 2020 року в ЗС України були створені чотири нові командування та призначені їхні командувачі. Одним із вказаних командувань стало Командування Військ зв'язку та кібернетичної безпеки ЗС України. Через це, наприкінці березня 2020 року, внесено зміни до Положення про ГШ ЗС України, відповідно до яких даний орган військово управління додатково: організовує планування операцій ЗС України та інших складових сил оборони у кіберпросторі; у тісній взаємодії з ДССЗЗІ України та СБ України займається організацією кіберзахисту інформаційної інфраструктури МО України та ЗС України [15].

Отже, як зазначалося вище, 26 серпня 2021 року було затверджено нову редакцію Стратегії кібербезпеки України. Чинною вона стала завдяки виданню Указу Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"» від 26.08.2021 № 447/2021. Принципово важливим у цьому нормативному документі стало те, що першою стратегічною ціллю у формуванні потенціалу стримування визначено дієву кібероборону для досягнення якої Україна має: створити і забезпечити розвиток підрозділів із повноваженнями ведення збройного протиборства в кіберпросторі; сформувати належну правову, організаційну і технологічну модель їх функціонування та застосування; здійснити забезпечення ефективної взаємодії головних суб'єктів національної системи кібербезпеки і сил оборони під час здійснення заходів з кібероборони, належний рівень навчання та фінансового забезпечення цих структур; організувати систематичне проведення кібернавчань, оцінювання спроможностей та ефективності підрозділів, розробку та імплементацію індикаторів оцінки їх діяльності [16].

Водночас, Указом Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про невідкладні заходи з кібероборони держави"» від 26.08.2021 р. № 446/2021 Кабінету Міністрів України, з метою створення в системі МО України кібервійськ і набуття ними відповідних спроможностей, доручено здійснити розрахунки потреб щодо: обсягу матеріально-технічних і фінансових ресурсів, необхідних для створення й забезпечення належного функціонування кібервійськ; комплектування особового складу кібервійськ з урахуванням оптимального співвідношення військовослужбовців, працівників МО України, а також зарахованих у запас, резервістів та інших категорій осіб [17].

Крім того, Указом Президента України «Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року "Про Стратегічний оборонний бюлетень України"» від 17.09.2021 р. № 473/2021 було затверджено черговий Стратегічний оборонний бюлетень України. У цьому документі 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. Також Указом 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 [18].

Отже, здійснивши огляд головних нормативно-правових актів, що регулюють сферу кібербезпеки України та її Збройних Сил, з метою підкреслення актуальності цієї проблеми додатково розглянемо деякі питання захисту інформації під час застосування електронних

систем обміну даними, що використовуються МО України і підпорядкованими йому підрозділами. Так, дійсно, у Законі про кібербезпеку зазначено, що вдосконалення систем інформаційної і кібербезпеки, систем захисту інформації та безпеки інформаційних ресурсів є серед головних завдань МО України та ГШ ЗС України [13]. Цим же законом окреслено інші завдання, зокрема: забезпечення інформаційної та кібербезпеки; посилення спроможностей зміцнення інституціональних і технічних можливостей суб'єктів сектору безпеки та оборони з метою дієвої боротьби з кіберзагрозами воєнного характеру, кіберзлочинністю, кібершпигунством, та кібертероризмом; поглиблення міжнародного співробітництва у цій сфері; формування підрозділів забезпечення кібербезпеки й кіберзахисту ЗС України; здійснення міжвідомчої координації та взаємодії з цих питань в інтересах забезпечення обороноздатності держави; створення необхідних матеріально-технічних ресурсів для забезпечення здатності протидіяти іноземним технічним розвідкам, інформаційним, кібернетичним атакам, спецопераціям противника; створення ефективних сучасних зразків кіберзброї; розвитку Мережі реагування на комп'ютерні надзвичайні події «Команда реагування на комп'ютерні надзвичайні події України» (англ. «Computer Emergency Response Team of Ukraine») (далі – CERT-ua).

Через це, важливе значення має той факт, що з початку 2014 року головний орган військового управління ЗС України під час обміну інформацією в електронних системах для захисту конфіденційності документа використовує криптографічні засоби, а саме електронно-цифровий підпис. Означений підпис може бути застосований завдяки використанню відкритого ключа, підтвердження належності фізичній чи юридичній особі якого здійснюється спеціальною організацією або підрозділом у ЗС України та акредитованим центром сертифікації ключів, який, таким чином, забезпечує надійність і захист криптографічних ключів.

З огляду на це, науковці В. Дідик., А. Гончарук та І. Сімоненкова акцентували увагу на тому, що для надійного протистояння кіберзлочинам у ЗС України, завдяки використанню надсучасних програмних алгоритмів, має бути створена система протидії, яка здатна протистояти атакам і втручанням в роботу інформаційно-телекомунікаційних систем (далі – ІТС). Тобто, на різних рівнях кіберпростору необхідно застосовувати систему захисту інформації, що гарантуватиме здійснення таких заходів: розмежування доступу користувачів до ІТС із використанням криптографічного захисту інформації під час зберігання та обміну нею; застосування міжмережевого екранування з одночасним використанням маршрутизаторів та фаєрволів; забезпечення створення й практичного застосування віртуальних приватних мереж; системне використання антивірусного захисту; унеможливлення застосування програмних продуктів потенційними опонентами; застосування системи виявлення вторгнень (IDS) за умови використання підсистеми профілактики вторгнень (IPS); встановлення механізму автентифікації й авторизації; забезпечення резервного зберігання даних на носіях інформації, до яких обмежений будь-який несанкціонований доступ [11].

Натомість, маємо констатувати, сьогодні, організування і керівництво забезпеченням кібербезпеки й виконання інших функцій управління зв'язку, у тому числі зазначених вище заходів, здійснюють підрозділи ГШ ЗС України, а саме: Головне управління зв'язку та кібербезпеки (далі – ГУЗК ГШ ЗС України) і Центральне управління охорони державної таємниці та захисту інформації (ЦУ ОДТта ЗІ ГШ ЗС України). З метою захисту інформації та протидії кіберзагрозам підрозділи ГУЗК ГШ ЗС України співпрацюють зі СБ України, ДССЗЗІ України, Національною поліцією України. Крім того, вони взаємодіють із CERT-ua, що входить до структури ДССЗЗІ України, і виконують завдання в сфері кібернетичного захисту національної

інформаційної системи України. Водночас, задля протидії кіберзагрозам у ЗС України функціонують окремі підрозділи, що стежать за належним станом використання ІТС на організаційному, технічному й правовому рівнях. Проте, незважаючи на заходи, що гарантують захист інформації у кіберпросторі, мусимо констатувати прояви негативних факторів, що впливають на якість кіберзахисту ЗС України, зокрема: дефіцит спеціалістів ІТ напряму відповідної підготовки для роботи у кіберпросторі й протидії кіберзагрозам; відсутність належним чином затвердженої для кожного рівня управління штатної структури, положень про структурні підрозділи, посадові інструкції і відповідно підібраних фахівців, які спроможні діяти проти будь-яких потенційних кіберзлочинів і працювати в команді; нестача, а в окремих випадках, повна відсутність сучасного технічного забезпечення, інформаційних та інфокомунікаційних технологій, призначених для захисту і протидії кіберзагрозам; нестача ліцензійного програмного забезпечення і невикористання антивірусних захистів; низький рівень обізнаності особового складу, що працює на персональних комп'ютерах, про правила їх використання, недопущення потрапляння і подальшого поширення шкідливого програмного забезпечення [11].

На наше переконання, за умов, що склалися для МО України та ЗС України важливим і вкрай

необхідним є питання розробки та затвердження ІТ-стратегії, якою має передбачатися створення єдиної системи управління з власним центром обробки даних і започаткуванням роботи підрозділів з кібербезпеки. За таких обставин, нова ІТ-стратегія має передбачати практичне формування дієздатних підрозділів оборонного відомства в сфері кіберборотьби не лише на верхніх рівнях управління, а й у військових частинах (підрозділах), що комплексно забезпечуватиме надійну і захищену обробку даних. Також, доцільно внести зміни і доповнення до діючих нормативно-правових актів, що регулюють нагальні проблеми національного кіберпростору, враховуючи вимоги стандартів НАТО і міжнародних стандартів в галузі ІТ (ISO/IEC).

Отже, як показує практика цивілізованих країн світу, організація високого рівня кібероборони вимагає вирішення цілої низки важливих завдань і, насамперед, усунення прогалин у нормативно-правовій базі. Як можна було пересвідчитися, дотепер законодавством України не конкретизовано основи кібероборони, що унеможливлює адекватне формування завдань для кібервійськ, які мають відігравати провідну роль у виконанні практичних заходів кібероборони і повинні бути створені на вимогу Указу Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про невідкладні заходи з кібероборони держави"» від 26.08.2021 р. № 446/2021.

Саме тому, слід розробити та ухвалити окремий Закон України «Про кібероборону України», в якому, з-поміж решти аспектів, визначити особливості національної кібероборони, її суб'єкти та об'єкти, мету (цілі), принципи і завдання, структуру побудови та управління, вимоги до підготовки кадрів, специфіку організування і реалізації. Крім того, унормувати місце і роль кібервійськ ЗС України в ній, а також – відповідні повноваження, функції та завдання органів військового управління, ряду інших державних інституцій, обов'язки, права і відповідальність посадових осіб, а також права й обов'язки громадян України та ін. Тобто, законодавчо варто передбачити необхідність реформування існуючих Військ зв'язку і кібербезпеки ЗС України в окремі спеціальні війська, зокрема, у Війська зв'язку ЗС України і Кібервійська ЗС України. Для цього доцільно врахувати досвід США та інших країн-членів НАТО. Структура, склад і чисельність новостворених Кібервійськ ЗС України мають, насамперед, окреслюватися на основі визначених для них переліку й обсягів завдань, спрямованих на забезпечення кібероборони України, їхні частини та підрозділи – входити до структури всіх видів та окремих родів військ (сил) ЗС України.

За таких умов варто переформувати сучасне Командування Військ зв'язку та кібербезпеки ЗС України у Командування сил кібероборони ЗС України. Реформоване Командування повинне займатися питаннями ведення кібернетичної, радіоелектронної та інформаційної боротьби, протидії технічним розвідкам противника та управління електромагнітним спектром. Його склад повинен включати наступні компоненти: кібервійська ЗС України; Війська радіоелектронної боротьби ЗС України, які зараз перебувають у підпорядкуванні Командування сил підтримки ЗС України; сили й засоби здійснення інформаційних операцій; структуру з управління електромагнітним спектром. У зв'язку із запропонованим, у проєктах Державних Програм розвитку ЗС України та їхнього озброєння і військової техніки, а також у Стратегічному плані застосування ЗС України та інших документах оборонного планування і планування оборони держави доречно конкретизувати мету (цілі), завдання і заходи з розвитку Кібервійськ ЗС України, вимоги до підготовки їхнього особового складу та практичне застосування.

Для повноцінного аналізу ситуації, доцільно також визнати, що на сьогодні, разом із не вирішеними кадровими, фінансовими, матеріально-технічними і нормативними проблемами, стосовно зміцнення кібероборони держави й створення ефективних Кібервійськ ЗС України, існує ще одна, більш складна. Ця проблема стосується зміни усвідомленого системно-персонального мислення і дій щодо перспектив розвитку цієї сфери. У даному випадку мається на увазі відмова від комплексного розгляду питань кібероборони, здебільшого, через призму виконання заходів кіберзахисту і кібербезпеки ЗС України й набуття ними спроможностей для виконання поставлених завдань всеохоплюючої оборони держави, першочергово її кібероборони, в кіберпросторі та через кіберпростір. Зважаючи на вищевикладені застереження, вважаємо за доцільне висловити власне бачення вирішення проблем кібероборони держави і посилення ролі кіберзахисту в ЗС України, а саме:

розробити і внести в установленому порядку на розгляд РНБО України проєкт Стратегії кібероборони України і, за таких умов, звернути увагу не лише на кіберзахисних (кібероборонних) діях об'єднаних сил/військ кібероборони, а й інших напрямах діяльності;

визначити цілі, завдання і заходи щодо розбудови об'єднаних сил/військ кібероборони, організування їх ефективної підготовки з метою подальшого використання під час відбивання збройних агресій. Пропонується вказані аспекти передбачити у проєктах Стратегії воєнної безпеки України, Стратегічному оборонному бюлетені України, Державних програмах розвитку ЗС України та їх озброєння і військової техніки, а також у проєкті Плану оборони України. Водночас, першочергово врахувати в проєкті Стратегічного плану застосування ЗС України,

інших структурних частинах сил оборони з відсічі збройній агресії;

окреслити в нормативно-правових актах структуру системи кібероборони держави, завдання, функції і склад суб'єктів її забезпечення, а також об'єкти кібероборони;

відобразити в Щорічному плані Кабінету Міністрів України заходи по реалізації Стратегії кібербезпеки України, що застосовуватимуться МО України і ГШ ЗС України з метою посилення кібероборони держави й підвищення кібероборонних спроможностей об'єднаних сил/військ кібероборони, першочергово, для виконання яких, надаватиметься допомога з боку НАТО;

унормувати термін «кібероборонні спроможності» і його поняття у Військовому стандарті 01.004.002-2019(02) «Воєнна безпека. Стратегічне планування. Терміни та визначення» від 01.01.2020 р. й внести його до Єдиного переліку (каталогу) спроможностей МО України, ЗС України та інших складових сил оборони, затвердженого Наказом МО України «Про затвердження Порядку організації та здійснення оборонного планування в МО України, ЗС України та інших складових сил оборони» від 22.12.2020 р. № 484. Використовувати цей термін під час оборонного планування і планування оборони країни;

врахувати те, що Директорат інформаційної політики в сфері оборони і стратегічних комунікацій МО України й Департамент військово-технічної політики, розвитку озброєння та військової техніки МО України, мають під час формування і реалізації воєнної й військово-технічної політики та політики військово-технічного співробітництва з іншими державами визначати пріоритети, напрями і заходи в сфері кібероборони України;

внести необхідні зміни до структури і штату Головного управління зв'язку й кібербезпеки ГШ ЗС України для підвищення його спроможностей у плануванні кібероборони держави та забезпечення належної реалізації інших повноважень ГШ ЗС України, пов'язаних із діями ЗС України у кіберпросторі;

скоригувати назву Командування Військ зв'язку та кібербезпеки ЗС України, замінивши в ній лексичну одиницю «кібербезпеки» на лексичну одиницю «кібероборони»;

окреслити в Положенні про Командування Військ зв'язку та кібероборони ЗС України виконання ним завдань з підготовки об'єднаних сил/військ кібероборони, нарощування їхніх кібероборонних спроможностей та ін.

Крім запропонованих рекомендацій, варто також звернути увагу на результати аналізу тенденцій у безпековій політиці НАТО, що був здійснений вітчизняним вченим А. Войціховським, і, на наше переконання, доцільно використати для гарантування національної кібероборони. Зокрема науковець засвідчив:

Україна потребує такої системи кібернетичної безпеки, що постійно трансформується і відповідає вимогам країн-членів НАТО, де виклики національній безпеці дедалі частіше отримують риси, відмінні від традиційних загроз. Питання захисту у кіберпросторі – невід'ємна складова реалізації державної політики в сфері забезпечення національної безпеки;

поглиблення співробітництва України з НАТО значною мірою посилює спроможності нашої країни в протидії кіберзагрозам. Завдяки використанню ресурсів Трастового фонду НАТО з кібербезпеки, Україна змогла зміцнити власний кіберзахист, а також співпраця вигідна Альянсу, оскільки дає змогу в реальних умовах випробувати технічні та організаційні рішення;

зважаючи на значний прогрес і досвід НАТО у виробленні та удосконаленні механізму забезпечення кібербезпеки країн-членів НАТО, Україна має стати активним учасником безпекових процесів. Беручи до уваги євроатлантичні прагнення України, це сприятиме покращенню її іміджу, а також впливатиме на формування організаційно-правової основи її національної кібербезпеки, залучення до Альянсу і формування моделі надійного захисту кіберпростору України;

в умовах розроблення національної системи кібербезпеки, дієвим фактором є запозичення досвіду країн-членів НАТО та їх певних органів щодо організації протидії кіберзагрозам, запровадження в Україні інформаційно-комунікаційних і технологічних стандартів НАТО, а також розвиток технічних можливостей груп реагування CERT на кібервипадки. В умовах російської агресії та запровадження практик електронного врядування питання кібербезпеки мають постійно перебувати в центрі уваги державної політики України [12].

Висновки та перспективи подальших досліджень

Підсумовуючи зазначимо, що в статті окреслено стан, проблеми і можливі перспективи щодо покращення кіберзахзисту в Збройних Силах України**.** У цьому контексті встановлено, що кібероборона, кібербезпека і кіберзахист є самостійними й водночас різними за змістом, складовими компонентами (суб'єктами та об'єктами) в діяльності кіберпростору України. Не зважаючи на таке розмежування, мусимо констатувати, що до нині залишаються невизначеними на рівні нормативно-правових актів структура кібероборони держави, склад, функції і завдання суб'єктів її забезпечення, а також об'єкти кібероборони. Наразі виконання провідних завдань із забезпечення кібероборони і кіберзахисту держави, відповідно до чинного законодавства, покладається на Міністерство оборони України та Генеральний штаб Збройних Сил України, що покликані застосовувати заходи з кібероборони (активного кіберзахисту) для забезпечення суверенітету держави, її

обороноздатності, запобігання збройним конфліктам і відсічі збройних агресій. Визнаючи, що кіберзахист як складова кібероборони, є важливою частиною сучасної загальної оборони держави, і з метою посилити кібероборону, запропоновано низку можливих, на думку авторів статті, рекомендацій для Міністерства оборони України і Збройних Сил України. На наше переконання, формування і реалізація державної політики України в сфері оборони мають здійснюватися з урахуванням пріоритетів, напрямів й заходів щодо кібероборони, кібербезпеки, кіберзахисту, а також у співпраці з НАТО.

Перспективи подальших досліджень полягають у вивченні специфіки залучення провідних засобів кіберзахисту в Збройних Силах України.

Література

1. Грицюк Ю.І. Кіберінтервенція та кібербезпека України: проблеми та перспективи їх подолання. *Науковий вісник НЛТУ України.* 2016. Вип. 26. С. 8. **2. Грищук Р.В., Даник Ю.Г.** Основи кібернетичної безпеки: монографія. Житомир : ЖНАЕУ, 2016. 636 с. **3. Дубов Д.В., Ожеван М.А.** Кібербезпека: світові тенденції та виклики для України. Київ : Вид-во НІСД, 2011. 30 с. **4. Бурячок В.Л., Толубко В.Б., Хорошко В.О., Толюпа С.В.** Інформаційна та кібербезпека: соціотехнічний аспект: підручник. Київ : ДУТ, 2015. 288 с. **5. Кирилюк Р., Шелест Є.** Кібервійська як складова трансформації системи національної безпеки. *Оборонний вісник :* Центр воєнної політики та політики безпеки. 2021. № 9. С. 4–10. **6. Климчик О.О**. Кримінально-правова кваліфікація використання комп'ютерних технологій для вчинення терористичних актів. *Інформаційна безпека людини, суспільства, держави.* 2010. №1 (3). С. 26–30. **7. Ліпкан В.А., Ліпкан О.С.** Національна і міжнародна безпека у визначеннях та поняттях. Київ : Текст, 2008. 400 с. **8. Мельник С.В., Кащук В.І.** Актуальні напрями попередження правопорушень у кіберпросторі як складова стратегії кібернетичної безпеки держави. *Інформаційна безпека: виклики і загрози сучасності* : зб. матеріалів наук.-практ. конф. 5 квітня 2013 р., м. Київ. Київ : Наук.-вид. центр НА СБ України, 2013. 416 с. **9. Шеломенцев В.П.** Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення. Боротьба з організованою злочинністю і корупцією (теорія і практика). 2012. Вип. 1. С. 312–320. **10. Стратегія** програми НАТО з удосконалення військової освіти (DEEP) в частині забезпечення дистанційного навчання. 2021. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2023/2/pdf/230208-deep-strategy-for-distance-learni-1.pdf (дата звернення: 05.12.2022). **11. Дідик В. О., Гончарук А. А., Сімоненкова І. В.** Кіберзахист в Збройних Силах України для протидії можливим варіантам кіберзлочинності. *Кібербезпека в Україні: правові та організаційні питання*: матер. Всеукр. наук.-практ. конф. (м. Одеса, 17 листопада 2017 р.). Одеса: Одес. держ. ун-т внутр. спр., 2017. С. 94–95. **12. Войціховський А. В.** Кібербезпека як напрям євроатлантичної інтеграції України. *Право і безпека у контексті європейської та євроатлантичної інтеграції*: збірник статей та тез наукових повідомлень за матеріалами дискусійної панелі II Харківського міжнародного юридичного форуму, м. Харків, 28 вересня 2018 р. / редкол: Ю. Г. Барабаш, Т. М. Анакіна, Д. В. Аббакумова. Харків : Право, 2018. С. 42–48. **13. Закон України** «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. № 2163-VIII URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 05.12.2022). **14. Закон України** «Про оборону України» від 06.12.1991 р. № 1932-XII. URL: https://zakon.rada.gov.ua/laws/show/1932-12#Text (дата звернення: 05.12.2022). **15. Указ Президента України** «Про Положення про Генеральний штаб Збройних Сил України» від 30.01.2019 р. № 23/2019. URL: https://zakon.rada.gov.ua/laws/show/23/2019#Text (дата звернення: 05.12.2022). **16. Указ Президента** України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"» від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 05.12.2022). **17. Указ Президента України** «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про невідкладні заходи з кібероборони держави"» від 26.08.2021 р. № 446/2021. URL: https://zakon.rada.gov.ua/laws/show/446/2021#Text (дата звернення: 05.12.2022). **18. Указ Президента України** «Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року "Про Стратегічний оборонний бюлетень України"» від 17.09.2021 р. № 473/2021. URL: https://www.president.gov.ua/documents/4732021-40121 (дата звернення: 05.12.2022).

PROBLEMATIC ASPECTS OF CYBER DEFENSE: PLACE AND ROLE OF CYBER DEFENSE IN THE ARMED FORCES OF UKRAINE

***Olexandr Ternovyy*[1]**
***Oleksii Shkurenko*[2]**
***Liudmyla Minenko (Ph.D.)*[3]**

The National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine

The article discusses the problematic aspects of our country's cyber defense, as well as the place and role of cyber defense in the Armed Forces of Ukraine. The authors emphasizes that the formation of the information society has led to numerous cyber threats. It is shown that cyberspace not only provides resources and opportunities, but also carries certain problems that are destructive in nature and pose a threat to the existence of the State, its functioning and development. The authors emphasizes that Ukraine is not among the leading

countries in the field of information and communication technologies and cyber defense among the civilized countries of the world. It is argued that such areas of scientific research are extremely relevant because cyber defense is strategically important both in the civilian sphere and in the military sphere. It has been proven that in times of war, Ukraine is one of the countries most affected by cyber threats. The main danger in this sense is posed by the Russian Federation as a military aggressor. It is emphasized that this is why one of the main tasks of today is to ensure cybersecurity. The authors analyzes scientific works on the topic of the article, systematizes and characterizes the content of Ukraine's regulatory legal acts in the field of cybersecurity, and highlights the measures envisaged to prepare for countering information aggression and cyber attacks. It is noted that today there are a number of problematic issues related to the cyber defense of the State that need to be urgently addressed. The authors groups and presents a number of practical recommendations for the Ministry of Defense of Ukraine and the Armed Forces of Ukraine regarding the expediency of taking regulatory and administrative steps and using an algorithm for their implementation.

Keywords: *cyberspace; interactive information environment; cyber defense; cybersecurity; cyber threats; cyber defense; recommendations for state cyber defense.*

References

1. Hrytsiuk, Yu. I. (2016). Cyber Intervention and Cybersecurity in Ukraine: Problems and Prospects for Overcoming Them. Naukovyi visnyk, 26, 8. **2. Hryshchuk, R. V., Danyk, Yu. H.** (2016). Basics of cyber security: monohrafiia. Zhytomyr : ZhNAEU, 636. **3. Dubov, D. V., Ozhevan, M. A.** (2011). Cybersecurity: global trends and challenges for Ukraine. Kyiv: Vyd-vo NISD, 30. **4. Buriachok, V. L., Tolubko, V. B., Khoroshko, V. O., Toliupa, S. V.** (2015). Information and cybersecurity: the socio-technical aspect: pidruchnyk. Kyiv : DUT, 288. **5. Kyryliuk, R., Shelest, Ye.** (2021). Cyber Forces as a Component of the National Security System Transformation. Oboronnyi visnyk : Tsentr voiennoi polityky ta polityky bezpeky, 9, 4–10. **6. Klymchyk, O. O.** (2010). Criminal Legal Qualification of the Use of Computer Technologies for Committing Terrorist Acts. Informatsiina bezpeka liudyny, suspilstva, derzhavy, 1(3), 26–30. **7. Lipkan, V. A., Lipkan, O. S.** (2008). National and international security in definitions and concepts. Kyiv : Tekst, 400. **8. Melnyk, S. V., Kashchuk, V. I.** (2013). Current Areas of Prevention of Offenses in Cyberspace as a Component of the State's Cyber Security Strategy: zb. materialiv nauk.-prakt. konf. 5 kvitnia 2013 r., m. Kyiv. Kyiv : Nauk.-vyd. tsentr NA SB Ukrainy, 416. **9. Shelomentsev, V. P.** (2012). Legal support of the cyber security system of Ukraine and the main directions of its improvement. Fighting organized crime and corruption (theory and practice), 1, 312–320. **10. Strategy of the NATO** Defence Education Enhancement Program (DEEP) in terms of distance learning. (2021). URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2023/2/pdf/230208-deep-strategy-for-distance-learni-1.pdf (data zvernennia: 05.12.2022). **11. Didyk, V. O., Honcharuk, A. A., Simonenkova, I. V.** (2017). Cybersecurity in the Armed Forces of Ukraine to counter possible variants of cybercrime. Kiberbezpeka v Ukraini: pravovi ta orhanizatsiini pytannia: mater. Vseukr. nauk.-prakt. konf. (m. Odesa, 17 lystopada 2017 r.). Odesa: Odes. derzh. un-t vnutr. spr., 94–95. **12. Voitsikhovskyi, A. V.** (2018). Cybersecurity as a direction of Ukraine's Euro-Atlantic integration. Pravo i bezpeka u konteksti yevropeiskoi ta yevroatlantychnoi intehratsii: zbirnyk statei ta tez naukovykh povidomlen za materialamy dyskusiinoi paneli II Kharkivskoho mizhnarodnoho yurydychnoho forumu, m. Kharkiv, 28 veresnia 2018 r. / redkol: Yu. H., Barabash, T. M., Anakina, D. V., Abbakumova. Kharkiv : Pravo, 42–48. **13. Law of Ukraine** «On the Basic Principles of Ensuring Cybersecurity of Ukraine», 05.10.2017, 2163-VIII URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (data zvernennia: 05.12.2022). **14. Law of Ukraine** «On Defense of Ukraine», 06.12.1991, 1932-XII. URL: https://zakon.rada.gov.ua/laws/show/1932-12#Text (data zvernennia: 05.12.2022). **15. Decree of the President of Ukraine** «On the Regulation on the General Staff of the Armed Forces of Ukraine», 30.01.2019, 23/2019. URL: https://zakon.rada.gov.ua/laws/show/23/2019#Text (data zvernennia: 05.12.2022). **16. Decree of the President of Ukraine** «On the Decision of the National Security and Defense Council of Ukraine of May 14, 2021 "On the Cybersecurity Strategy of Ukraine"», 26.08.2021, 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (data zvernennia: 05.12.2022). **17. Decree of the President of Ukraine** «On the Decision of the National Security and Defense Council of Ukraine of May 14, 2021 "On Urgent Measures for the State's Cyber Defense"», 26.08.2021, 446/2021. URL: https://zakon.rada.gov.ua/laws/show/446/2021#Text (data zvernennia: 05.12.2022). **18. Decree of the President of Ukraine** «On the Decision of the National Security and Defense Council of Ukraine of August 20, 2021 "On the Strategic Defense Bulletin of Ukraine"», 17.09.2021, 473/2021. URL: https://www.president.gov.ua/documents/4732021-40121 (data zvernennia: 05.12.2022).