DOI 10.33099/2618-1614-2024-27-4-40-48
УДК 355.4

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

Кібероборона України як складова оборони держави

Питання кібероборони України розглядається з позиції, що це складова оборони держави, а не кібербезпеки. Сьогодні законодавство України з питань оборони розглядає кібероборону обмежено – лише як вид воєнних дій у виконанні Збройних Сил України разом з іншими військовими формуваннями у фазі відбиття збройної агресії, що не вичерпує всіх можливостей захисного (оборонного) потенціалу України в кіберпросторі. При цьому, на відміну від поняття «оборона України», національним законодавством щодо оборони поняття кібероборони України не визначене, безпосередньо питання кібероборони держави не ставиться. Водночас розуміння предмету кібероборони України та його наслідки є концептуально найважливішим та актуальним теоретичним і практичним завданням, яке має бути розв'язане першочергово.
У зв'язку із цим виключно з позиції законодавства України з питань оборони на основі застосування системного підходу і структурно-логічного методу дослідження вперше обґрунтовано сутність кібероборони України як складової оборони держави, окреслено елементи відповідної загальнодержавної системи та взаємозв'язки між ними, намічено основні етапи її реалізації (здійснення).

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

Постановка проблеми. Стрімкий розвиток упродовж останніх десятиліть інформаційних технологій та інформаційних систем на їхній основі спричинив утворення потужної складової загального інформаційного простору – простору електронних інформаційних ресурсів (ЕІР), який одержав назву «кіберпростір». Це створило новий вид взаємодії – взаємодії в сигнально-електронному виді. Поряд з іншим, така взаємодія може бути реалізована і з метою шкідливого впливу шляхом кібератаки (або їх сукупності) для нанесення вразливого кіберудару технічним елементам інформаційної інфраструктури суперника (противника) або ментальності його соціального середовища через «присутність» людини в 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 реалізації такими підрозділами різноманітних агресивних дій у кіберпросторі шляхом генерації шкідливих програмних кодів, спеціальних електронних медіапродуктів маніпулятивно-підступного змісту, а також створення різних завад для ЕІР, кіберпростір сьогодні виступає як базова платформа здійснення гібридних воєнних дій. Для України агресія в кіберпросторі проявилася надзвичайно гостро під час російсько-української війни, коли різноманітні кібератаки на елементи інформаційної інфраструктури держави стали повсякденним явищем. Тому очевидною є практична проблема кібероборони України як один з необхідних механізмів протидії гібридним воєнним загрозам через агресії в кіберпросторі. Сьогодні питання кібероборони України є новим розділом знань, що потребує належного теоретичного опрацювання та відповідних наукових досліджень.

Аналіз останніх досліджень і публікацій. Конституція України розмежовує сферу національної безпеки (отже, і кібербезпеку як її складову) та сферу оборони, а сферу оборони України відносить до компетенції Збройних Сил України (ЗСУ). Із цієї причини Законом України «Про оборону України» [1] питання кібероборони зосереджуються у сфері оборони за домінуючої ролі ЗСУ у фазі відбиття збройної агресії проти України. Тому питання кібероборони України, зокрема її теоретичних засад, може розглядатися з позиції, що це складова оборони держави. Водночас у нечисленних публікаціях, де висвітлюється тема кібероборони України, наприклад [2, 3], автори тяжіють до поняття кібероборони як складової кібербезпеки, не критикуючи при цьому відверто невдалі та взаємно суперечливі законодавчі тлумачення сутності кібероборони, що

викликає різні підходи у висвітленні цієї теми, а також у формулюванні положень підзаконних нормативних документів. Тобто питання кібероборони сьогодні, передусім з наукового погляду, є дискусійним, відповідна теорія перебуває в стані формування. Зважаючи на це, у статті автора [4] вперше започатковано розгляд теми кібероборони виключно *з позиції законодавства України з питань оборони*, що на основі застосування системного підходу та структурно-логічного методу дослідження засвідчило таке:

- 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 розпочалась – у кіберпросторі чи поза його межами, або одночасно в усіх можливих сферах життєдіяльності держави;
- у сукупності чинних положень законодавства стосовно оборони кібероборона розглядається як одна з функцій ЗСУ (сил оборони) в разі збройної агресії проти України, тобто 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) – це кібероборона у вузькому розумінні поняття «оборона», що слід розглядати як вид воєнних дій військ (сил).

Зазначене дало підстави сформулювати визначення:

кібероборона (*як вид воєнних дій*) – дії військ (сил), що застосовуються в умовах відбиття (відсічі) збройної агресії проти держави для комплексного кіберзахисту середовища електронних інформаційних ресурсів власних сил оборони, нанесення ураження (шкоди) середовищу електронних інформаційних ресурсів противника, а також прикриття критичних об'єктів інформаційної діяльності держави від ударів засобами традиційної зброї, з метою досягнення інформаційної переваги над противником у кіберпросторі в процесі збройної боротьби.

Це визначення дає підстави окреслити структурно-логічну схему організації виконання завдання кібероборони зусиллями переважно ЗСУ (сил оборони) безпосередньо *в процесі відбиття збройної агресії проти України*. Тобто сьогодні законодавство України з питань оборони, де йдеться про кібероборону (Закон України «Про оборону України» [1], Стратегія воєнної безпеки України [5], Указ Президента України «Про невідкладні заходи з кібероборони держави» [6]), розглядає кібероборону обмежено – лише як вид воєнних дій. Іншими словами, на відміну від поняття «оборона України», законодавством України щодо оборони поняття *кібероборони України* не визначене, безпосередньо *питання кібероборони держави не ставиться*.

Але з точки зору оборони держави кібероборона як вид воєнних дій у виконанні ЗСУ (сил оборони) не вичерпує всіх можливостей захисного (оборонного) потенціалу держави в кіберпросторі, й до того ж такі дії сил оборони не можуть бути реалізовані без використання можливостей держави, що висуває потребу розуміння загальної сутності кібероборони України. Це розуміння та його наслідки концептуально є найважливішим та актуальним теоретичним і практичним завданням, яке має виконуватись у пріоритетному порядку.

У зв'язку із зазначеним **метою статті** є обґрунтування сутності кібероборони України як складової оборони держави та окреслення основних елементів загальнодержавної системи її реалізації.

Викладення основного матеріалу. Для досягнення поставленої мети першочергово підкреслимо, що як і у випадку інформаційної інфраструктури ЗСУ, яка в різноманітті реалізацій мереж комп'ютеризованих об'єктів інформаційної діяльності (ОІД) утворює кіберпростір (середовище EIP) для інформаційного забезпечення процесів управління військами (силами) та зброєю в цифровому (автоматизованому) режимі [4], так і інформаційна інфраструктура держави аналогічно утворює національний кіберпростір, але в більших масштабах, в інтересах забезпечення інформаційних потреб у різних галузях життєдіяльності.

Питання кібероборони України пов'язане з усім кіберпростором держави, але на відміну від кібероборони як виду воєнних дій має розглядатись у широкому розумінні поняття «оборона», визначеному в Законі України «Про оборону України» [1] в редакції:

оборона України – система політичних, економічних, соціальних, воєнних, наукових, науково-технічних, інформаційних, правових, організаційних, інших заходів держави щодо підготовки до збройного захисту та її захист у разі збройної агресії або збройного конфлікту.

Як видно, оборона України – це комплексний процес, який охоплює сукупність різних необхідних заходів усієї держави та передбачає *дві фази – фазу підготовки* до збройного захисту держави та *фазу захисту* в разі збройної агресії або збройного конфлікту. Відповідно, це стосується і кібероборони України як складової частини загального процесу оборони держави.

При цьому неможливо уявити реалізацію кібероборони як виду воєнних дій без першої фази – попередньої підготовки сил і засобів ЗСУ (сил оборони) до рівня необхідних спроможностей. При цьому кібероборона як вид воєнних дій реалізується впродовж другої фази – шляхом умілого застосування набутих спроможностей за призначенням у процесі кібероперацій (кіберакцій) під час відбиття збройної агресії. Важливо зазначити, що всі необхідні умови та інструменти для реалізації обох фаз надає (забезпечує) держава. Отже, в цьому випадку маємо розглядати поєднаний процес в інтересах оборони України. Тому цілком очевидно, що *кібероборона як вид воєнних дій ЗСУ (сил оборони)* –

складова кібероборони України, що потребує цього доповнення до визначення, наведеного в [4].

Щодо інших складових кібероборони України зазначимо таке.

По-перше, згідно із Законом України «Про оборону України» [1] у разі збройної (воєнної) агресії проти України виключне право на ведення воєнних (бойових) дій у кіберпросторі у формі проведення кібероперацій (кіберакцій) надається лише ЗСУ (силам оборони). Це означає, що всі решта суб'єктів в Україні, котрі мають у своєму підпорядкуванні (розпорядженні) ОІД або їхні мережі (середовища ЕІР), такими повноваженнями не наділені. Тому вони в інтересах кібероборони України здійснюють лише доступні їм заходи *комплексного кіберзахисту*, який, поряд із прикриттям силами та засобами ЗСУ критичних ОІД національної інформаційної інфраструктури від механічних (кінетичних) ударів під час кібероборони як виду воєнних дій, як уже зазначалося в [4], також охоплює:

- радіоелектронний захист технічних елементів у складі мереж ОІД (середовищ ЕІР, що утворюють національний кіберпростір);
- захист наявних ЕІР від кібератак противника шляхом його скритного проникнення через комунікаційні мережі (мережевий кіберзахист);
- захист від негативного інформаційно-психологічного впливу, ворожої пропаганди на різні соціальні групи України через широкодоступні кіберпросторові платформи на основі Інтернет.

Пояснюючи ці елементи комплексного кіберзахисту, зазначаємо таке.

Радіоелектронний захист, незалежно від форми власності середовищ ЕІР, в умовах воєнної (збройної) агресії здійснюється відповідно до технічних регламентів застосування режимів роботи технічних елементів у складі мереж ОІД, тобто впроваджених заздалегідь на етапі їх створення, передбачених для умов експлуатації, – забезпечується діями штатного персоналу на таких засобах.

Захист наявних ЕІР на критичних ОІД держави від кібератак противника (мережевий кіберзахист) здійснюється шляхом обов'язкового впровадження стандартизованих для всієї держави інструментів мережевого кіберзахисту в межах запровадження організаційно-технічної моделі кіберзахисту відповідно до постанови Кабінету Міністрів України № 1426 від 29 грудня 2021 р. [7] – забезпечується кожною юридичною особою – утримувачем мережі (мереж) ОІД самостійно.

Захист від негативного інформаційно-психологічного впливу, ворожої пропаганди на різні соціальні групи України, включно з військовою аудиторією, реалізуються в системі загальнодержавних профілактичних заходів (заборона деяких мереж, посилення кібергігієни, медіакомпетентності тощо).

Наведені елементи комплексного кіберзахисту є захисними інструментами неагресивного (невоєнного) характеру, але вони мають принципове значення для будь-якого ОІД у державі на випадок збройної (воєнної) агресії проти України. Як правило, ці заходи плануються та запроваджуються у фазі підготовки кібероборони України і можуть бути застосовані ще в мирний час та продовжуються (посилюються) у фазі захисту держави в разі збройної агресії проти неї.

Отже, *невоєнні інструменти комплексного кіберзахисту*, насамперед критичних ОІД – носіїв ЕІР (критичних об'єктів інформаційної інфраструктури держави) незалежно від їхньої форми власності, поряд з інструментом кібероборони як виду воєнних дій, у своїй сукупності є *іншою складовою кібероборони України*. Це означає, що як у фазі підготовки кібероборони, так і у фазі ведення кібероборони в частині комплексного кіберзахисту залучаються всі суб'єкти – утримувачі критичних ОІД (носіїв ЕІР) держави, тобто відповідні структурні одиниці критичних об'єктів інформаційної інфраструктури сил оборони, всіх органів державної влади, органів місцевого самоврядування, а також визначені юридичні і фізичні особи, віднесені до таких, що провадять важливу для України діяльність, пов'язану з ЕІР та їхнім захистом.

По-друге, якщо уявити, що в державі відсутнє середовище ЕІР (національний кіберпростір), тоді буде відсутня й необхідність використовувати ЕІР за призначенням, а також їх усебічно захищати (ЕІР немає!), отже, відпадає саме питання кібероборони. Але сьогодні ЕІР є стратегічним ресурсом, без якого вже неможливо уявити життєдіяльність будь-якої держави, як і України. Чим більший потенціал ЕІР держави, тим ефективніше реалізуються процеси управління в багатьох сферах, у тому числі у сфері оборони. Лише створення чи вдосконалення різноманітних комп'ютеризованих інформаційних систем і за їхньою допомогою одержання необхідних інформаційних продуктів може забезпечити необхідний та достатній обсяг ЕІР, зокрема в інтересах підвищення інформаційних можливостей сил оборони України. Це дає змогу реалізувати надійне інформаційне забезпечення управління військами та зброєю в цифровому (автоматизованому) режимі в єдиному інформаційному просторі (кіберпросторі воєнної сфери), зокрема за мережоцентричним принципом ведення воєнних (бойових) дій, а також здійснювати різноманітний електронно-інформаційний вплив на противника для реалізації управління його діями на свою користь. Зазначене означає першочергову потребу наявності розвиненого кіберпростору України (національного середовища ЕІР), причому з необхідністю досягнення (забезпечення) можливостей у формуванні та використанні ЕІР на рівні, достатньому для успішного виконання завдань оборони держави. Саме

тому таке середовище ЕІР має створюватися та постійно розвиватися, зокрема в цілях оборони України. При цьому національне середовище ЕІР є водночас об'єктом як забезпечення власних конструктивних дій через кіберпростір, так і об'єктом захисту від негативного впливу. Отже, за фактом, національне середовище ЕІР, поряд з іншим, являє собою інформаційну платформу реалізації через кіберпростір заходів кібероборони держави. Із цієї причини *формування й подальше розширення національного кіберпростору для збільшення обсягу ЕІР у ньому є невід'ємною складовою кібероборони України*, при цьому є також найбільшим завданням у фазі підготовки кібероборони держави, про що в такому контексті, на жаль, зовсім не йдеться у відомих публікаціях.

Зважаючи на окреслені особливості, ґрунтуючись на положеннях національного законодавства з питань оборони, підходимо до розуміння узагальненої сутності кібероборони України в такій редакції:

кібероборона України – це складова оборони держави як сукупність загальнодержавних заходів, спрямованих на розвиток (розширення) національного кіберпростору, підготовку комплексного кіберзахисту критичних ОІД національної інформаційної інфраструктури та набуття спроможностей ЗСУ (сил оборони) для кібероборони як виду воєнних (бойових) дій, а також використання досягнутих сукупних спроможностей в інтересах захисту України в разі здійснення проти неї збройної (воєнної) агресії.

За цими базовими ознаками кібероборона України як невід'ємна складова оборони держави є фактично справою всього українського народу, що потребує єдиної політики організації та координації на загальнодержавному рівні. Отже, має діяти відповідна система. Допускаючи, як уже зазначено тут, а також у [4], що положення законодавства України з питань оборони, які потребують зміни в інтересах кібероборони, встановленим порядком доповнені, то йтиметься про *перспективну систему кібероборони держави*.

Окреслити обриси цієї системи означає вказати її суб'єктів, сформулювати їхні рольові завдання та означити взаємозв'язки між ними. Кібероборона України, як зазначено, є загальнодержавною справою, тому система, яка її впроваджує в практику, має поширюватися на широке коло інституцій, які, відповідно, стають суб'єктами системи кібероборони держави.

У роботі [4] кібероборона була розглянута як вид воєнних дій, що є складовою кібероборони України, на підставі чого визначені її основні суб'єкти у фазі відсічі збройній агресії проти України: Головнокомандувач ЗСУ, підпорядковані йому Генеральний штаб ЗСУ, загалом Збройні Сили України (сили оборони), а також розвідувальний орган Міністерства оборони України; показані їхня рольова місія та взаємозалежність у процесі спільних дій. Тому вони є серед основних суб'єктів системи кібероборони України, а їхні місії у фазі підготовки кібероборони України будуть розкриті нижче. Стосовно інших задіяних у цій загальнодержавній системі основних суб'єктів зазначаємо таке.

Верховна Рада України здійснює законодавче регулювання питань кібероборони України.

Президент України здійснює загальне керівництво кібероборoною держави з організацією координації шляхом видання указів і розпоряджень, а як *Верховний Головнокомандувач ЗСУ* – наказів та директив з питань оборони. Основою для керівництва кібероборoною держави є затверджений Президентом України План кібероборони України як складова Плану оборони України.

Рада національної безпеки і оборони України (РНБОУ) здійснює координацію діяльності щодо кіберборони держави відповідно до закону, указів та розпоряджень Президента України. Слід зазначити, що законодавством України не розкривається сутність цього процесу, тому на підставі положень низки нормативно-правових актів це буде пояснено згодом.

Міністерство оборони України (МОУ) – відповідно до Закону України «Про національну безпеку України» [8] до його повноважень належить, поряд з іншим, здійснення в установленому порядку координації діяльності державних органів та органів місцевого самоврядування щодо *підготовки держави до кібероборони* як однієї зі складових оборони держави. При цьому, згідно з Положенням про МОУ [9], воно «взаємодіє з іншими державними органами, допоміжними органами і службами, утвореними Президентом України, та тимчасовими консультативними, дорадчими та іншими допоміжними органами, утвореними Кабінетом Міністрів України, органами місцевого самоврядування, об'єднаннями громадян, громадськими спілками, профспілками та організаціями роботодавців, відповідними органами іноземних держав і міжнародних організацій, а також підприємствами, установами і організаціями». Отже, на перший погляд, виникає ефект дублювання з РНБОУ, що небажано.

У зв'язку із цим звернімося за уточненням до пункту 8 цього Положення, де визначено: «...накази Міноборони, видані в межах повноважень, передбачених законом, є обов'язковими для виконання центральними органами виконавчої влади, їхніми територіальними органами, місцевими держадміністраціями, органами влади Автономної Республіки Крим, органами місцевого самоврядування, підприємствами, установами і організаціями незалежно від форми власності і громадянами». Тобто МОУ має повноваження координувати та взаємодіяти лише в межах переліку цих суб'єктів, причому виключно з питань підготовки оборони держави, отже, поряд з іншим, і з *підготовки*

кібероборони. Це обмежений рівень повноважень, оскільки до цього переліку не входять окремі суб'єкти сектору безпеки та оборони України, які підпорядковані Президенту України та мають залучатися до процесів кібероборони відповідно до законодавства.

Зважаючи на вказане, повертаючись до координаційної ролі РНБОУ, логічно вважати, що на основі її рішень, затверджених указом Президента України, в питаннях підготовки кібероборони вона безпосередньо координує як МОУ, так і державні органи, підпорядковані Президенту України, у тому числі шляхом надання доручень Голови РНБОУ її членам для забезпечення взаємодії та гармонійної інтеграції зусиль щодо кібероборони, та встановленим порядком здійснює контроль виконання обраних заходів.

Крім цього додамо: потреба проведення загальнодержавних профілактичних заходів, які протидіють негативному інформаційно-психологічному впливу, ворожій пропаганді через кіберпростір на різні соціальні групи України та є складовими комплексного кіберзахисту в процесі кібероборони України, зумовлює необхідність як у першій фазі (підготовки кібероборони), так і у фазі другій (ведення кібероборони) реалізації єдиної державної політики та належної координації за цим напрямом діяльності. Загальнодержавна значущість проведення в життя такої політики вимагає координації зусиль на найвищому рівні. Із цієї причини цю координацію в обох фазах кібероборони також має здійснювати РНБОУ відповідно до її повноважень.

У зв'язку із зазначеним МОУ, за координаційної ролі з боку РНБОУ, маючи повноваження, визначені законодавством, шляхом відповідних наказів міністерства та безпосередньої взаємодії координує діяльність державних органів (крім підпорядкованих Президентові України) та органів місцевого самоврядування щодо підготовки держави до кібероборони. У цій діяльності основні зусилля МОУ мають зосереджуватися на:

- формуванні та розвитку національного кіберпростору України шляхом удосконалення інформаційної інфраструктури держави в інтересах формування дружнього середовища ЕІР для потреб оборони;
- створенні умов забезпечення комплексного кіберзахисту середовища ЕІР критичних ОІД інформаційної інфраструктури України;
- упровадженні та реалізації в державі заходів захисту соціальної свідомості суспільства, насамперед особового складу сил оборони, від негативного інформаційно-психологічного впливу в кіберпросторі зі змістом, спрямованим на підрив суверенітету, територіальної цілісності й недоторканності України.

Поза цим, відповідно до Закону України «Про національну безпеку України» [8], у підпорядкуванні МОУ перебувають ЗСУ, якими Міністр оборони України здійснює військово-політичне та адміністративне керівництво (безпосередньо або через своїх заступників та Головнокомандувача ЗСУ). Тому МОУ, забезпечуючи всебічно життєдіяльність ЗСУ згідно з потребами, визначеними Генеральним штабом ЗСУ [10], шляхом видання наказів і директив та безпосередньо також координує і спрямовує діяльність ЗСУ, інших складових сил оборони щодо підготовки кібероборони за напрямами:

- формування та розвитку кіберпростору воєнної сфери шляхом удосконалення цифрової інформаційної інфраструктури сил оборони як основи інтегрованого інформаційного середовища ЕІР для задоволення інформаційних потреб військових споживачів та забезпечення оперативної електронної комунікації;
- створення умов забезпечення комплексного кіберзахисту середовища ЕІР критичних ОІД інформаційної інфраструктури сил оборони;
- забезпечення формування і підготовки спроможностей сил та засобів ЗСУ, інших складових сил оборони для кібероборони як виду воєнних дій у разі відбиття збройної (воєнної) агресії проти України.

Маючи повноваження з питань оборони держави, МОУ з метою організації кібероборони держави та запровадження механізму координації у фазі підготовки кібероборони розробляє структуру і порядок розроблення Плану кібероборони України (як частини Плану оборони України) та організовує розроблення його складових. У Плані кібероборони України мають бути складові, які відображають рольові функції всіх суб'єктів системи кібероборони держави, за типом тих їхніх функцій, які вже були означені вище.

Після затвердження Президентом України Плану кібероборони України як частини Плану оборони України МОУ здійснює координацію передбачених заходів підготовки кібероборони.

Генеральний штаб ЗСУ в питаннях підготовки кібероборони діє під координацією МОУ. Для цього Генеральний штаб ЗСУ:

- розробляє пропозиції до Плану кібероборони України (як частини Плану оборони України);
- визначає вимоги щодо ЕІР ЗСУ, інших складових сил оборони, а також відомчих ЕІР для потреб оборони держави, а спільно з *Державною службою спеціального зв'язку та захисту інформації України* (ДССЗЗІУ) – щодо забезпечення комплексного кіберзахисту середовища ЕІР критичних ОІД інформаційної інфраструктури України, у тому числі інформаційної інфраструктури сил оборони;
- здійснює планування кібероборони з питань удосконалення інформаційної інфраструктури ЗСУ та інших складових сил оборони як основи інтегрованого інформаційного середовища ЕІР (кіберпростору воєнної сфери) для задоволення інформаційних потреб

військових споживачів ЕІР, здійснення оперативної електронної комунікації;

• здійснює планування заходів забезпечення комплексного кіберзахисту середовища ЕІР критичних ОІД інформаційної інфраструктури сил оборони;

• організовує та здійснює заходи щодо формування і підготовки спроможностей сил та засобів ЗСУ та інших складових сил оборони для кібероборони як виду воєнних дій у разі відбиття збройної (воєнної) агресії проти України;

• організовує взаємодію та здійснює контроль складових сил оборони щодо набуття ними необхідних об'єднаних спроможностей з питань кібероборони.

Збройні Сили України (сили оборони) з питань підготовки кібероборони координуються МОУ (через Генеральний штаб ЗСУ) та здійснюють заходи щодо набуття ними необхідних об'єднаних спроможностей з питань кібероборони як виду воєнних (бойових) дій.

Слід зауважити, що в мирний час ЗСУ (сили оборони) можуть використовувати набуті в процесі підготовки кібероборони спроможності, зокрема кібервійськ (мають бути у складі ЗСУ [4]), в інтересах моніторингу кіберпростору (розвідувальної діяльності) та кіберзахисту власних ЕІР.

Головні рольові функції Генерального штабу ЗСУ, а також ЗСУ з питань ведення кібероборони в умовах воєнного часу та відбиття збройної агресії проти України окреслені в роботі [4] під час розгляду кібероборони як виду воєнних дій.

Крім зазначених, суб'єктами системи кібероборони України є також *інші державні органи, органи місцевого самоврядування, підприємства, установи та організації, віднесені до критичних об'єктів інфраструктури, а також суб'єкти господарювання, громадяни України та об'єднання громадян, особи, які провадять діяльність та/або надають послуги, пов'язані з національними ЕІР, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями та кіберзахистом* незалежно від їхньої форми власності, які діють в інтересах кібероборони.

Основні завдання інших суб'єктів системи кібероборони України з питань підготовки кібероборони полягають у вдосконаленні їхнього власного цифрового комунікативного середовища (середовища ЕІР – власного кіберпростору), в тому числі в інтересах оборони держави, та проведенні заходів щодо забезпечення його комплексного кіберзахисту. Координація їхньої діяльності та взаємодія у фазі підготовки кібероборони проводиться відповідно до наказів МОУ, за винятком суб'єктів, підпорядкованих Президентові України, які мають залучатися до процесів кібероборони держави (такі суб'єкти координуються на основі рішень РНБОУ або через доручення Голови РНБОУ її членам).

Слід окремо зауважити, що серед суб'єктів системи кібероборони України в питанні підготовки кібероборони держави особливі місце та роль належать ДССЗЗІУ, котра згідно із Законом [11] здійснює формування та реалізацію державної політики, зокрема щодо захисту державних ЕІР та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту критичних об'єктів інформаційної інфраструктури тощо. Із цією метою ДССЗЗІУ забезпечує впровадження організаційно-технічної моделі кіберзахисту (у наведеному вище розумінні мережевого кіберзахисту). Положення про таку модель затверджене урядовою постановою [7], де викладені загальні рекомендації щодо організації кіберзахисту об'єктів інформаційної діяльності на національному, галузевому (регіональному, місцевому) та об'єктовому (підприємства, установи, організації) рівнях. При цьому відповідно до концепції моделі заходи кіберзахисту на кожному рівні покладаються на спеціалізовані органи (підрозділи, команди) – сили кіберзахисту. У цих заходах сили кіберзахисту мають застосовувати засоби кіберзахисту, перелічені в Положенні в сенсі їхнього функціонального призначення, зокрема:

• системи виявлення вразливостей та реагування на кіберінциденти і кібератаки;

• інформаційні технології, технічні і програмні засоби (пристрої, обладнання, комплекси), які використовуються в інтересах забезпечення кіберзахисту національних ЕІР, комунікаційних і технологічних систем, а також критичних об'єктів інформаційної інфраструктури.

Як рекомендація загального характеру цей перелік засобів кіберзахисту не викликає сумніву. Але реалізація цього положення без додаткових пояснень неодмінно призводить до різноманітних підходів до практики кіберзахисту ЕІР конкретних ОІД («на місцях»), причому на кожному із зазначених рівнів, та, відповідно, нерівномірності в ефективності кіберзахисту ЕІР різних ОІД. Такий наслідок є небажаним, зокрема з погляду кібероборони України. Із цієї причини в інтересах рівної міцності кібероборони доцільно стандартизувати набори засобів кіберзахисту для кожного рівня організаційно-технічної моделі кіберзахисту.

Ініціатива щодо розроблення таких стандартів і методичних рекомендацій щодо їх впровадження, на наш погляд, має належати ДССЗЗІУ, що стало б чи не найголовнішим елементом реалізації всієї організаційно-технічної моделі кіберзахисту та спростило б завдання кіберзахисту ЕІР усіх суб'єктів системи кібероборони України.

Координацію щодо впровадження цих стандартів в інтересах кібероборони України відповідно до компетенції мають здійснювати РНБОУ та МОУ.

В умовах воєнного часу та відбиття збройної агресії проти України *суб'єкти системи кібероборони України* в процесі реалізації заходів кібероборони як виду воєнних (бойових) дій координуються Генеральним штабом ЗСУ – робочим органом Ставки Верховного Головнокомандувача, згідно з наказами і директивами Верховного Головнокомандувача ЗСУ з питань оборони та діють відповідно до компетенції та набутих спроможностей.

Кабінет Міністрів України в обох фазах оборони держави забезпечує здійснення державної політики щодо кібероборони України у спосіб організації та забезпечення необхідними силами, засобами і ресурсами заходи кібероборони шляхом:

- формування, розміщення, фінансування та виконання відповідного державного оборонного замовлення на поставку (закупівлю) продукції, виконання робіт, надання послуг для потреб ЗСУ та інших складових сил оборони, а також програм (планів) з питань кібероборони інших державних суб'єктів системи кібероборони України в межах коштів, виділених на фінансування цих заходів у затвердженому Верховною Радою України Державному бюджеті України;
- створення сприятливих умов для впровадження заходів комплексного кіберзахисту власного середовища ЕІР суб'єктами системи кібероборони України недержавної форми власності, які провадять діяльність та/або надають послуги, пов'язані з національними ЕІР, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями та кіберзахистом.

Наведений вище перелік суб'єктів системи кібероборони України, з'ясування їхнього функціонального призначення у фазах підготовки кібероборони та ведення кібероборони, виходячи з положень чинного законодавства держави з питань оборони, уточнення взаємозв'язків між ними та особливостей координації в цій системі дає змогу зобразити перспективний варіант її структурно-логічної схеми, як представлено на *рисунку 1*, що відображає сутність концептуальної архітектури системи кібероборони України (її перспективний структурний обрис).

З урахуванням викладеного стає можливим пропонувати перелік основних етапів створення перспективної системи кібероборони України відповідно до положень національного законодавства з питань оборони.

Етап 1. *Сформувати належну правову основу організації кібероборони України шляхом внесення необхідних змін до національного законодавства з питань оборони*, виходячи при цьому з понять кібероборони як у широкому, так і у вузькому розумінні процесу оборони, а також того, що кібероборона передбачає наявність двох фаз – підготовка кібероборони та ведення кібероборони, до яких залучається широкий перелік суб'єктів держави відповідно до їхньої компетенції, котрі при цьому утворюють систему кібероборони України.

Деталізація шляхів організації кібероборони держави може бути зосереджена в окремій Стратегії кібероборони України, але після попереднього внесення необхідних змін щодо кібероборони до Законів України «Про оборону України», «Про розвідку», «Про Збройні Сили України» та до Стратегії національної безпеки України і Стратегії воєнної безпеки України.

Етап 2. *Створити у ЗСУ кібервійська* з повноваженнями протиборства в кіберпросторі шляхом розвідки в кіберпросторі, кіберзахисту ЕІР на ОІД ЗСУ (сил оборони), нанесення поразки агресору в кіберпросторі або через кіберпростір у разі збройної (воєнної) агресії проти України, забезпечивши створені війська належними фінансовими, кадровими і технічними ресурсами.

Етап 3. *Створити в Україні єдину мережу галузевих, регіональних, місцевих ситуаційних центрів з питань кіберзахисту*, здатну забезпечити оперативне реагування на кіберзагрози на рівні, що відповідає потребам кібероборони держави.

Етап 4. *Уточнити План кібероборони України* як керівництво щодо підготовки кібероборони держави та її здійснення в разі воєнної (збройної) агресії проти України, зокрема з такими складовими:

- розвиток національного середовища ЕІР (розширення національного кіберпростору України), зокрема в інтересах активного функціонування єдиного цифрового інформаційного середовища сил оборони;
- когнітивна безпека України в кіберпросторі (безпека соціальної свідомості суспільства під час використання кіберпростору);
- комплексний кіберзахист у національному кіберпросторі України (захист критичних ОІД держави від традиційної зброї, впровадження організаційно-технічної моделі кіберзахисту на основі стандартизованих процедур);
- набуття спроможностей і кібероперації (кібердії) ЗСУ та інших складових сил оборони, у тому числі дії кібервійськ у кіберпросторі (мережевий кіберзахист ЕІР, мережеві акції, радіоелектронна боротьба);
- ресурсне забезпечення системи кібероборони України (кадрове, матеріально-технічне, фінансове);
- механізми керівництва, координації та контролю в системі кібероборони України.

Етап 5. *Забезпечити реалізацію заходів уточненого Плану кібероборони України* в перспективній системі кібероборони України.

Цими етапами означено, на наш погляд, найбільш принципові особливості в системному розумінні шля-

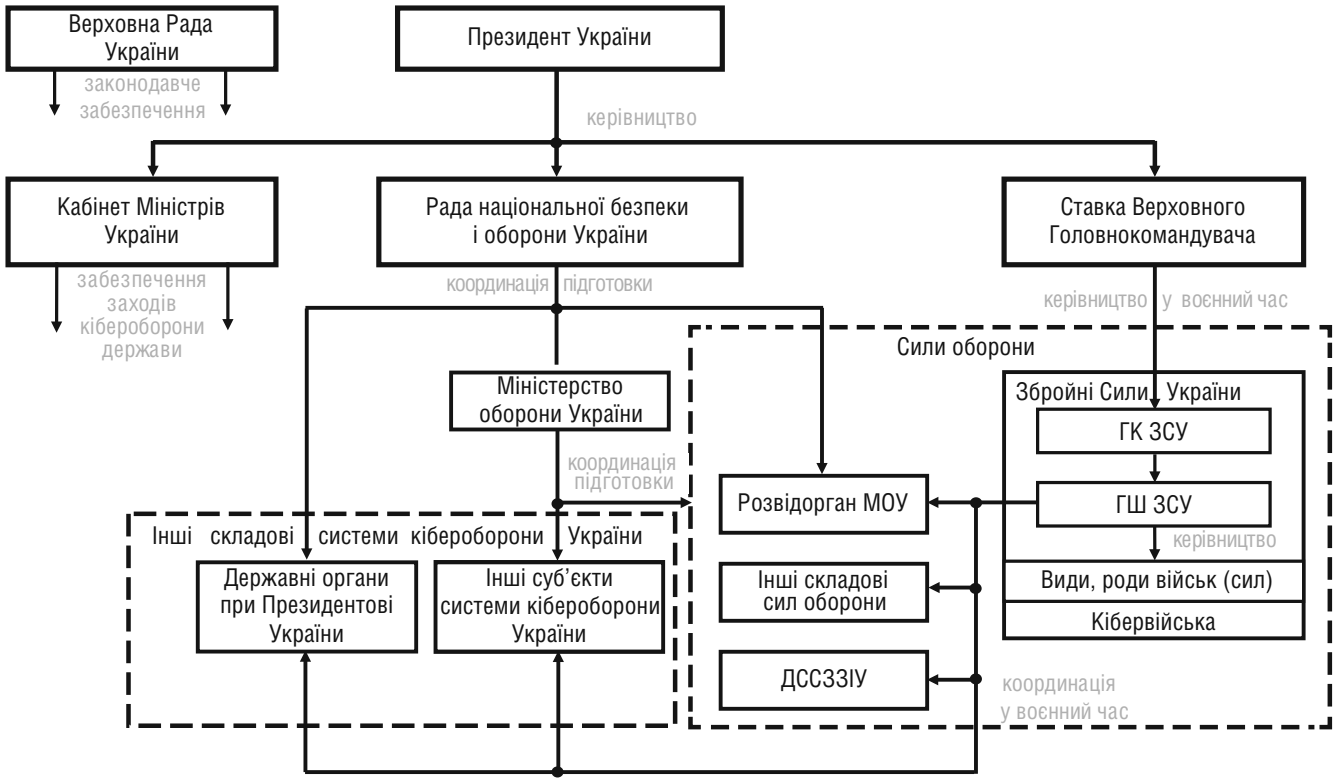

Рис. 1. Структурно-функціональна схема перспективної системи кібероборони України

хів практичної реалізації наміченого обрису перспективної системи кібероборони України, що слід вважати головними орієнтирами розвитку цієї системи.

Висновки

1. Оскільки Конституція України розмежовує сферу національної безпеки (включно зі складовою кібербезпеки) і сферу оборони, а сферу оборони України відносить до компетенції ЗСУ, то питання кібероборони України може розглядатися з позиції, що це складова оборони держави, а не кібербезпеки. Водночас сьогодні законодавство України з питань оборони розглядає кібероборону обмежено – лише як вид воєнних дій у виконанні ЗСУ разом з іншими військовими формуваннями у фазі відбиття збройної агресії. При цьому, на відміну від поняття «оборона України», законодавством України щодо оборони поняття кібероборони України не визначене, безпосередньо питання кібероборони держави не ставиться.

2. З погляду оборони держави кібероборона як вид воєнних дій у виконанні ЗСУ (сил оборони) не вичерпує всіх можливостей захисного (оборонного) потенціалу України в кіберпросторі і, до того ж, такі дії сил оборони не можуть бути реалізовані без використання можливостей держави, що зумовлює потребу розуміння загальної сутності кібероборони України. Це розуміння та його наслідки концептуально є найважливішим та актуальним теоретичним і практичним завданням, яке має бути розв'язане в пріоритетному порядку. У зв'язку із цим, виключно з позиції законодавства України з питань оборони на основі застосування системного підходу і структурно-логічного методу дослідження вперше обгрунтовано сутність кібероборони України як складової оборони держави, окреслено складові відповідної загальнодержавної системи та взаємозв'язки між ними, намічено основні етапи її реалізації.

Подальші дослідження можуть бути зосереджені на формуванні та розвитку теоретичних засад кібероборони України як складової оборони держави, виходячи з її сутності та особливостей реалізації, а також на обґрунтуванні пропозицій щодо вдосконалення національного законодавства з питань оборони в частині положень про кібероборону держави.

Перелік літератури

1. 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.

2. *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.

3. *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.

4. *Сніцаренко П. М.* Про сутність кібероборони як виду воєнних дій [Електронний ресурс] / П. М.Сніцаренко // Наука і оборона. – 2024. – № 3. – С. 45–54. – Режим доступу : https://doi.org/10.33099/2618-1614-2024-26-3-45-54.

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

6. 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#n5.

7. Положення про організаційно-технічну модель кіберзахисту [Електронний ресурс] : затверджене постановою Кабінету Міністрів України № 1426 від 29 грудня 2021 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/1426-2021-п#Text.

8. Про національну безпеку України [Електронний ресурс] : Закон України № 2469-VIII від 21 червня 2018 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2469-19#Text.

9. Положення про Міністерство оборони України [Електронний ресурс] : затверджене постановою Кабінету Міністрів України № 671 від 26 листопада 2014 р. (у редакції постанови Кабінету Міністрів України № 730 від 19 жовтня 2016 р.) // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/671-2014-п#Text.

10. Положення про Генеральний штаб Збройних Сил України [Електронний ресурс] : затверджене Указом Президента України № 23/2019 від 30 січня 2019 р. // Верховна Рада України. Законодавство України. – Режим доступу :