Живило Євген Олександрович,
аспірант кафедри інформаційних технологій і систем управління,
ХарРІ НАДУ, м. Харків
ORCID 0000-0003-4077-7853

УДК 351.865 **doi:10.342/db.19.01.03**

СУЧАСНІ ПІДХОДИ ДО ВИЗНАЧЕННЯ СКЛАДОВИХ КІБЕРОБОРОНИ ДЕРЖАВИ

Розглянуто підходи держав-членів НАТО щодо реагування на загрози в кіберпросторі. Визначено складові системи кібероборони, розкрито й деталізовано її інституалізаційну складову. Досліджено питання активного впливу в кіберпросторі в рамках кібероборони держави. Урахування деталізованої інституалізаційної складової кібероборони в ході створення системи кібероборони дозволить підвищити ефективність її функціонування в інтересах досягнення цілей, які визначені перед суб'єктами сектору безпеки і оборони, які забезпечують кібербезпеку.

Ключові слова: кіберпростір; кіберзагрози; кібероборона держави; спроможності; телекомунікаційна інфраструктура; кіберзахист критичної інформаційної інфраструктури.

Постановка проблеми в загальному вигляді. Держави світу в інтересах реалізації своїх національних інтересів активно опановують кіберпростір. Україна не є винятком. Стрімкий розвиток телекомунікаційної інфраструктури, зростання потреби в якісних електронних послугах створили передумови використання кіберпростору як окремої сфери ведення бойових дій [1]. З огляду на це оборона України повинна мати системний характер і поряд із забезпеченням захисту суверенітету, територіальної цілісності та недоторканості своїх кордонів держави бути спрямованою на забезпечення захисту інтересів держави у кіберпросторі.

У цілому від ефективності реалізації державної політики кібербезпеки, особливо в частині створення потенціалу кіберзахисту та активного впливу в кіберпросторі, безпосередньо залежать подальший розвиток ситуації, пов'язаної з агресією Російської Федерації проти України й тимчасовою окупацією частини української території, а також проведення операції Об'єднаних сил на території Донецької та Луганської областей, суспільно-політична обстановка в державі й особливо на Донбасі, та наші позиції на міжнародній арені.

© Живило Є. О., 2019

На досягнення цього значною мірою впливають внутрішні чинники, які обмежують можливості держави протидіяти негативному впливу в кіберпросторі, основними з яких є:

– нерозвиненість, моральна та фізична застарілість, уразливість від протиправного впливу існуючої інформаційної інфраструктури (в першу чергу інформаційно-телекомунікаційних мереж і систем) держави, яка використовується в інтересах оборони держави;

– активне впровадження та використання в державі інформаційних технологій (систем, продуктів) іноземного походження, які не забезпечують належного рівня безпеки використання та несуть в собі складність контролю за їх обігом;

– ускладненість щодо розмежування військових і цивільних об'єктів критичної інфраструктури держави в кіберпросторі;

– можливість недержавних суб'єктів та неавторизованих (індивідуальних) користувачів здійснювати протиправні дії (кібервпливи) в кіберпросторі та проблематичність їх виявлення;

– порушення встановленого національним законодавством порядку обміну інформацією з обмеженим доступом у сфері оборони;

– зниження науково-технічного потенціалу України, нерозвиненість національної інноваційної системи в інформаційній сфері та низький рівень конкурентоспроможності в ній;

– недостатнє нормативно-правове регулювання діяльності суб'єктів забезпечення кібербезпеки держави в частині їх участі в підготовці та веденні кібероборони;

– недостатній з огляду на зростаючий обсяг завдань кількісно-якісний склад сил (підрозділів) суб'єктів забезпечення кібербезпеки держави, їх недостатня укомплектованість кваліфікованими фахівцями.

У той же час Україна має потужний людський ресурс, ІТ-потенціал держави й тривалий досвід відсічі збройної агресії з боку РФ. Тому пріоритетними напрямками спрямування зусиль Міноборони, Збройних Сил та

© Zhivilo E. O., 2019

Держспецтрансслужби України є розвиток державно-приватного партнерства, різноманітних проектів громадянського суспільства, залучення волонтерів і добровольців до заходів з оборони держави та забезпечення її інформаційної і кібербезпеки, а також набуття оперативної сумісності із збройними силами держав-членів НАТО для спільних дій з упровадження сучасних підходів щодо ефективних дій у кіберпросторі.

За таких умов набуває актуальності дослідження кібероборони, а саме її сутності та призначення.

Аналіз останніх досліджень і публікацій. Відповідно до Закону України "Про основні засади забезпечення кібербезпеки України" (далі – Закон), кібероборона – це сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії [4].

Україна взяла на себе зобов'язання перед НАТО та державами-партнерами щодо впровадження сучасних підходів до кібероборони, розвитку необхідних спроможностей сектору безпеки і оборони держави для дій в кіберпросторі та досягнення оперативної сумісності з питань забезпечення кібербезпеки з Альянсом.

Зокрема, ст. 8 Закону України "Про основні засади забезпечення кібербезпеки України" [4] на Міністерство оборони України (далі – Міноборони), Генеральний штаб Збройних Сил України покладено, відповідно до компетенції, завдання щодо здійснення заходів з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони), здійснення військової співпраці з НАТО та іншими суб'єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз і впровадження заходів із забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану.

Аналіз правових та організаційних основ у сфері кібербезпеки держави

© Живило Є. О., 2019

дозволяє деталізувати сам термін "кібероборона" як інтегровану форму дій за єдиним замислом і планом визначених сил та засобів Міноборони, Збройних Сил, Держспецтрансслужби у взаємодії з іншими суб'єктами забезпечення національної безпеки держави відповідно до їх повноважень у кіберпросторі, через кіберпростір та (за необхідності) через інші домени збройного протиборства для впливу на кіберпростір, в результаті якого досягається визначена мета. Виходячи з цього, головною метою кібероборони та її складовими в сучасних умовах є захист інтересів України в кіберпросторі в умовах загрози та відбиття воєнної агресії проти України. В подальшому з набуттям необхідних спроможностей Міноборони, Збройними Силами та Держспецтрансслужбою їх повноваження щодо кібероборони можуть бути поширені на захист інших інтересів особи, суспільства та держави, які пов'язані з кіберпростором.

Мета статті – розкрити сучасні підходи до визначення складових кібероборони Української держави.

Виклад основного матеріалу. За результатами вивчення підходів держав-членів НАТО щодо реагування на загрози в кіберпросторі [2], а також з урахуванням досвіду проведення Антитерористичної операції та операції Об'єднаних сил на території Донецької й Луганської областей найбільш сучасною й одночасно перспективною формою реалізації державної політики за напрямком забезпечення кібербезпеки у воєнній сфері слід вважати створення та ефективне функціонування системи кібероборони як організованої сукупності суб'єктів і об'єктів кібероборони з визначеними зв'язками між ними, об'єднаних єдиним керівництвом.

Основним змістом ведення кібероборони є сукупність узгоджених і взаємопов'язаних за метою, завданнями, об'єктами, місцем та часом одночасних і послідовних заходів у кіберпросторі та через кіберпростір щодо запобігання, виявлення, стримування, активного реагування на агресію противника та мінімізації наслідків від його кібервпливу, які готуються й проводяться за єдиним замислом і планом силами та засобами Збройних Сил із

© Zhivilo E. O., 2019

залученням необхідних можливостей інформаційної інфраструктури та ресурсів держави у взаємодії з військовими формуваннями та правоохоронними органами, іншими суб'єктами забезпечення кібербезпеки держави відповідно до їх компетенції.

Ураховуючи комплексний характер підготовки та ведення кібероборони, з метою розподілу та узгодження практичних заходів діяльності органів військового управління та дій військ (сил) в Міноборони, Збройних Силах та Держспецтрансслужбі пропонується визначити організаційну, інституалізаційну, функціональну, виконавчу, просторову та часову складові системи кібероборони.

Організаційна складова кібероборони випливає із нормативного визначення сутності кібероборони та включає сукупність заходів, розподілених на політичні, економічні, соціальні, військові, наукові, науково-технічні, інформаційні, правові, освітні, організаційні та інші заходи.

Інституалізаційна складова кібероборони реалізується шляхом створення, розвитку та функціонування органів державної влади, органів управління військ (сил), окремих військових частин (підрозділів), установ, організацій з визначеними завданнями та повноваженнями щодо підготовки та ведення кібероборони.

До участі в підготовці та веденні кібероборони залучаються у встановленому порядку структурні підрозділи Міноборони, Генерального штабу Збройних Сил, Держспецтрансслужби, інші органи військового управління всіх рівнів, війська (сили), військові навчальні заклади, науково-дослідні установи, інші установи та організації Міноборони, Збройних Сил та Держспецтрансслужби.

Враховуючи інноваційний характер набуття Міноборони, Збройними Силами та Держспецтрансслужбою необхідних спроможностей з кібероборони, зазначене потребує створення та функціонування принципово нових організаційних одиниць органів управління та військ (сил) за напрямом кібербезпеки [4], у т.ч. наукових, навчальних, експериментальних, навчально-

© Живило Є. О., 2019

бойових, випробувальних тощо, включаючи формування інтегруючого роду військ для забезпечення кібербезпеки.

Функціональна складова кібероборони включає [5]:

– запобігання (англ. – "Prevention") – заходи щодо завчасного виявлення, уникнення, стримування, запобігання можливих (потенційних) кіберзагроз чи кібератак, припинення підготовки до них;

– захист (англ. – "Protection") – заходи щодо забезпечення випереджувального захисту від можливих кібератак (кібервпливу) противника, в першу чергу в інтересах всебічного та стійкого забезпечення у кіберпросторі процесів управління власними військами та зброєю;

– попередження (англ. – "Mitigation") – заходи щодо безпосереднього виявлення, відвернення загрози, зменшення можливих втрат (збитків, пошкоджень) в разі безпосередньої загрози проведення кібератак. При певних умовах в межах зазначеного можуть проводитися випереджувальні (зустрічні) заходи активного кіберзахисту;

– реагування (англ. – "Response") – заходи комплексного реагування та впливу на противника, у т.ч. шляхом активного кіберзахисту в умовах безпосереднього проведення ним кібератак з одночасним проведенням заходів захисту власної інфраструктури, особового складу, ресурсів тощо від впливу противника;

– відновлення (англ. – "Recovery") – заходи, направлені на відновлення інформаційної та іншої інфраструктури, яка стала об'єктом кібератак противника, стабілізацію ситуації та ліквідації інших негативних наслідків.

Виконавча складова кібероборони реалізується через систему заходів присутності, використання та дій у кіберпросторі відповідно до завдань та повноважень Міноборони, Збройних Сил та Держспецтрансслужби.

Іншими складовими ведення активної кібероборони є необхідні заходи в межах здійснення розвідувальної діяльності, радіоелектронне придушення роботи телекомунікаційних та інших засобів, фізичний вплив (вогневе ураження) на об'єкти інформаційної інфраструктури, здійснення кіберзахисту

© Zhivilo E. O., 2019

(у т.ч. активного кіберзахисту) власної інформаційної інфраструктури (засобів рухомого зв'язку, як апаратної, так і контентної складових, додатків та сервісів зв'язку, інших інформаційно-телекомунікаційних систем та об'єктів інформаційної діяльності суб'єктів оборони держави) від кібератак та кібервпливу противника [6], що забезпечує необхідний рівень інформаційного забезпечення управління військами та зброєю, інші дії в кіберпросторі тощо. Зазначені заходи можуть проводитися як складова частина кібероборони або як окремі самостійні заходи під час підготовки та застосування військ (сил), їх участі в проведенні операції Об'єднаних сил, антитерористичній операції тощо.

Просторова складова кібероборони носить умовний характер, оскільки на відміну від визнаних (традиційних) сфер (доменів) збройного протиборства, якими є "суша", "повітря", "вода", "космос", сфера "кіберпростір" не має чітко визначених кордонів. Тому просторова складова системи кібероборони розглядається переважно стосовно місць (районів) фізичного розташування об'єктів інформаційної інфраструктури (у т.ч. з урахуванням їх національної належності та державних кордонів) та районів застосування (відповідальності) військ (сил) щодо виконання ними завдань за призначенням.

Часова складова кібероборони на теперішній час розглядається стосовно умов мирного часу, у випадку воєнної агресії проти України або загрози нападу на Україну (в особливий період, під час воєнного стану (в умовах правового режиму воєнного стану), в воєнний час), а також в умовах правового режиму надзвичайного стану, під час проведення антитерористичної операції та заходів із забезпечення національної безпеки і оборони, відсічі і стримування збройної агресії Російської Федерації у Донецькій та Луганській областях. У межах зазначеного заходи кібероборони розподіляються на заходи завчасної підготовки, безпосередньої підготовки кібероборони та власне заходи ведення кібероборони.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямку. Зазначена тематика є актуальною з огляду на те, що стрімкий розвиток телекомунікаційної інфраструктури, зростання потреби в

© Живило Є. О., 2019

якості електронних послуг створили передумови використання кіберпростору як окремої сфери і нагальної необхідності забезпечення ефективної кібероборони, що має базуватися на науковій основі.

Автор дослідив підходи держав-членів НАТО щодо реагування на загрози в кіберпросторі та запропонував проводити розгляд кібероборони через організаційну, інституалізаційну, функціональну, виконавчу, просторову та часову складові системи кібероборони.

Урахування наведених складових кібероборони в ході створення системи кібероборони дозволить підвищити ефективність її функціонування в інтересах досягнення цілей, які визначені перед суб'єктами сектору безпеки і оборони, які забезпечують кібербезпеку.

Список використаних джерел

1. Матриця досягнення стратегічних цілей і виконання основних завдань оборонної реформи : Указ Президента України від 06.06.2016 р. № 240. *Офіційний вісник Президента України*. 2016. № 17. Ст. 466.

2. Офіційний сайт Міністерства оборони США. URL: https://media.defense.gov/2018/sep/18/2002041658/1/cyber_strategy_summary_%20final.%20pdf (дата звернення:04.03.2019).

3. Про Державну програму розвитку Збройних Сил України на період до 2020 р. : Указ Президента України від 22.03.2017 р. № 73. Дата оновлення: 22.03.2017. URL: https://www.president.gov.ua/documents/732017-21498 (дата звернення:04.03.2019).

4. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2469-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403.

5. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 07.09. 2005 р. № 2824-IV. *Відомості Верховної Ради України*. 2006. № 5. Ст. 128 – 71.

6. Стратегія кібербезпеки України : Указ Президента України від 15.03.2016 р. № 96. *Офіційний вісник Президента України*. 2016 № 10. Ст. 198.

References

1. Matrytsia dosiahnennia stratehichnykh tsilej i vykonannia osnovnykh zavdan' oboronnoi reformy: Ukaz Prezydenta Ukrainy vid 06.06.2016 r. № 240. (2016). *Ofitsijnyj visnyk Prezydenta Ukrainy, 17, art. 466*.

2. Official website of the Department of Defense of the USA. URL:https://media.defense.gov/2018/sep/18/2002041658//1/cyber_strategy_summary_%20final.%20pdf.

3. Pro Derzhavnu prohramu rozvytku Zbrojnykh Syl Ukrainy na period do 2020 r.: Ukaz Prezydenta Ukrainy vid 22.03.2017 r. № 73. Data onovlennia: 22.03.2017. URL: https://www.president.gov.ua/documents/732017-21498.

4. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy vid 05.10.2017 r. №2469-VIII. (2018). *Vidomosti Verkhovnoi Rady Ukrainy, 45, art. 403*.

5. Pro ratyfikatsiiu Konventsii pro kiberzlochynnist': Zakon Ukrainy vid 07.09.2005 r. № 2824-IV. (2005). *Vidomosti Verkhovnoi Rady Ukrainy, 5, art. 128, art. 71*.

6. Stratehiia kiberbezpeky Ukrainy: Ukaz Prezydenta Ukrainy vid 15.03.2016 r. 96. (2016). *Ofitsijnyj visnyk Prezydenta Ukrainy, 10, art. 198.*

© Zhivilo E. O., 2019

Zhivilo E. O.,
Post-Graduate Student of the Department of Information Technologies and Control Systems,
KRI NAPA, Kharkiv
ORCID ID 0000-0003-4077-7853

Modern approaches to the definition of the components of the cyber defense of the state

The mentioned topics are relevant given the rapid development of telecommunication infrastructure around the world today, the growth of the need for quality electronic services has created preconditions for the use of cyberspace as a separate sphere and requires the urgent need to provide an effective cyber-defense, which should be based on a scientific basis.

In the course of the study, the author substantiates the components of the cyber defense system. The approaches of the NATO member states and the EU member states to the response to threats in cyberspace are investigated and the implementation of the cyber defense system through the organizational, institutionalized, functional, executive, spatial and temporal components of the national security and defense system of the state has been proposed. Expanded and detailed institutionalization component of the cyber-defense. The issue of active influence in cyberspace within the framework of the cyber defense of the state is researched.

Taking into account the detailed institutionalization component of the cyber-defense in the course of the creation of the cyber-defense system will increase the efficiency of its functioning in the interests of achieving the goals defined by the security and defense sector that provide cybersecurity.

The prospect of further development of this area is the acquisition by the Ministry of Defense of Ukraine, the Armed Forces of Ukraine and the State Special Service of Ukraine of Transport of Ukraine of the necessary capabilities on the cyber defense, which requires the creation and operation of fundamentally new organizational units of government and troops (forces) in the direction of cyber security, including: scientific, educational, experimental, training, combat, testing, etc., including the formation of an integrative army to provide cyber security.

Key words: cyberspace; cyber threats; cyber defense of the state; capabilities; telecommunication infrastructure; cyber defense of critical information infrastructure.

Надійшла до редколегії 18.04.2019 р.

© Живило Є. О., 2019