Державне управління

УДК 351.865

Живило Євген Олександрович
аспірант кафедри інформаційних технологій і систем управління
Харківського регіонального інституту державного управління
Національної академії державного управління при Президентові України
Живило Евгений Александрович
аспирант кафедры информационных технологий и систем управления
Харьковского регионального института государственного управления
Национальной академии государственного управления
при Президенте Украины
Zhivilo Evgen
Postgraduate Student of the
Department of Information Technologies and Management Systems
Kharkiv Regional Institute of Public Administration of the
National Academy of Public Administration under the President of Ukraine

ШЛЯХИ ВРЕГУЛЮВАННЯ НОРМАТИВНО-ПРАВОВОЇ БАЗИ ІЗ ЗАХИСТУ ІНФОРМАЦІЇ, КІБЕРБЕЗПЕКИ ТА КІБЕРОБОРОНИ УКРАЇНИ
ПУТИ УРЕГУЛИРОВАНИЯ НОРМАТИВНО-ПРАВОВОЙ БАЗЫ ПО ЗАЩИТЕ ИНФОРМАЦИИ, КИБЕРБЕЗОПАСНОСТЬ И КИБЕРОБОРОНА УКРАИНЫ
WAYS OF REGULATION OF THE LEGISLATIVE BASIS ON INFORMATION PROTECTION, CYBER SECURITY AND CYBER DEFENSE OF UKRAINE

Анотація. *В статті автором було здійснено аналіз нормативно-правових актів в безпековій сфері та виокремлено ті норми, які мають безпосереднє відношення до державної політики кібербезпеки у сфері кібероборони, визначено основні напрями державної політики кібербезпеки, виявлено фактори, які визначають державну політику кібернетичної безпеки та її основну мету. Запропоновано авторське розуміння категорії "кібернетичне суспільство". Акцентовано увагу на тому, що перелік напрямів державної політики кібербезпеки не може бути статичним, оскільки відбуваються постійні зміни в кіберсуспільстві, тому існує потреба швидкої реакції та вжиття відповідних заходів.*

Сьогодні загальнодержавна нормативно-правова база України не містить дієвих вимог та механізмів щодо організації та виконання органами державної влади, а також операторами і провайдерами телекомунікацій усіх форм власності завдань сфери оборони із забезпечення спеціального зв'язку та захисту інформації в інформаційно-телекомунікаційних системах, кібербезпеки та кібероборони як у мирний час так і в умовах кризових ситуацій, воєнного стану, в особливий період.

Зазначене унеможливлює:

- *організацію ефективного функціонування як національної системи зв'язку так і системи зв'язку Збройних Сил України, інших військових формувань та правоохоронних органів в умовах кризових ситуацій, воєнного стану та в особливий період;*
- *організацію ефективної кібероборони держави.*

Також на загальнодержавному рівні вимоги нормативно-правової бази України унеможливлюють виконання вимоги оперативної цілі 1.5 "Удосконалення системи кібербезпеки та захисту інформації" Матриці досягнення стратегічних цілей і виконання основних завдань оборонної

реформи (додаток до Стратегічного оборонного бюлетеня України, схваленого Указом Президента України від 06.06.2016 № 240/ 2016) в частині: "впровадження заходів із захисту інформації відповідно до вимог нормативно-правових актів України та з урахуванням стандартів НАТО і ISO/IEC [1, с.342]. Впроваджено систему захисту інформації та кібербезпеки з урахуванням стандартів НАТО і ISO/IEC".

Ключові слова: *кібернетичний простір, кібернетичні загрози, кібероборона держави.*

Аннотация. *В статье автором был осуществлен анализ нормативно-правовых актов в сфере безопасности и выделены те нормы, которые имеют непосредственное отношение к государственной политике кибербезопасности в сфере кибероборонны, определены основные направления государственной политики кибербезопасности, выявлены факторы, которые определяют государственную политику кибернетической безопасности и ее основную цель . Предложено авторское понимание категории "кибернетическое общество". Акцентировано внимание на том, что перечень направлений государственной политики кибербезопасности не может быть статичным, поскольку происходят постоянные изменения в киберсуспильстви, поэтому существует потребность быстрой реакции и принятия соответствующих мер.*

Сегодня общегосударственная нормативно-правовая база Украины не содержит действенных требований и механизмов относительно организации и выполнения органами государственной власти, а также операторами и провайдерами телекоммуникаций всех форм собственности задач сферы обороны по обеспечению специальной связи и защиты информации в информационно-телекоммуникационных системах, кибербезопасности и

кибероборонь как в мирное время так и в условиях кризисных ситуаций, военного положения, в период.

Указанное исключает:

- *организацию эффективного функционирования как национальной системы связи так и системы связи Вооруженных Сил Украины, других военных формирований и правоохранительных органов в условиях кризисных ситуаций, военного положения и в особый период;*
- *организацию эффективной кибероборонь государства.*

Также на общегосударственном уровне требования нормативно-правовой базы Украины делают невозможным выполнение требования оперативной цели 1.5 "Совершенствование системы кибербезопасности и защиты информации" Матрицы достижения стратегических целей и выполнения основных задач военной реформы (приложение к Стратегического оборонного бюллетеня Украины, одобренного Указом Президента Украины от 06.06.2016 № 240/ 2016) в части: "внедрение мероприятий по защите информации в соответствии с требованиями нормативно-правовых актов Украины и с учетом стандартов НАТО и ISO/IEC. Внедрена система защиты информации и кибербезопасности с учетом стандартов НАТО и ISO/IEC".

Ключевые слова: *кибернетическое пространство, кибернетические угрозы, кибероборона государства.*

Summary. *The article analyzes the normative legal acts in the security sphere and identifies those norms that are directly related to the state cybersecurity policy, identifies the main directions of the state cybersecurity policy, identifies the factors that determine the state policy of cyber security and cyber security. . The author's understanding of the category "cybernetic society" is offered. Attention is drawn to*

the fact that the list of directions of state cybersecurity policy cannot be static, as there are constant changes in the cyber society, so there is a need for rapid response and appropriate measures.

Today, the national regulatory and legal framework of Ukraine does not contain effective requirements and mechanisms regarding the organization and implementation by government bodies, as well as operators and telecommunications providers of all forms of ownership of the defense tasks to ensure special communication and information protection in information and telecommunication systems, cybersecurity and cyber defense in peacetime and in times of crisis situations, martial law, in the period.

Specified excludes:

- *the organization of effective functioning of both the national communication system and the communication system of the Armed Forces of Ukraine, other military formations and law enforcement agencies in conditions of crisis situations, martial law and in a special period;*
- *the organization of an effective cyber defense state.*

Also at the national level, the requirements of the regulatory framework of Ukraine make it impossible to meet the requirements of operational objective 1.5 "Improving the cybersecurity system and information protection" Matrix of achieving strategic goals and fulfilling the main objectives of military reform (annex to the Strategic Defense Bulletin of Ukraine, 06.06 approved by the President's Decree of Ukraine). 2016 No. 240/2016) in part: "the introduction of measures for the protection of information in accordance with the requirements of regulatory and legal acts of Ukraine and with m NATO and ISO / IEC standards. An information security and cyber security system has been implemented, taking into account NATO and ISO / IEC standards".

Key words: *cyber space, cyber threats, cyber defense of the state.*

Постановка проблеми. Головною загрозою в умовах сучасності для України є висока ймовірність запровадження в кіберпросторі великомасштабної агресії РФ проти України.

Створення Системи, здатної забезпечувати режим постійної готовності об'єктів критичної інформаційної інфраструктури до реальних і потенційних кіберзагроз будь-якого (розвідувально-підривного, терористичного, воєнного, кримінального) характеру є пріоритетним завданням.

Тому вироблення механізмів ефективного реагування на кібератаки, ліквідації їх наслідків, а також швидкому відновленню функціонування об'єктів критичної інформаційної інфраструктури у відповідності до сучасного міжнародного нормативно-правового поля є вкрай важливим та необхідним.

Аналіз останніх досліджень і публікацій. Проблеми забезпечення кібернетичної безпеки України, нормативно-правові відносини в цій галузі , актуальні напрями підвищення ефективності системи забезпечення кібернетичної безпеки, її функції та завдання розглядаються у наукових працях вітчизняних дослідників, а саме: Є. Ю. Бабіч [2], Д. В. Дубов [3], Н. Є. Новікова, І. В. Діордіци, С. В. Мельника, В. І. Кащука та інших.

Проте, незважаючи на значну кількість робіт із даної тематики, існує багато невирішених питань щодо шляхів врегулювання нормативно-правової бази із захисту інформації, кібербезпеки та кібероборони України [3, с. 12].

Формулювання цілей статті (постановка завдання). Мета статті полягає у формуванні та наданні пропозицій до існуючих нормативно-правових актів України у сфері кібербезпеки. Виконання цих заходів надасть можливість забезпечити впровадження у Збройних Силах України заходів із захисту інформації та кібербезпеки відповідно до існуючої сучасної міжнародної нормативно-правової бази таз урахуванням стандартів НАТО і

ISO/IEC і підвищити існуючі спроможності складових сил кібероборони України.

Виклад основного матеріалу. Протягом 2017-2019 років Міністерством оборони України та Генеральним штабом Збройних Сил України постійно проводилась робота щодо упорядкування законодавства у сфері кібероборони України. З цією метою:

- опрацьовано проект Закону України "Про внесення змін до деяких законодавчих актів України щодо протидії загрозам національній безпеці в інформаційній сфері", реєстраційний № 6688 (від 24.07.2017 № 220/5687);
- надані пропозиції до комітетів Верховної Ради України з питань національної безпеки і оборони та з питань інформатизації та зв'язку (від 24.07.2017 № 300/1/с/2970) щодо внесення змін до законів України "Про оборону України", "Про Збройні Сили України", "Про телекомунікації", "Про захист інформації в інформаційно-телекомунікаційних системах" [4, с. 12].

Вищезазначені пропозиції не були розглянуті та впроваджені.

На даний час існуюча нормативно-правова база України не дозволяє Збройним Силам України та іншим військовим формуванням здійснювати ефективну підготовку держави до відбиття воєнної агресії у кіберпросторі (кібероборони) та виконувати заходи з кібероборони як у мирний час, так і в умовах кризових ситуацій, воєнного стану та в особливий період. Зокрема, це пов'язано із відсутністю дієвих вимог та механізмів щодо виконання операторами і провайдерами телекомунікацій усіх форм власності завдань Генерального штабу Збройних Сил України з кібероборони, контролю і блокування трафіка в телекомунікаційних мережах.

Для надання Збройним Силам України та іншим військовим формуванням нормативно-правових підстав для забезпечення належного рівня захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсічі збройної агресії у кіберпросторі, а також з метою нормативно-правового врегулювання порядку виконання вимог:

- підпункту 4 пункту 2 статті 8 Закону України "Про основні засади забезпечення кібербезпеки України" від 05.10.2017 № 2163-VIII в частині "здійснення Генеральним штабом Збройних Сил України заходів з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони)";
- Указу Президента України від 14.03.2016 № 92/2016 "Про рішення Ради національної безпеки і оборони України від 4 березня 2016 року "Про Концепцію розвитку сектору безпеки і оборони України" [5, с.2]., а саме додатку до Указу – "Розподіл відповідальності складових сектору безпеки і оборони України за організацію планування, реагування на загрози та під час виконання завдань за призначенням", в частині виконання Збройними Силами України організації планування і реагування на загрози "здійснення системних та масштабних дій проти інтересів України у кіберпросторі іноземними державами (групами держав), зокрема із залученням кіберпідрозділів збройних сил іноземних держав, шляхом використання спеціальних засобів (кіберозброєнь)";
- підпункту 11 пункту 1 статті 8 Закону України "Про правовий режим воєнного стану" від 12.05.2015 № 389-VIII в частині "заборони на передачу інформації через комп'ютерні мережі", пропонується **ініціювати розробку проекту Закону України** "Про внесення змін до деяких Законів України", до редакції якого включити такі пропозиції:

Внести зміни до таких нормативно-правових актів України:

1. **У Законі України “Про телекомунікації” від 18.11.2003 № 1280-15 (із змінами):**

а) частину першу статті 39 після пункту 13 доповнити новим пунктом такого змісту:

“14) за повідомленням Генерального штабу Збройних Сил України надавати інформацію про свої телекомунікаційні мережі та організовувати виконання організаційних і технічних заходів з кібероборони (активного кіберзахисту)”.

У зв’язку з цим пункт 14 частини першої вважати пунктом п’ятнадцятим;

б) статтю 65 доповнити новим п’ятим пунктом такого змісту:

“5. Оператори, провайдери телекомунікацій в умовах воєнного стану та в особливий період зобов’язані забезпечувати виконання розпоряджень Генерального штабу Збройних Сил України з кібероборони, кібербезпеки, контролю і блокування трафіка в телекомунікаційних мережах усіх форм власності”.

2. **В “Порядку оперативно-технічного управління телекомунікаційними мережами в умовах надзвичайних ситуацій, надзвичайного та воєнного стану”, затвердженому постановою Кабінету Міністрів України від 29.06.2004 № 812 (із змінами):**

а) доповнити редакцію після пункту 7 новим пунктом такого змісту:

“8. На період введення воєнного стану в Україні або в окремих її місцевостях та в особливий період Національний центр та центри управління мережами виконують розпорядження Генерального штабу Збройних Сил України з кібероборони, кібербезпеки, контролю і блокування трафіка в телекомунікаційних мережах усіх форм власності”.

У зв'язку з цим пункт восьмий вважати пунктом дев'ятим;

3. У Законі України "Про оборону України" від 06.12.1991 № 1932-12 (із змінами):

а) статтю 1 доповнити новими абзацами такого змісту:

кібероперація – сукупність узгоджених дій воєнних підрозділів кібербезпеки в кіберпросторі, спрямованих на забезпечення кібероборони держави";

б) друге речення частини другої статті 4 доповнити текстом такого змісту:

"у тому числі проведення спеціальних операцій (розвідувальних, інформаційно-психологічних, інформаційних тощо) та кібероперацій у кіберпросторі";

в) частину другу статті 10 після абзацу шістнадцятого доповнити новими абзацами такого змісту:

"здійснює інформаційно-аналітичну діяльність в інтересах кібероборони держави";

"здійснює постійний моніторинг кіберпростору, виявляє потенційні та реальні кіберзагрози національній безпеці та обороні України, проводить аналіз воєнно-політичної обстановки та визначає рівень воєнної загрози національній безпеці України з використанням кіберпростору";

г) статтю 11 після частини другої доповнити новою частиною третьою такого змісту:

"Генеральний штаб Збройних Сил України є головним органом з кібероборони держави та головним військовим органом з планування кібероборони держави, координації та контролю за виконанням завдань у сфері кібероборони органами виконавчої влади, органами місцевого самоврядування, операторами і провайдерами телекомунікацій, військовими

формуваннями, утвореними відповідно до законів України, правоохоронними та розвідувальними органами у межах, визначених законами України і нормативно-правовими актами Президента України, Верховної Ради України та Кабінету Міністрів України.

У зв'язку з цим частину третю вважати частиною четвертою;

д) абзац восьмий частини третьої статті 11 викласти в такій редакції:

"бере участь в організації та контролює підготовку системи зв'язку, національної системи кібербезпеки, комунікацій і в цілому території держави до оборони";

е) абзац одинадцятий частини третьої статті 11 викласти в такій редакції:

"бере участь в організації використання та контролю за повітряним, водним, інформаційним простором і кіберпростором держави та здійснює його в особливий період";

ж) абзац шістнадцятий частини третьої статті 11 викласти в такій редакції:

"організовує використання національної системи зв'язку та національної системи кібербезпеки в інтересах оборони, здійснює відповідно до закону управління та регулювання в сфері використання радіочастотного ресурсу, виділеного для цілей оборони";

з) частину третю статті 11 після абзацу 16 доповнити новим абзацом такого змісту:

"організовує та координує заходи з кібероборони, кібербезпеки, контролю і блокування доступів до інформації в інформаційно-телекомунікаційних системах усіх форм власності на період введення воєнного стану в Україні або в окремих її місцевостях та в особливий період".

У зв'язку з цим абзац сімнадцятий частини третьої вважати абзацом вісімнадцятим;

и) абзац 8 частини першої статті 13 викласти в такій редакції:

"узгоджують з Генеральним штабом Збройних Сил України питання використання повітряного, водного, інформаційного простору та кіберпростору держави";

4. У Законі України "Про Збройні Сили України" від 06.12.1991 № 1934-12 (із змінами):

1) частину другу статті 1 викласти в такій редакції:

"Збройні Сили України забезпечують стримування збройної агресії проти України та відсіч їй, охорону повітряного простору держави та підводного простору у межах територіального моря України, здійснення заходів щодо кібероборони (активного кіберзахисту) у випадках, визначених законом, беруть участь у заходах, спрямованих на боротьбу з тероризмом";

2) доповнити статтю 1 новою третьою частиною, яку викласти в такій редакції:

"З'єднання, військові частини і підрозділи Збройних Сил України відповідно до закону можуть залучатися до виконання завдань кібероборони (активного кіберзахисту) та проведення військових розвідувальних, інформаційно-психологічних, інформаційних операцій, кібероперацій тощо";

У зв'язку з цим частину третю вважати частиною четвертою;

3) доповнити статтю 1-1 новою третьою частиною, яку викласти в такій редакції:

"Під час залучення до виконання завдань з кібероборони (активного кіберзахисту) з'єднання, військові частини і підрозділи Збройних Сил України мають право:

розробляти, зберігати і використовувати спеціальні засоби та зброю для ведення кіберрозвідки, кіберзахисту та активних (бойових) дій у кіберпросторі".

У зв'язку з цим частину третю вважати частиною четвертою.

5. У Законі України "Про захист інформації в інформаційно-телекомунікаційних системах" від 05.07.1994 № 80/94-ВР (із змінами):

доповнити статтю 10 новим абзацом такого змісту:

"Вимоги до захисту систем оборонного та військового призначення встановлюються Генеральним штабом Збройних Сил України з урахуванням положень міжнародних стандартів та стандартів НАТО".

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі. Внесення змін до зазначених нормативно-правових актів України, зокрема, надасть можливість:

– створити систему кібероборони – забезпечити нормативно-правові засади та ввести правові механізми для виконання вимог Закону України "Про основні засади забезпечення кібербезпеки України" за напрямом кібероборони;

– створити вертикаль органів управління у сфері кібероборони – забезпечити ефективну взаємодію та спільне виконання завдань з кібероборони Міністерством оборони України, Генеральним штабом ЗС України, Держспецзв'язку України, правоохоронними, розвідувальними і контррозвідувальними органами; врегулювати питання державно-приватної взаємодії Збройних Сил України у сфері кібербезпеки; забезпечити участь суб'єктів кібербезпеки держави, операторів та провайдерів телекомунікацій у виконанні заходів з кібероборони;

– надати Збройним Силам України повноваження на виконання заходів з кібероборони на законодавчому рівні (урегулювати питання щодо недопущення застосування вимог Кримінального кодексу України до особового складу під час виконання завдань у кіберпросторі);

– організувати ефективну підготовку держави до відбиття воєнної агресії у кіберпросторі (кібероборони) у мирний час та ефективну кібероборону держави в умовах кризових ситуацій, воєнного стану, в особливий період;

– в подальшому, як перспективи розвитку - внесення змін до зазначених нормативно-правових актів України, надасть можливість забезпечити впровадження у Збройних Силах України заходів із захисту інформації та кібербезпеки відповідно до вимог нормативно-правових актів України та з урахуванням стандартів НАТО і ISO/IEC.

Література

1. Матриця досягнення стратегічних цілей і виконання основних завдань оборонної реформи, додаток № 1 до Стратегічного оборонного бюлетеня України, схваленого Указом Президента України від 6 червня 2016 р. № 240/2016 // Офіційний вісник Президента України від 22.06.2016 – 2016 р., № 17, С. 11, ст. 466.
2. Бабич Є. Ю. Забезпечення кібербезпеки в Україні / Є. Ю. Бабич // Актуальні задачі та досягнення у галузі кібербезпеки : матеріали Всеукр. наук.-практ. конф., м. Кропивницький, 23–25 листопада 2016 р. Кропивницький : КНТУ, 2016. С. 77–78.
3. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія / Д. В. Дубов. К: НІСД, 2014. С. 328.

4. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 7 вересня 2005 року № 2824-IV // Відомості Верховної Ради України. 2006. № 5. С. 128. Ст. 71.
5. Указ Президента України №92/2016 від 14 березня 2016 року, Про рішення Ради національної безпеки і оборони України від 4 березня 2016 року “Про Концепцію розвитку сектору безпеки і оборони України”. URL: https://zakon.rada.gov.ua/laws/show/92/2016.

References

1. Matrycja dosjaghnennja strateghichnykh cilej i vykonannja osnovnykh zavdanj oboronnoji reformy, dodatok # 1 do Strateghichnogho oboronnogho bjuletenja Ukrajiny, skhvalenogho Ukazom Prezydenta Ukrajiny vid 6 chervnja 2016 r. # 240/2016 // Oficijnyj visnyk Prezydenta Ukrajiny vid 22.06.2016 – 2016 r., # 17, S. 11, st. 466.
2. Babych Je. Ju. Zabezpechennja kiberbezpeky v Ukrajini / Je. Ju. Babych // Aktualjni zadachi ta dosjaghnennja u ghaluzi kiberbezpeky : materialy Vseukr. nauk.-prakt. konf., m. Kropyvnycjkyj, 23–25 lystop. 2016 r.Kropyvnycjkyj : KNTU, 2016. S. 77–78.
3. Dubov D. V. Kiberprostir jak novyj vymir gheopolitychnogho supernyctva : monoghrafija / D. V. Dubov. K: NISD, 2014. S. 328.
4. Pro ratyfikaciju Konvenciji pro kiberzlochynnistj: Zakon Ukrajiny vid 7 veresnja 2005 roku # 2824-IV // Vidomosti Verkhovnoji Rady Ukrajiny. 2006. # 5. S. 128. St. 71.
5. Ukaz Prezydenta Ukrajiny #92/2016, Pro rishennja Rady nacionaljnoji bezpeky i oborony Ukrajiny vid 4 bereznja 2016 roku “Pro Koncepciju rozvytku sektoru bezpeky i oborony Ukrajiny”. URL: https://zakon.rada.gov.ua/laws/show/92/2016.