DOI 10.33099/2618-1614-2024-26-3-45-54
УДК 355.4

П. М. Сніцаренко,
доктор технічних наук,
старший науковий співробітник,
Національний університет оборони України

Про сутність кібероборони як виду воєнних дій

Конституція України розмежовує сферу національної безпеки (отже, кібербезпеку як її складову) і сферу оборони. Тому питання кібероборони України та її теоретичних засад може розглядатися з точки зору, що це складова оборони держави. Аналіз засвідчив, що в сукупності чинних положень законодавства України стосовно оборони кібероборона є однією з функцій Збройних Сил України разом з іншими військовими формуваннями (отже, силами оборони) в разі збройної агресії проти України. Тобто йдеться не про кібероборону держави загалом, а лише про її складову у виконанні ЗСУ (сил оборони) у фазі відбиття (відсічі) збройної агресії (ведення кібероборони) – кібероборону у вузькому розумінні поняття «оборона», що слід розглядати як вид воєнних дій військ (сил). Між тим у законодавстві України та у відомих публікаціях така особливість не розкривається. Це означає, що на шляху до розуміння сутності кібероборони України як концептуально найважливішого теоретичного завдання, першочергово слід визначитися щодо кібероборони як виду воєнних дій військ (сил), що спричинило мету статті.

Поглиблений розгляд питання кібероборони з позиції законодавства України з питань оборони, ролі ЗСУ, кібервійськ у їхньому складі та інших суб'єктів сил оборони дав підстави визначити сутність кібероборони як виду воєнних дій, а також окреслити особливості реалізації основних заходів і структурно-логічну схему її організації в процесі відбиття збройної агресії проти України.

Ключові слова: оборона, кібероборона, кібероборона як вид воєнних дій, законодавство України.

Постановка проблеми. Поряд із традиційними сферами «Земля», «Море», «Повітря» та «Космос», «Інформаційний простір» сьогодні незворотньо став ареною протиборства. Держави світу активно опановують цей простір в інтересах реалізації своїх національних інтересів. Особливо це стало можливим завдяки бурхливому розвитку впродовж останніх кількох десятиліть інформаційних технологій та інформаційних систем на їхній основі, що призвело до утворення потужного сегмента загального інформаційного простору – простору електронних інформаційних ресурсів (EIP), який на підставі цієї головної сутності в різних інтерпретаціях розуміння одержав назву «кіберпростір».

Зауважмо, що інформаційні системи і технології, які утворюють кіберпростір, дають змогу синтезувати різні види інформаційних ресурсів (когнітивних, неелектронних та власне електронних) у форматі EIP (це електронна кодограма для їхнього створення, зберігання, обробки або передачі (представлення) споживачу). Цей формат є технічною основою та водночас умовою для інформаційної взаємодії між різними елементами глобального кіберпростору. При цьому взаємодія, поряд з іншим, може бути реалізована і з метою шкідливого впливу шляхом кібератаки (або їх сукупності) для нанесення уразливого кібердару технічним елементам інформаційної інфраструктури противника (суперника) або ментальності його соціального середовища через його переважно споживацьку роль у кіберпросторі. Таким чином, виникає ситуація агресії в кіберпросторі, яка, зокрема, може мати воєнний характер.

З метою виконання завдань у кіберпросторі, що мають воєнний характер, сьогодні дедалі активніше діють відповідні підрозділи збройних сил та спецслужб провідних держав світу. Зважаючи на можливість різноманітних агресивних дій у кіберпросторі, особливо надзвичайно прихованого характеру включно з генерацією спеціальних медіа-продуктів маніпулятивно-підступного змісту, а також створенням різних перешкод для EIP, кіберпростір сьогодні виступає як базова платформа забезпечення реалізації гібридних воєнних дій. Із цієї причини та в умовах, що склалися останніми роками, виникла загальнодержавна практична проблема кібероборони України як одного з необхідних механізмів протидії гібридним воєнним загрозам через агресії в кіберпросторі. Попри очевидну практичну потребу реалізації необхідних заходів, питання кібероборони України є новим розділом знань, що потребує належного теоретичного підґрунтя, чого на сьогодні бракує, отже, і відповідних наукових досліджень.

Аналіз останніх досліджень і публікацій. Питання боротьби в кіберпросторі з усією очевидністю для України постало вже на рубежі XX та XXI століть,

а у формулюванні кібероборони вперше окреслене 2016 р. у Стратегії кібербезпеки України як відбиття воєнної агресії в кіберпросторі [1], утім, без розкриття понять «воєнна агресія в кіберпросторі», а також що таке її «відбиття». Це не давало змоги належним чином розуміти подальші практичні дії щодо формування і застосовування моделі кібероборони та провокувало довільне сприйняття цього завдання. Зокрема в Міністерстві оборони України (МОУ) та Генеральному штабі (ГШ) Збройних Сил України (ЗСУ), яким доручалося, відповідно до компетенції, здійснювати заходи (лише!) з підготовки держави до відбиття воєнної агресії в кіберпросторі (кібероборони).

Наступним кроком розвитку питання кібероборони стало прийняття 2017 р. Закону України «Про основні засади забезпечення кібербезпеки України» [2], яким визначено сутність кібероборони в редакції:

«*Кібероборона* – сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі і спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії».

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.

Цим самим Законом, зокрема, було визначено, що МОУ, ГШ ЗСУ відповідно до компетенції, знову ж таки, здійснюють заходи з підготовки держави до відбиття воєнної агресії в кіберпросторі (кібероборони), що принципово відрізняється за сутністю від наведеного вище визначення кібероборони. Зауважимо, що в подальшому це положення скасоване та замінене іншим з орієнтацією МОУ у сфері кібербезпеки на реалізацію кіберзахисту в інформаційних системах, власником (розпорядником) яких є МОУ, ЗСУ та інші утворені відповідно до законів України військові формування. Згодом ще одним законом зазначене положення знову повернуте в законодавче поле держави, що свідчить про існуючу дискусійність щодо цього питання навіть на такому рівні.

Цим самим Законом щодо кібербезпеки [2] внесені зміни до Закону України «Про оборону України» [3] такого змісту (як одне з положень підготовки держави до оборони): здійснення заходів з кібероборони (активного кіберзахисту) для захисту суверенітету держави та забезпечення її обороноздатності, запобігання збройному конфлікту та відсічі збройній агресії.

Із цього положення випливає: кібероборона – це активний кіберзахист, що є третім варіантом розуміння сутності кібероборони. При цьому додатково виникає риторичне запитання, чи може кібероборона обмежуватися лише кіберзахистом та чи взагалі може бути неактивний (пасивний) кіберзахист, тим більше в умовах відсічі збройній агресії.

Розглядаючи одночасно всі зазначені 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, тобто проблемою, яка перешкоджає гармонізувати практичну діяльність на шляхах побудови (створення) дієвої системи кібероборони держави.

До наведеного слід додати, що наукових публікацій на тему кібероборони України зовсім небагато, серед них можна виділити окремий розділ підручника авторства Ю. Г. Даника, П. П. Воробієнка, В. М. Чернеги [4] та статтю В. А. Савченка [5]. У цих роботах приділено увагу загальним підходам до організації системи кібероборони держави, але лише з позиції законодавства України про кібербезпеку. При цьому законодавчі визначення щодо кібероборони авторами не піддаються сумніву та не критикуються, а використовуються як основа для формування їхньої позиції, тому не з усіма думками авторів цих публікацій можна погодитися.

Усе наведене означає, що питання теоретичних засад кібероборони України сьогодні є дискусійним та потребує подальших зусиль для їх становлення задля кращих практик. Для адекватного формування цих теоретичних засад важливо передусім правильно визначитися, з якої позиції слід розглядати сутність кібероборони України – як складову забезпечення кібербезпеки держави чи складову її оборони. Це важливо з причини, що Конституція України розмежовує сферу національної безпеки і сферу оборони, а сферу оборони України відносить до компетенції ЗСУ. Через це Законом України «Про оборону України» [3] питання кібероборони зосереджуються якраз у сфері оборони, про що вже зазначалося, та домінуючій ролі ЗСУ у фазі відсічі збройній агресії проти України. Тому, на наш погляд, питання кібероборони України, а отже, і її теоретичних засад, слід розглядати з позиції, що це складова оборони держави.

Зазначимо, що тема кібероборони окреслюється у двох чинних законодавчих документах України з питань оборони – у вже згаданому Законі України «Про оборону України» [3], а також у Стратегії воєнної безпеки України [6] та спеціальному Указі Президента України «Про невідкладні заходи з кібероборони держави» [7].

Про кібероборону як активний кіберзахист, про що йдеться в Законі України [3], уже сказано як про одне з невдалих законодавчих положень, тому що із цього неможливо зрозуміти сутність кібероборони як процесу.

У цьому самому Законі (щодо відсічі збройній агресії проти України) є положення:

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

Підкреслимо важливі наслідки, які випливають із цього положення.

1. ЗСУ розпочинають воєнні дії (операції) в кіберпросторі лише (виключно) в разі збройної агресії проти України. Це означає, що за законом ведення воєнних дій (операцій) ЗСУ в кіберпросторі в умовах мирного часу не передбачається.

2. Відсіч збройній (воєнній) агресії проти України у кіберпросторі здійснюється незалежно від того, де вона розпочалась – у кіберпросторі чи поза його межами (тобто не лише відбиття агресії, що здійснена в кіберпросторі проти України, про що йдеться в чинній Стратегії воєнної безпеки України [6] – тут певна колізія із цим Законом).

3. У разі збройної агресії проти України ЗСУ розпочинають воєнні дії (операції) в кіберпросторі не самі, а разом іншими військовими формуваннями, тобто з іншими складовими сил оборони, які передані в підпорядкування Головнокомандувача ЗСУ та діють під його керівництвом та управлінням.

4. Якщо ЗСУ (сили оборони) в разі збройної агресії проти України проводять спеціальні операції (розвідувальні, інформаційно-психологічні тощо) в кіберпросторі, то за цією законодавчою логікою це мають виконувати лише Сили спеціальних операцій ЗСУ, оскільки, відповідно до Законів України [3, 8, 9], лише вони проводять такі операції. При цьому зауважмо, що розвідувальні та інформаційно-психологічні дії в кіберпросторі логічно вважати заходами кібероборони. Про інше щодо кібероборони чи дій військових формувань у кіберпросторі в чинних законах України з питань оборони держави не йдеться. У зв'язку із цим постає питання щодо доцільності створення в системі МОУ окремого структурного утворення – кібервійськ (відповідно до Указів Президента України про Стратегію кібербезпеки України [10] та про невідкладні заходи з кібероборони держави [7]), що суперечить положенням Законів України [3, 8, 9]. Тут також законодавча колізія, яка усувається, на наш погляд, шляхом коректних змін Закону України «Про оборону України» [3] у питані кібероборони, сутність якої маємо з'ясувати, оскільки в законах України з питань оборони вона не розкрита.

Спробуймо з'ясувати деякі питання щодо кібероборони на основі положень, які містяться в Стратегії воєнної безпеки України [6], котра визначає засадничі положення всеохоплюючої оборони України. У цій Стратегії серед пріоритетних завдань реалізації всеохоплюючої оборони України вказані:

- розвиток спроможностей щодо забезпечення ... кібероборони під час підготовки та ведення всеохоплюючої оборони України;
- підвищення рівня боєздатності ЗСУ та інших складових сил оборони з досягненням і підтриманням визначених спроможностей щодо ... відбиття агресії в кіберпросторі (ведення кібероборони).

Як видно, формулювання першого пріоритетного завдання не розкриває сутності кібероборони, але підкреслює дві її фази – підготовки та ведення в загальному процесі всеохоплюючої оборони України, тобто кібероборона є складовою оборони України.

Попри певну колізійність другого формулювання (на відміну від Закону України «Про оборону України» [3] кібероборона акцентується лише на випадок воєнної агресії в кіберпросторі) маємо іншу важливу деталь: цим положенням Стратегії ведення кібероборони прямо покладається на ЗСУ та інші складові сил оборони, оскільки в наведеному положенні йдеться про спільні спроможності за цим напрямом діяльності. Отже, в разі збройної агресії проти України кібероборону здійснюють загалом сили оборони України.

Звернімо також увагу на Указ Президента України «Про невідкладні заходи з кібероборони держави» [7], де наголошується «необхідність ужиття невідкладних заходів щодо створення умов формування в системі МО України кібервійськ для захисту суверенітету держави, забезпечення її обороноздатності, запобігання збройному конфлікту та відсічі збройній агресії у кіберпросторі» з підготовкою законопроєкту про створення та функціонування кібервійськ.

Розгляньмо, що означають такі формулювання.

По-перше, на відміну від попередніх законодавчих актів щодо оборони, тут вперше акцентується питання кібероборони держави, а не просто кібероборони в невизначеному значенні. Але питання кібероборони держави, як і саме це поняття, жодним чином не визначені ані цим документом, ані законодавством України. Тому поняття кібероборони держави (України) потребує окремого обґрунтування.

По-друге, підкреслимо, що в контексті кібероборони держави формування кібервійськ у системі МОУ є невідкладним заходом, тобто не єдиним, а лише окремим серед інших, можливо, більш рядових заходів цього напряму діяльності! Це означає, що створенням кібервійськ кібероборона держави (України) в повному обсязі не забезпечується, оскільки створення таких військ є лише інструментом у складі ЗСУ, який підвищує їхні спроможності для виконання місії в кіберпросторі, визначеної національним законодавством, у разі збройної агресії проти України.

Узагальнюючи викладене, можна стверджувати таке.

1. Законодавство України з питань оборони розглядає кібероборону як елемент відсічі (протидії, спротиву) збройній (воєнній) агресії проти України, незалежно від того, як та де така агресія вперше розпочалася – у кіберпросторі чи поза його межами, або одночасно в усіх можливих сферах діяльності.

2. На відміну від поняття «оборона України», законодавством України щодо оборони поняття кібероборони України не визначене, безпосередньо питання кібероборони держави не ставиться.

3. У сукупності чинних положень законодавства стосовно оборони кібероборона розглядається як одна з функцій ЗСУ (сил оборони) в разі збройної агресії проти України. Іншими словами, йдеться не про кібероборону держави загалом, а лише про її складову у виконанні ЗСУ разом з іншими військовими формуваннями у фазі відбиття (відсічі) збройної агресії (ведення кібероборони). Отже, це кібероборона у вузькому розумінні поняття «оборона», тобто як вид воєнних дій військ (сил).

Довідково. Відповідно до Словника основних термінів та скорочень, які використовуються в НАТО [11]: оборона (defence) – вид дій військ (сил), що застосовуються для відбиття наступу або атак, як правило, переважаючими силами противника, з метою утримання або прикриття визначених територій, рубежів, районів чи об'єктів, економії сил і засобів на деяких напрямах, досягнення переваги над противником на інших, завдання ураження його силам нападу, а також створення умов своїм військам (силам) для контратак та переходу в наступ.

Таким чином, на шляху до розуміння сутності кібероборони України першочергово слід визначитися щодо кібероборони як виду воєнних дій військ (сил), про що якраз і йдеться у законодавстві України щодо оборони.

Метою статті є обґрунтування сутності кібероборони як виду воєнних дій військ (сил) та окреслення особливостей реалізації основних заходів з позиції законодавства України з питань оборони.

Викладення основного матеріалу. Для досягнення поставленої мети в умовах відсутності належної теоретичної бази розглядатимемо питання кібероборони, виходячи виключно з положень законодавства України щодо оборони держави. Ґрунтуючись на такому підході, з'ясуємо передусім характер воєнних (бойових) дій кібервійськ ЗСУ (разом з іншими військовими формуваннями) в кіберпросторі. Щодо інших військових формувань (зі складу сил оборони, підпорядкованих Головнокомандувачу ЗСУ) визначимося далі, а тому зосередимося на рольових особливостях кібервійськ, що мають діяти у складі ЗСУ. Із цього приводу звернімося до статті 1 Закону України «Про Збройні Сили України» [8], відповідно до якої мають діяти ЗСУ, а отже, і кібервійська в їхньому складі, тобто здійснюватися кібероборона як вид воєнних (бойових) дій.

У вказаній статті значиться таке.

1. ЗСУ – це військове формування, на яке відповідно до Конституції України покладаються оборона України, захист її суверенітету, територіальної цілісності і недоторканності.

Ця функція є конституційною, має загальний характер, кібервійська у складі ЗСУ, поряд з іншими складовими, беруть участь у її виконанні. Але наведена редакція не надає змістовності для визначальних ознак поняття кібероборони як виду воєнних (бойових) дій у фазі відбиття (відсічі) збройної агресії проти України.

2. ЗСУ забезпечують стримування збройної агресії проти України та відсіч їй, охорону повітряного простору держави та підводного простору в межах територіального моря України у випадках, визначених законом, беруть участь у заходах, спрямованих на боротьбу з тероризмом.

Цим положенням Закону не акцентуються дії ЗСУ в кіберпросторі. Між тим, можна стверджувати, що у фазі відбиття (відсічі) збройної агресії проти України (коли ЗСУ згідно із Законом [3] виконують функцію кібероборони як виду воєнних (бойових) дій), вимога «стримування збройної агресії проти України» у контексті кібероборони має означати «захист власного кіберпростору», тобто захист середовища власних ЕІР, а вимога «відсіч збройній агресії проти України» має означати «руйнівний вплив на кіберпростір противника», тобто руйнацію середовища його ЕІР. Отже, маємо два принципові складники кібероборони як виду воєнних (бойових) дій. Причому в обох випадках дій ЗСУ відповідні заходи реалізуються всіма доступними способами та засобами збройної боротьби.

3. З'єднання, військові частини і підрозділи ЗСУ відповідно до закону можуть залучатися до здійснення заходів ... захисту критичної інфраструктури, ... проведення військових інформаційно-психологічних операцій...

ЗСУ у сфері захисту критичної інфраструктури забезпечують організацію захисту військових об'єктів критичної інфраструктури ЗСУ від терористичних загроз ..., виконання завдань з протиповітряного прикриття важливих об'єктів держави (критичної інфраструктури)...

Як видно, в цьому положенні Закону:

по-перше, підтверджується положення Закону України «Про оборону України» [3], що в кіберпросторі ЗСУ разом з іншими військовими формуваннями

(силами оборони) можуть проводити військові інформаційно-психологічні операції;

по-друге, очевидно, що лише протиповітряне прикриття критично важливих об'єктів держави, зокрема критичних об'єктів інфраструктури ЗСУ, не рятує їх від артилерійських ударів, руйнівних диверсійних дій тощо, що це потребує інших способів прикриття та певного законодавчого уточнення для реалізації необхідного комплексу дій;

по-третє, законодавчий акцент на захисті військових інфраструктурних об'єктів лише від терористичних загроз, є обмежено-недостатнім, оскільки існують суттєві відмінності між тероризмом і збройною агресією проти держави, що також потребує вдосконалення цього положення Закону шляхом внесення змін, зокрема щодо розширення до кіберзагроз в інтересах здійснення кібероборони.

Зазначимо, що значна кількість критичних об'єктів інфраструктури ЗСУ може містити комп'ютеризовану інформаційну систему (тобто локальний кіберпростір) – складову всієї інформаційної інфраструктури ЗСУ, котра у своєму різноманітті реалізацій утворює загальний кіберпростір для здійснення процесів управління військами (силами) та зброєю в цифровому (автоматизованому) режимі. Іншими словами, це діюча сукупність різноманітних за функціями та призначенням середовищ ЕІР, утворених єдиними (об'єднуючими) мережами комп'ютеризованих об'єктів інформаційної діяльності (ОІД) ЗСУ.

Довідково. Відповідно до [12], об'єкт інформаційної діяльності – інженерно-технічна споруда (приміщення), де здійснюється процес, пов'язаний з інформацією, що підлягає захисту.

Такі ОІД (а не вся інфраструктура!) можуть бути ідентифіковані як критичні об'єкти інформаційної інфраструктури ЗСУ, оскільки порушення їхньої роботи неодмінно призведе до відчутної шкоди всьому критичному об'єкту військової інфраструктури. Тому відповідно до наведеного положення Закону критичні ОІД у ЗСУ мають бути захищені силами та засобами самих ЗСУ.

Слід підкреслити, що в умовах ведення активних воєнних дій критичні ОІД ЗСУ (тобто базові елементи формування кіберпростору) можуть піддаватися ворожим ударам, по-перше, із застосуванням традиційної (конвенційної) зброї, а по-друге, шляхом проведення кібератак як у цифровій формі, так і шляхом застосування енергії в електромагнітному чи звуковому спектрі, що реально підтверджено в процесі російсько-української війни. Отже, такі ОІД повинні мати як захист від руйнівного механічного впливу, так і захист від безпосереднього проникнення до їхніх наявних ЕІР через електротехнічні чи акустичні канали доступу. Тобто мова йде про комплексний кіберзахист критичних об'єктів інформаційної інфраструктури ЗСУ як складний процес протидії негативному впливу на наявні ЕІР, що містяться в таких об'єктах.

Таким чином, у законодавчому контексті щодо оборони України якраз комплексний кіберзахист критичних об'єктів інформаційної інфраструктури, якими є критичні ОІД ЗСУ (носії власних ЕІР), що означає «захист власного кіберпростору», слід розглядати як складову кібероборони та як одну з функцій ЗСУ у фазі відбиття (відсічі) збройної агресії проти України.

Вимога «відсіч збройній агресії проти України» в нашому випадку, як вище зазначено, має означати руйнацію елементів ворожої інформаційної інфраструктури (ОІД як носіїв ЕІР противника) силами і засобами ЗСУ. Руйнівний вплив на кіберпростір противника може бути реалізований із застосуванням різної зброї: як традиційної – механічної (кінетичної) дії, так і інформаційної (кіберзброї) – шляхом кібератак (цифрова форма проникнення чи глушіння в електромагнітному або звуковому спектрі частот засобами радіоелектронної боротьби). Тому відповідно до цієї вимоги законодавства України щодо оборони, механічне руйнування елементів інформаційної інфраструктури (тобто ОІД) противника та руйнівні кібератаки на його ЕІР, що сукупно означає «руйнівний вплив на кіберпростір противника», також слід розглядати як складову кібероборони та як ще одну з функцій ЗСУ у фазі відбиття (відсічі) збройної агресії проти України.

Окреслення зазначених складових кібероборони як важливих функцій ЗСУ у фазі відбиття (відсічі) збройної агресії проти України загалом означає, що збереження обсягу власних ЕІР та нанесення максимальної шкоди ЕІР противника є комплексним завданням і головною умовою досягнення інформаційної переваги над противником у кіберпросторі, яка порівняно з противником забезпечує:

- вищу оперативність і якість інформаційного забезпечення процесів цифрового (автоматизованого) управління військами (силами) та зброєю;
- можливість рефлексивного управління діями цільових аудиторій сторони противника на свою користь (у спосіб інформаційно-психологічного впливу через кіберпростір на визначені цільові аудиторії);
- дії на випередження власних військ (сил) у процесі збройної боротьби в умовах сприятливого ментального стану противника.

Таким чином, розуміючи відповідно до законодавства України з питань оборони кібероборону як одне з комплексних завдань ЗСУ у фазі відбиття (відсічі) збройної агресії проти України, маємо визначитися

стосовно ролі кібервійськ як інструменту ЗСУ у виконанні цього задання, тобто їхньої мети і характеру воєнних (бойових) дій у кіберпросторі.

Зауважимо, що в разі збройної агресії проти України відповідно до Закону [3] ЗСУ розпочинають воєнні дії, в тому числі проведення операцій у кіберпросторі, коротко – кібероперацій. Тому у фазі відбиття (відсічі) збройної агресії проти України кібероперація – основна форма ведення (здійснення) кібероборони ЗСУ, тобто їхніх воєнних дій у кіберпросторі. Менш масштабні дії в кіберпросторі або складові кібероперації слід вважати кіберакціями. При цьому, зважаючи на викладене, основними складовими кібероперації повинні бути комплексний захист кіберпростору ЗСУ та руйнівний вплив на кіберпростір противника.

Очевидно, що завдання проведення кібероперації в повному обсязі (за її основними складовими) покласти на окремий рід військ ЗСУ – кібервійська неможливо через низку причин.

По-перше, у процесі комплексного кіберзахисту власних ОІД (критичних об'єктів військової інформаційної інфраструктури) не видається можливим покладати на кібервійська, зокрема, завдання захисту наявних ЕІР на ОІД через удари засобами традиційної зброї противника. З одного боку, в такі ОІД (як споруди, приміщення чи інші складні інженерно-технічні конструкції) у їх різноманітті ще на етапі створення закладається певний рівень механічної стійкості та живучості. На цей конструкційний рівень ОІД у процесі його експлуатації вже ніщо не впливає. З другого боку, в умовах застосування противником під час бойових дій традиційних засобів ураження принаймні критичні ОІД ЗСУ повинні обов'язково мати необхідне цільове зовнішнє прикриття від ураження кінетичними засобами противника. Таке прикриття (не лише протиповітряне, а й в інші способи) є традиційним заходом у загальній системі оборони критичних інфраструктурних об'єктів держави і не потребує додаткового рішення щодо покладання цього елемента комплексного кіберзахисту на окремий рід військ, зокрема на кібервійська.

По-друге, в реалізації заходів радіоелектронного захисту ОІД (отже, ЕІР) ЗСУ від кібератак, що здійснюються шляхом шкідливого впливу енергії (завад) у радіочастотному чи звуковому спектрі, роль кібервійськ також виглядає сумнівною, оскільки такі захисні спроможності конструктивно закладені у відповідні зразки озброєння та технічні регламенти їхнього застосування. Ці технічні регламенти у своїй практиці застосовують частини і підрозділи ЗСУ, пов'язані з експлуатацією такого озброєння у складі ОІД.

Отже, в ситуації комплексного кіберзахисту (насамперед під час кібероперації) кібервійськам доцільно відвести роль захисту наявних ЕІР критичних ОІД ЗСУ від руйнівного впливу кібератак, що здійснюються противником шляхом скритного проникнення через комунікаційні мережі – це мережевий кіберзахист. При цьому підрозділи (групи, фахівці) кібервійськ, які виконують завдання мережевого кіберзахисту, мають діяти на ОІД, зокрема у військах зв'язку, спостереження, навігації, автоматизованих центрах (пунктах) управління, ситуаційних центрах тощо.

Щодо виконання ЗСУ завдань руйнівного впливу на кіберпростір противника під час ведення кібероборони зазначимо таке.

Очевидно, що на кібервійська неможливо покладати завдання механічного ушкодження ОІД противника (елементів його інформаційної інфраструктури як носіїв ЕІР). Це завдання як складову кібероперації ЗСУ або операції угруповання військ (сил) з елементами кібероперації зможуть виконувати війська (сили), призначені для вогневого ураження противника або здійснення проти нього спеціальних дій. Яскравими прикладами виконання таких завдань є обидва епізоди знищення українськими засобами протиповітряної оборони авіаційних розвідувальних комплексів А-50 у зоні Азовського моря в січні-лютому 2024 р. або нанесення ракетного удару по центру зв'язку Чорноморського флоту РФ у Севастополі в березні того самого року, чи знищення багатьох наземних радіолокаторів противника. Усі ці вогневі (механічні) ураження критично важливих ОІД (джерел ЕІР) призвели до значної шкоди через виключення їх із процесу формування кіберпростору противника та актуального інформаційного забезпечення ворожої військової системи управління. Принагідно зауважимо, що, на наш погляд, наведені приклади бойових епізодів мають чіткі ознаки складових кібероперацій або загалом повноцінних кібероперацій, попри поширені твердження про інші види операцій сил оборони України в цих випадках.

Як уже зазначалося, під час кібероперації також здійснюються руйнівні кібератаки на ворожі ОІД скритним проникненням до ЕІР через комунікаційні мережі, а також глушіння (блокування) таких ЕІР традиційними засобами радіоелектронної боротьби. На наш погляд, такі завдання сьогодні, під час війни з РФ, виконуються різними виконавцями іноді розрізнено, епізодично і некоординовано, попри їхню єдину інформаційну спрямованість. Саме ці складові ураження кіберпростору противника необхідно покласти виключно на кібервійська ЗСУ, оскільки таке рішення відповідатиме як положенням Закону [3] про воєнні (бойові) дії ЗСУ безпосередньо у кіберпросторі, так і підвищеним можливостям координованої реалізації відповідних заходів.

На основі викладеного стверджуємо, що дії кібервійськ ЗСУ мають бути складовою воєнних (бойових) дій ЗСУ в інтересах загальної мети – досягнення

інформаційної переваги над противником у кіберпросторі (середовищі ЕІР), а їхній характер зумовлюється необхідністю виконання таких основних завдань:

- захист наявних ЕІР критичних ОІД у складі ЗСУ від кібератак противника через комунікаційні мережі (здійснення мережевого кіберзахисту);
- здійснення руйнівних кібератак на визначені ворожі ОІД скритним проникненням до їхніх ЕІР через комунікаційні мережі;
- глушіння (блокування) ЕІР визначених ворожих ОІД засобами радіоелектронної боротьби.

Ефективне застосування кібервійськ у складі ЗСУ неможливе без розвідувального забезпечення їхніх дій у кіберпросторі, зокрема в реальному часі. У Законі України «Про оборону» [3] ідеться про необхідність ведення ЗСУ (з іншими військовими формуваннями) розвідувальної діяльності в кіберпросторі. Але відповідно до Закону України «Про розвідку» [9] такої можливості у ЗСУ, отже, в кібервійськ, сьогодні немає. Тому розвідувальне забезпечення дій кібервійськ мають здійснювати розвідувальні органи інших суб'єктів з повноваженнями щодо ведення розвідки в кіберпросторі або слід надати такі повноваження самим кібервійськам. Це спричиняє потребу відповідного законодавчого регулювання.

Виходячи з наведених законодавчих підходів (за умови внесення необхідних змін) та враховуючи щойно окреслену роль кібервійськ у складі ЗСУ, доходимо висновку, що кібероборона як вид воєнних дій військ (сил) ЗСУ – це складний комплексний процес, який здійснюється в умовах відбиття (відсічі) збройної агресії проти України з метою досягнення інформаційної переваги над противником у кіберпросторі в інтересах одержання можливості власних дій на випередження в процесі збройної боротьби та включає (передбачає) такі основні заходи:

- прикриття (захист) власних критичних ОІД (як базових елементів військової інформаційної інфраструктури та носіїв ЕІР) від механічного ураження противником;
- здійснення радіоелектронного захисту елементів у складі військових мереж ОІД (середовищ ЕІР) відповідно до технічних регламентів застосування їхніх штатних режимів роботи;
- нанесення ударів традиційною зброєю по визначених елементах інформаційної інфраструктури противника (його ОІД як носіях ЕІР) для їхнього механічного ураження з руйнівними наслідками для ворожих ЕІР;
- дії кібервійськ у кіберпросторі з виконанням своїх основних завдань;
- здійснення інформаційно-психологічного впливу на цільові аудиторії противника через кіберпростір.

Зауваження. Здійснення інформаційно-психологічного впливу через кіберпростір на цільові аудиторії противника (шляхом модифікації чи підміни коду контенту середовища ЕІР противника) в інтересах рефлексивного управління його діями на свою користь не має здійснюватися кібервійськами. Причина полягає в тому, що для виконання такого завдання в системі МОУ, зокрема у ЗСУ, створені та діють відповідні структурні підрозділи. Це означає, що сьогодні у складі сил оборони вже є необхідні спроможності для таких дій. Тому цей елемент кібероборони як виду воєнних дій мають виконувати саме ці підрозділи в процесі кібероперацій (кіберакцій) з їхньою опцією в кіберпросторі.

Зазначені основні заходи кібероборони реалізуються у формі кібероперацій або кіберакцій (залежно від масштабу та обсягу завдань) у процесі та на підтримку операцій ЗСУ (загалом сил оборони держави).

У реалізації зазначених воєнних заходів полягає загальна (концептуальна) сутність кібероборони як виду воєнних дій ЗСУ у фазі відбиття (відсічі) збройної агресії проти України відповідно до положень національного законодавства з питань оборони.

Тепер зазначимо, що інші військові формування, які діють у складі сил оборони в підпорядкуванні Головнокомандувача ЗСУ в інтересах кібероборони, залучаються до виконання завдань у процесі кібероперацій (кіберакцій) відповідно до їхніх функціональних спроможностей.

Зауважмо також, що крім указаних воєнних заходів доцільно проводити захисні дії невоєнного характеру проти ворожої пропаганди в кіберпросторі (заборона сумнівних мереж, посилення кібергігієни, медіакомпетентності тощо), які можуть вважатися елементами комплексного кіберзахисту і складовою кібероборони держави. За цією ознакою такі невоєнні дії цілком логічно не вважати складовими кібероборони як виду воєнних (бойових) дій, отже, вони повинні реалізовуватися в системі загальнодержавних профілактичних заходів.

Наведена сутність кібероборони як виду воєнних дій загалом відповідає чинним положенням законодавства України з питань оборони. Водночас слід розглянути, чи все в такому розумінні є коректно-достатнім з позиції логіки оборони держави у випадку воєнної (збройної) агресії проти неї. Із цього приводу зауважимо, що відповідно до законодавства України з питань оборони [8] ЗСУ забезпечують відсіч у разі збройної агресії проти України. Це стосується, зокрема, всебічного захисту зусиллями ЗСУ будь-яких об'єктів держави, особливо важливих, від ударів противника в межах усієї її території, в тому числі і комп'ютеризованих критичних ОІД як елементів загальнодержавної інформаційної

інфраструктури та носіїв важливих ЕІР різноманітного спрямування та рівня. Це означає, що й завдання кібероборони (як виду воєнних дій) поширюються на кіберпростір усієї держави. Тому важливо визначитися, у який спосіб ЗСУ в цьому випадку мають забезпечити захист критичних ОІД поза межами інформаційної інфраструктури ЗСУ (сил оборони). На перший погляд, усе може бути аналогічно тому, як це зазначено вище стосовно комплексного кіберзахисту критичних ОІД (носіїв ЕІР) у складі ЗСУ (сил оборони), але є особливості.

Справді, прикриття (захист) критичних ОІД держави від їх механічного ураження противником в умовах воєнної (збройної) агресії є традиційним заходом у загальній системі оборони держави – це завдання в частині відбиття нападів (ударів) противника мають виконувати ЗСУ (сили оборони).

Радіоелектронний захист елементів у складі критичних ОІД держави в умовах воєнної (збройної) агресії забезпечується відповідно до технічних регламентів застосування їхніх штатних режимів роботи – цей вид захисту здійснюється без участі ЗСУ (сил оборони).

Захист наявних ЕІР на критичних ОІД держави від кібератак противника (мережевий кіберзахист) здійснюється в системах заходів утримувачів мереж ОІД самостійно відповідно до загальнодержавних стандартів та регламентів – незалежно від заходів кібероборони як виду воєнних дій ЗСУ (сил оборони) через неможливість охоплення кібервійськами всього різноманіття середовищ ЕІР, утворених мережами ОІД в Україні, тобто також без участі ЗСУ (сил оборони).

Таким чином, кібероборона як вид воєнних дій ЗСУ (сил оборони), поряд з іншим, містить (як складову комплексного кіберзахисту) також заходи прикриття силами та засобами ЗСУ критичних ОІД держави від їх механічного ураження противником в умовах воєнної (збройної) агресії. Зазначені особливості фіналізують можливість представлення загальної структурно-логічної схеми організації здійснення кібероборони як виду воєнних дій у виконанні ЗСУ (сил оборони) відповідно до повноважень з позиції логіки оборони держави у випадку воєнної (збройної) агресії проти неї. Така структурно-логічна схема зображена на *рисунку 1*.

Примітка. Підпорядковані Головнокомандувачу ЗСУ сили й засоби інших складових сил оборони, які в інтересах ведення кібероборони діють у складі угруповань ЗСУ, на схемі не показані.

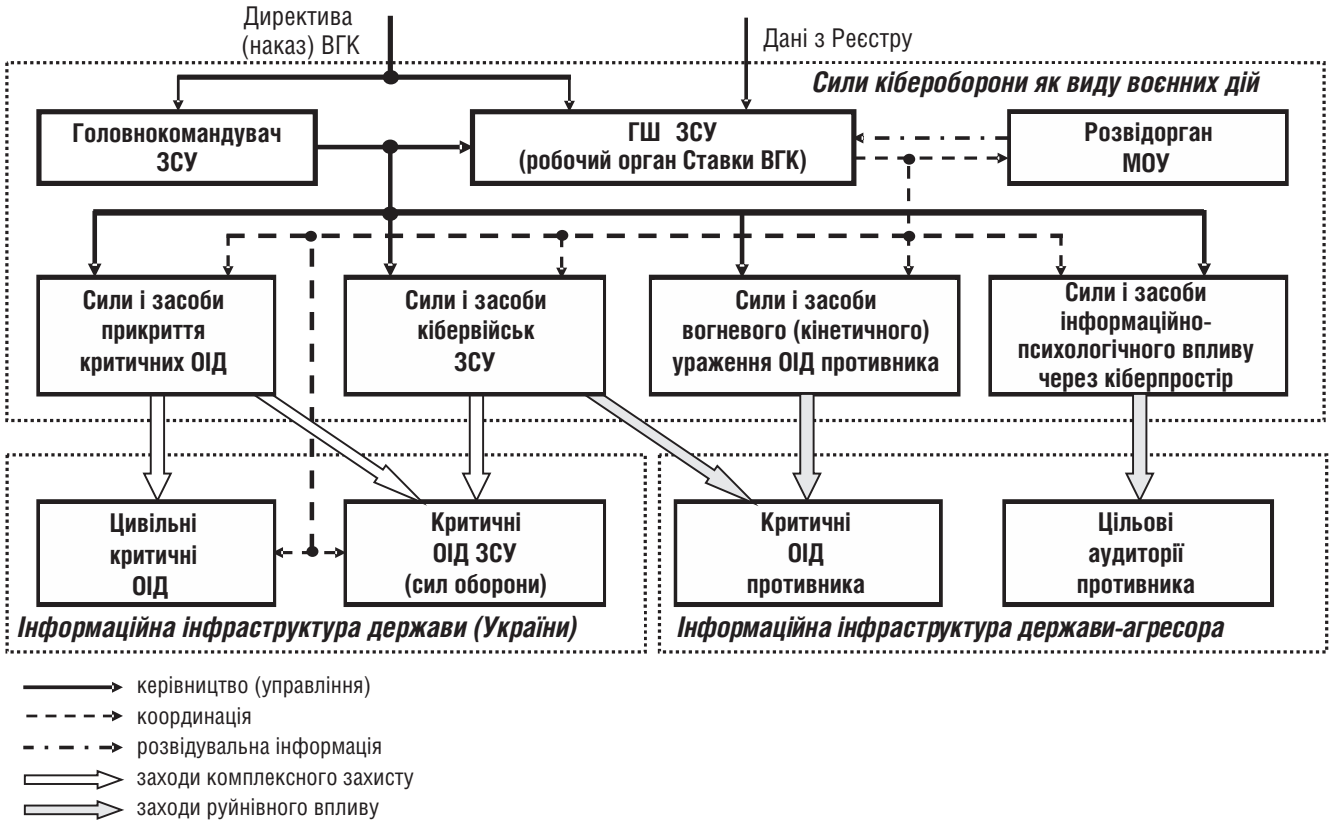

Рис. 1. Структурно-логічна схема організації (здійснення) кібероборони як виду воєнних дій

Коментуючи цю схему, зазначимо таке.

Кібероборона як вид воєнних дій розпочинається з моменту воєнної (збройної) агресії проти України на основі рішення Президента України у формі директиви (наказу) Верховного Головнокомандувача ЗСУ про введення воєнного стану та застосування ЗСУ (сил оборони) і продовжується до його скасування.

Первинними (вхідними) даними для планування та здійснення кібероборони як виду воєнних дій ЗСУ (сил оборони) є перелік критичних ОІД держави, що підлягають захисту (разом із критичними ОІД сил оборони), з національного Реєстру об'єктів критичної інфраструктури за запитом ГШ ЗСУ.

Головнокомандувач ЗСУ здійснює керівництво кібероборoною як видом воєнних (бойових) дій.

ГШ ЗСУ в умовах воєнного часу та відсічі збройній агресії проти України, як робочий орган Ставки Верховного Головнокомандувача, на основі наказів і директив Верховного Головнокомандувача ЗСУ та під безпосереднім керівництвом Головнокомандувача ЗСУ здійснює планування, координацію і контроль з усіх питань щодо кібероборони як виду воєнних дій. Для цього може бути створена оперативна (цільова) група з питань кібероборони.

Збройні Сили України (сили оборони) здійснюють заходи кібероборони як виду воєнних (бойових) дій шляхом застосування визначених сил і засобів у формі кібероперацій (кіберакцій).

Щодо розвідки в інтересах кібероборони. Відповідно до Закону України «Про розвідку» [9], розвідувальну діяльність у сфері оборони здійснює розвідувальний орган МОУ, який за встановленим законодавством порядком надає розвідувальну інформацію визначеним Президентом України суб'єктам сектору безпеки та оборони України, серед яких значаться ЗСУ. У разі відсічі збройній агресії проти України на основі директив, наказів Президента України як Верховного Головнокомандувача ЗСУ, а також рішень Ставки Верховного Головнокомандувача розвідувальна інформація для забезпечення воєнних (бойових) дій ЗСУ (сил оборони), у тому числі ведення кібероборони, цим розвідувальним органом має надаватися.

Водночас розвідувальна інформація від розвідувального органу МОУ в низці випадків, особливо в разі дій у масштабі реального часу в процесі кібероперацій (кіберакцій), може бути недостатньою. Тому, насамперед з метою ведення кібердорозвідки під час воєнних (бойових) дій, у складі кібервійськ ЗСУ необхідно утворити окремий розвідувальний підрозділ, а кібервійська із цієї причини мають стати суб'єктом системи воєнної розвідки та складовою розвідувального співтовариства в Україні, що потребує окремого нормативно-правового регулювання.

Висновок. Поглиблений розгляд питання кібероборони в Україні забезпечив обґрунтування визначення поняття кібероборони як виду воєнних дій ЗСУ (сил оборони) в такій редакції:

«Кібероборона (як вид воєнних дій) – дії військ (сил), що застосовуються в умовах відбиття (відсічі) збройної агресії проти держави для комплексного кіберзахисту середовища ЕІР власних сил оборони, нанесення ураження (шкоди) середовищу ЕІР противника, а також прикриття критичних ОІД держави від ударів засобами традиційної зброї, з метою досягнення інформаційної переваги над противником у кіберпросторі в процесі збройної боротьби».

Таке визначення, одержане вперше, на нашу думку, є системно обґрунтованим та адекватним з позиції логіки оборони держави у випадку воєнної (збройної) агресії проти неї, має конкретизовано орієнтований зміст, у повному обсязі відповідає положенням законодавства України з питань оборони, є відправним пунктом становлення відповідних теоретичних засад та організації в силах оборони держави необхідних заходів кібероборони як виду воєнних дій (за умови, що зазначені суперечності деяких законів України усунуті і введений у дію закон про створення кібервійськ у складі ЗСУ).

Подальші дослідження мають зосередитися на обґрунтуванні сутності кібероборони України як складової оборони держави, оскільки кібероборона як вид воєнних дій у виконанні ЗСУ (сил оборони) не може вважатися єдиним механізмом кібероборони держави та бути реалізованою без використання всього захисного (оборонного) потенціалу держави в кіберпросторі.

Перелік літератури

1. Стратегія кібербезпеки України [Електронний ресурс] : затверджена Указом Президента України № 96/2016 від 15 березня 2016 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/96/2016/ed20160315#Text.

2. Про основні засади забезпечення кібербезпеки України [Електронний ресурс] : Закон України № 2163-VIII від 5 жовтня 2017 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2163-19#Text.

3. Про оборону України [Електронний ресурс] : Закон України № 1932-XII від 6 грудня 1991 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/1932-12#Text.

4. *Даник Ю. Г.* Основи кібербезпеки та кібероборони : підручник / Ю. Г. Даник, П. П. Воробієнко, В. М. Чернега. – Вид. 2-ге. – Одеса : ОНАЗ ім. О. С. Попова, 2019. – 320 с.

5. *Савченко В. А.* Забезпечення стійкості кібероборони держави в умовах збройного конфлікту [Електронний ресурс] / В. А. Савченко // Сучасний захист інформації. –

2023. – № 3 (55). – С. 6–11. – Режим доступу : https://doi.org/10.31673/2409-7292.2023.030001.

6. Стратегія воєнної безпеки України [Електронний ресурс] : затверджена Указом Президента України від 25 березня 2021 р. № 121/2021 // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/121/2021#Text.

7. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про невідкладні заходи з кібероборони держави» [Електронний ресурс] : Указ Президента України № 446/2021 від 26 серпня 2021 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/446/2021#n 5.

8. Про Збройні Сили України [Електронний ресурс] : Закон України № 1934-XII від 6 грудня 1991 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/1934-12#Text.

9. Про розвідку [Електронний ресурс] : Закон України № 912-IX від 17 вересня 2020 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada. gov. ua/laws/show/912-20#Text.

10. Стратегія кібербезпеки України [Електронний ресурс] : затверджена Указом Президента України № 447/2021 від 26 серпня 2021 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/447/2021#n7.

11. Словник основних термінів та скорочень, які використовуються в НАТО / [Міністерство оборони України]. – К. : Леся, 2004. – 568 с.

12. Воєнна політика, безпека та стратегічне планування. Інформаційна безпека держави у воєнній сфері. Терміни та визначення : військовий стандарт : ВСТ01.004.004 – 2014 (01) : чинний від 27.02.2014 / [Міністерство оборони України]. – К. : [б. в.], 2014. – 24 с.