Якимчук Олег Феодосійович,
аспірант,
Національний університет водного господарства та природокористування,
м. Рівне
ORCID 0000-0002-0960-8835

УДК 351/354 **doi: 10.34213/ap.19.01.04**

ДЕРЖАВНЕ УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Розроблено напрями стимулювання реалізації заходів з національної безпеки, у тому числі із кібербезпеки. Виявлено основні загрози розвитку надійної системи кібербезпеки в Україні та запропопоновано рекомендації щодо її удосконалення на основі впровадження заходів із посилення інформатизації суспільства.
Ключові слова: кібербезпека, інформатизація, гібридна війна, законодавство.

Постановка проблеми. Інформаційні спецоперації, хакерські атаки, бойове використання соцмереж та інтернет-сервісів – це питання сучасного життя, які постали на порядку денному перед державними органами влади. Задля протидії цим загрозам, нівелювання негативних ризиків для громадянських прав і суспільної безпеки під час кібервійни держава повинна сформувати ефективну модель національної безпеки. Це завдання є надактуальним в сучасних умовах гібридної війни. Гібридна агресія Російської Федерації щодо України є поєднанням різноманітних комбінацій форм й методів деструктивного впливу, серед яких домінуючим напрямком є інформаційний й кібернетичний.

Важливим аспектом негативного інформаційного впливу, що намагаються здійснювати російські спецслужби, є його спрямованість на руйнування української державності починаючи від базового рівня – історичної пам'яті й самоусвідомлення нації як такої. Задля цього російські спецслужби використовують підконтрольні їм ЗМІ, інтернет-ресурси, групи у соцмережах, блогерів, тролів й навіть поштові сервіси. Саме через цю розгалужену мережу не лише збирається розвідувальна інформація про українських громадян, але й провадяться деструктивні пропагандистські інформаційні операції. Паралельно проводиться виснаження фінансових і матеріальних ресурсів України, створення передумов до втрати нею енергетичної незалежності, ослаблення транзитного потенціалу й дискредитація нашої держави на міжнародній арені із подальшим формуванням негативного політичного іміджу. При цьому, деструктивний інформаційний вплив та маніпулювання суспільною свідомістю російські спецслужби поєднують із веденням цинічних за задумом й катастрофічних за наслідками кібератак на стратегічні об'єкти України. Все це сформувало актуальність даного дослідження, її мету, об'єкт і предмет.

Аналіз останніх досліджень і публікацій. Існує чисельна кількість наукових публікацій із проблем безпеки. Проте, переважно вони розглядають сутність й механізми забезпечення національної безпеки. Зокрема, це питання досліджували такі вчені як Г. Андрощук, Т. Васильців, В. Геєць, В. Ліпкан, І. Татаркіна, Є. Хлобистов, О. Радченко, Є. Романенко та інші. Попри вагомі напрацювання вчених, питання кібербезпеки досліджувалися недостатньо. Все це сформувало мету, предмет та об'єкт даного дослідження.

Постановка завдання. Дослідити процес державного управління кібербезпекою України й розробити рекомендації щодо її удосконалення на основі впровадження заходів із посилення інформатизації суспільства.

Виклад основного матеріалу. Низка потужних й складних кібератак на комп'ютерні мережі енергетичного, транспортного секторів, банківського, галузі зв'язку, які відбулись від 2014 р., вкотре засвідчили, що російський агресор і надалі використовуватиме кібератаки як інструмент геополітичного впливу. Протидія цьому потребує управлінських ініціатив на національному рівні, а також відпрацювання дієвих механізмів міжнародного співробітництва. У якості яскравих прикладів активних інформаційних заходів російських спецслужб є такі, як спроба дестабілізувати ситуацію в Україні через використання заборонених соцмереж й розповсюдження антиукраїнського контенту, спрямованого на розкол українського суспільства й розхитування суспільно-політичної ситуації, намагання здійснити низку об'єднаних єдиним задумом провокацій, розгортання цілої агентурної мережі російських спецслужб у регіонах України, метою якої є інспірування масових заворушень та провокацій щодо патріотичних сил шляхом виготовлення та розвішування в публічних місцях прапорів із забороненою символікою тоталітарних режимів.

Сучасна діяльність державних й економічних органів будь-якої держави ґрунтується на використанні різного роду комп'ютерно-інформаційних систем, вплив на які може суттєво змінити хід справ економічного й політичного характеру. Мова іде про кібербезпеку держави і її структур. Саме тому питання забезпечення кібербезпеки є надзвичайно актуальними для України, особливо в умовах російської агресії, а заходи із протидії викликам і загрозам у зазначеній сфері перебувають на початковому етапі та поки що не мають комплексного характеру. В Інтернет протистоянні Росії проти України вперше було застосовано троянські програми, зокрема вірус "Uroborus". З одного боку, завданням цього вірусу було формування бот-мережі із заражених комп'ютерів й отримання повноцінного доступу до їх наповнення, а з іншого – викрадення інформації. Об'єкти атаки також, вочевидь, були обрані не випадково. Адже переважно це були веб-ресурси органів державної влади (в тому числі силових структур), стратегічних фінансових установ, засобів масової інформації, великих промислових підприємств [1]. Українські фахівці виявили кілька особливостей цього вірусу: складність програмного коду (що зумовлює можливість його розроблення із залученням значної чисельності людських, технічних і фінансових ресурсів (зокрема, це можуть бути державні установи, спецслужби, науково-дослідні установи, IT-корпорації, тощо) [2].

Тимчасова заборона російських соціальних мереж й програмних продуктів лише мотивувала російські хакерні компанії до пошуку нових хакерських розробок, вірусів задля впливу на кіберпростір. Щодня кількість кібератак проти України динамічно зростає. Схожа ситуація спостерігається у багатьох країнах Європи й США, які на тлі зростання кібератівності Росії і деяких східних країн започаткували низку нових ініціатив щодо кіберзахисту. Тому нині постає серйозне питання щодо готовності України реагувати на нові виклики. Якщо говорити про кібератаки на Україну з боку Росії, потрібно спочатку згадати про Крим, коли Росія захопила військові бази та інфраструктуру: теле- і радіовежі, кабельні та інтернет-мережі. Вони відключали українські канали і включили російські. Крим інформаційно з кінця лютого 2014 року залишився без підтримки і захисту із боку України. Рада Національної безпеки та оборони ще з березня 2014 року наголошувала на тім, що російські канали почали транслювати неправдиву інформацію про події в Криму, але конкретних дій спочатку не могли погодити. Український сайт ЦВК у 2014 р. зазнав хакерської атаки також. І таких прикладів надзвичайно багато.

Питання формування ефективного кіберпростору в Україні давно потребувало вирішення. Чинна нормативно-правова база [3-8] не охоплювала всі основні елементи, необхідні для ефективної протидії кіберзлочинам усіх рівнів складності. Однією із важливих проблем у цій сфері була термінологічна невизначеність. Спостерігалось надто довільне використання значної кількості кібербезпекових понять (та їх синонімів), часто неузгоджених між собою. Зокрема, у Законі України "Про основи національної безпеки України" згадуються *комп'ютерна злочинність* і *комп'ютерний тероризм,* причому жоден із цих термінів не отримав визначення ні у цьому, ані в інших нормативних документах.

Як стверджують фахівці, Закон України "Про основні засади забезпечення кібербезпеки України" переважно є декларативним й складає лише основу майбутніх нормативно-правових актів сфери кібербезпеки, яка повина бути напрацьована і створить належні умови боротьби із кіберзлочинністю. Досі дискусійними є питання щодо кінцевої відомчої підпорядкованості як новостворюваної структури, так й інших елементів, які визначатимуться як ключові в Національній системі кібербезпеки.

Проблемними питаннями, які повинні найближчим часом бути розробленими, є визначення об'єктів з критичною інфраструктурою, які повинен, відповідно Закону України "Про основні засади забезпечення кібербезпеки України", визначити Кабінет Міністрів України, визначення кіберзагроз у військовій і інших сферах, визначення форм і способів конкретних кібернетичних дій, організація проведення кібернетичних навчань й тренувань на рівні силових структур та органів державного і місцевого управління, створення сертифікованих засобів кібернетичної боротьби, визначення механізму сертифікації цих засобів, підготовка відповідних фахівців-професіоналів, удосконалення нормативно-правової та роз'яснюючої бази, створення координуючого навчально-випробувального кібернетичного центру підготовки та екстреної допомоги [3; 9–11].

Відповідно до діючих керівних документів із питань кіберзахисту держави та умовами агресії РФ на всіх рівнях управління з питань кібернетичного захисту, повинна здійснюватися завчасна та безпосередня підготовка, яка передбачає систему дій щодо кібернетичного захисту, кібернетичного впливу та кібернетичної розвідки. Особлива роль і значення розвитку кібербезпеки відводиться здійсненню кібернетичної розвідки як в у межах безпосередньої підготовки, так і завчасної – превентивної. Зокрема, у цьому напрямі завчасно повинні здійснюватися такі заходи: виявлення закономірностей та зв'язків між абонентами соціальної мережі, вивчення, накопичення і аналіз інформації про ймовірні об'єкти впливу; вибір об'єктів розвідки, виявлення факторів ризику й загроз безпеці держави й економіки; визначення сил та засобів, які можуть бути залучені до здійснення впливу; постійний моніторинг інформаційних джерел й збереження їх у базі даних; підсилення позитивного і локальна нейтралізація негативного повідомлення; автоматизація процесу вилучення інформації у повідомленні; формування прогнозів й рекомендацій щодо розвитку ситуації; виявлення механізмів блокування.

Вирішення цих питань, організація роботи головного центру кібернетичної безпеки й структурних підрозділів на рівні органів місцевої влади надасть змогу поставити на відповідний рівень питання кіберзахисту і забезпечити протистояння державних й інших структур у сфері кіберпростору. Це, безумовно, забезпечить можливість проведення постійного моніторингу кібернетичного простору, оперативного оповіщення органів державного управління

про виявлені загрози, дослідження програмно-апаратних засобів кібернетичної розвідки, захисту та впливу (активної протидії) на базі кібернетичного полігону, проведення наукових досліджень з питань інформаційної та кібернетичної безпеки, розробку пропозицій й відпрацювання питань щодо взаємодії із іншими установами, спецслужбами й організаціями, розробку теоретичних засад підготовки фахівців у сфері інформаційної й кібернетичної безпеки.

Регіональна програма інформатизації повинна враховувати низку напрямів, які складають програму соціально-економічного розвитку регіону. Механізми організації спільної діяльності державної адміністрації області та обласної ради щодо реалізації Концепції інформатизації діяльності органів державної влади й органів місцевого самоврядування повинні ґрунтуватися на принципах визначення конкретних завдань та механізмів їх вирішення в затверджених цільових програмах і планах робіт; максимального використання вже існуючих головних розробок, а також програмних, технічних засобів і новітніх інформаційних технологій; існування джерел фінансування у повному обсязі та їх надійності; затвердження термінів отримання кінцевого результату вирішення завдання; тривалості подальшої експлуатації впроваджених проектних рішень; належного рівня підготовленості персоналу розробників і користувачів.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямку. Кіберзлочинність набирає обертів по всьому світу, її жертвою може стати кожен активний користувач Всесвітньої мережі. Лише після масштабних кібератак, які були здійснені на чисельну кількість українських компаній і державні інституції, в Україні всерйоз задумалися про регулювання сфери кіберзахисту. Система управління інформатизацією адміністративно-територіальних одиниць України має включати структурні підрозділи органів виконавчої влади, які виконують функції замовника, а також мати представництво суспільних організацій та підприємницьких кіл. З метою вдосконалення системи управління інформатизацією органів необхідно створення Регіонального інформаційно-аналітичного центру, який буде здійснювати виконавчу, контрольну й координаційну функції. Інформаційно-аналітичні підрозділи управлінь органів державної адміністрації, органів місцевого самоврядування обласного, місцевого й районного рівнів, у свою чергу, мають забезпечувати інформаційно-аналітичну підтримку прийняття рішень керівництвом органів обласної державної адміністрації та органів місцевого самоврядування, впровадження й експлуатацію програмно-технічних модулів інформаційно-аналітичної системи органів державної влади та органів місцевого самоврядування, обслуговування й експлуатацію програмно-апаратних засобів, мережного обладнання засобів зв'язку. Світ змінює своє ставлення до проблем кібербезпеки, і на прикладі України зростає усвідомлення того, що найнебезпечнішими є не хакери-одинаки, а кібернетичні й інформаційні загрози, що виходять від агресивно-налаштованих країн та їх спецслужб.

Національною спецслужбою щодня нівелюються російські інформаційні впливи та відбиваються кібернетичні атаки. Для того, аби ця злагоджена команда працювала ще більш ефективно та зростала у своєму професіоналізмі потрібні дві речі: отримання нових законодавчо-визначених інструментів протидії російським кібернетичним та інформаційними впливам; збільшення фінансування підрозділів інформаційної та кібернетичної безпеки задля закупівлі новітнього програмного забезпечення і устаткування, а також матеріального стимулювання фахівців високого рівня. В сучасних умовах необхідне підвищення рівня громадянської свідомості й медійної грамотності населення,

яке є безпосереднім споживачем інформації. Нині лише спільними зусиллями громадськості й правоохоронних органів можна успішно та дієво протистояти пропаганді та інформаційній агресії проти України.

Список використаних джерел

1. Указ Президента України "Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року "Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України" № 449/2014 від 01.05.2014. URL: https://zakon.rada.gov.ua/laws/show/449/2014 (дата звернення: 26.01.2019).

2. Литвин А. Що дасть Україні новий закон про кібербезпеку. 2018. URL: https://biz.censor.net.ua/m3069149 (дата звернення: 26.01.2019).

3. Про інформацію : Закон України за станом на 06.12.2016 р. : офіц. вид. Верховна Рада України. Київ : Парлам. вид-во, 2016. 10 с.

4. Про основи національної безпеки України : Закон України за станом на 07.11.2017 р. : офіц. вид. Верховна Рада України. Київ : Парлам. вид-во, 2017. 16 с.

5. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України за станом на 27.03.2014 р. : офіц. вид. Верховна Рада України. Київ : Парлам. вид-во, 2014. 3 с.

6. Про основні засади забезпечення кібербезпеки України : Закон України за станом на 10.05.2018 р. : офіц. вид. Верховна Рада України. Київ : Парлам. вид-во, 2018. 8 с.

7. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України за станом на 05.10.2017 р. : офіц. вид. Верховна Рада України. Київ : Парлам. вид-во, 2017. 18 с.

8. Про державну таємницю : Закон України за станом на 12.07.2018 р. : офіц. вид. Верховна Рада України. Київ : Парлам. вид-во, 2018. 12 с.

9. Стратегія національної безпеки України "Україна у світі, що змінюється" : затв. Указом Президента України від 08.06.2012 р. № 389/2012. URL: http://zakon4.rada.gov.ua/laws/show/389/2012 (дата звернення: 26.01.2019).

10. Про затвердження Методичних рекомендацій щодо розрахунку рівня економічної безпеки України : наказ Міністерства економічного розвитку і торгівлі України № 1277 від 29.10.2013 р. URL: https://ips.ligazakon.net/document/ view/ME131588 (дата звернення: 26.01.2019).

11. Ліпкан В. А. Теорія національної безпеки : підручник. Київ : КНТ, 2009, с. 362–363.

References

1. Ukaz Prezydenta Ukrainy "Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 28 kvitnia 2014 roku "Pro zakhody shchodo vdoskonalennia formuvannia ta realizatsii derzhavnoi polityky u sferi informatsiinoi bezpeky Ukrainy" no. 449/2014 vid 01.05.2014. (2014). URL: https://zakon.rada.gov.ua/laws/show/449/2014.

2. Litvin, A. (2018). Shcho dast Ukraini novyi zakon pro kiberbezpeku. [What will give Ukraine a new law on cyber security]. URL: https://biz.censor.net.ua/m3069149 [in Ukrainian].

3. Pro informatsiiu: Zakon Ukrainy za stanom na 06.12.2016 r. (2016). *Ofits. vyd. Verkhovna Rada Ukrainy.* Kyiv: Parlam. vyd-vo.

4. Pro osnovy natsionalnoi bezpeky Ukrainy: Zakon Ukrainy za stanom na 07.11.2017 r. (2017). *Ofits. vyd. Verkhovna Rada Ukrainy*. Kyiv: Parlam. vyd-vo.

5. Pro zakhyst informatsii v informatsiino-telekomunikatsiinykh systemakh: Zakon Ukrainy za stanom na 27.03.2014 r. (2014). *Ofits. vyd. Verkhovna Rada Ukrainy.* Kyiv: Parlam. vyd-vo.

6. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy za stanom na 10.05.2018 r. (2018). *Ofits. vyd. Verkhovna Rada Ukrainy.* Kyiv: Parlam. vyd-vo.

7. Pro Derzhavnu sluzhbu spetsialnoho zviazku ta zakhystu informatsii Ukrainy: Zakon Ukrainy za stanom na 05.10.2017r. (2017). *Ofits. vyd. Verkhovna Rada Ukrainy*. Kyiv: Parlam. vyd-vo.

8. Pro derzhavnu taiemnytsiu: Zakon Ukrainy za stanom na 12.07.2018 r. (2018). *Ofits. vyd. Verkhovna Rada Ukrainy.* Kyiv: Parlam. vyd-vo.

9. Stratehiia natsionalnoi bezpeky Ukrainy "Ukraina u sviti, shcho zminiuietsia" : zatv. Ukazom Prezydenta Ukrainy vid 08.06.2012 r. No. 389/2012. (2012). URL: http://zakon4.rada.gov.ua/laws/show/389/2012.

10. Pro zatverdzhennia Metodychnykh rekomendatsii shchodo rozrakhunku rivnia ekonomichnoi bezpeky Ukrainy: Nakaz Ministerstva ekonomichnoho rozvytku i torhivli Ukrainy no. 1277 vid 29.10.2013 r. (2013). URL: https://ips.ligazakon.net/document/ view/ME131588.

11. Lipkan, V.A. (2009). Teoriia natsionalnoi bezpeky [The theory of national security']: pidruchnyk. Kyiv : KNT. [in Ukrainian].

Yakymchuk O. F., *Postgraduate Student, National University of Water and Environmental Engineering, Rivne*
ORCID 0000-0002-0960-8835

STATE MANAGEMENT OF KIBERSAFETY IN HYBRID WAR CONDITIONS

Information special operations, hacker attacks, combat use of social networks and Internet services – are a matter of today's life, which appeared on the agenda before the state authorities. In order to counteract these threats, leveling out the negative risks for civil rights and public security during cyberwar, the state must form an effective model of national security. This task is hypocritical in modern hybrid war conditions. The Question of formation of effective cyberspace in Ukraine has been needed to solve. The current normative and legal framework has not covered all the basic elements necessary for effective counteraction of cyber crimes of all levels of complexity. One of the important problems in this sphere was the terminology uncertainty. There was an overly arbitrary use of a large number of cybersecurity concepts (and their synonyms), often uncoordinated. In Particular, the Law of Ukraine "On the fundamentals of national security of Ukraine" mentions computer crime and computer terrorism, and none of these terms has not been defined in this, nor in other normative documents. Addressing these issues, organizing the work of the Head Centre for cyber security and structural subdivisions at the level of local authorities will provide an opportunity to put on the appropriate level of cyber defence issues and to ensure the confrontation between state and other Structures in the sphere of cyberspace. This will certainly provide an opportunity to carry out constant monitoring of cybernetic space, prompt notification of State authorities on detected threats, research of software and hardware means of cybernetic intelligence, protection and Influence (active counteraction) on the basis of cybernetic polygon, conducting scientific researches on information and cyber security issues, development of proposals and working out of cooperation with other institutions, special services and organizations, Development of theoretical principles of training specialists in the sphere of information and cyber security.

Key words: kibersafety, hybrid war, informatization, legislation.

Надійшла до редколегії 16.03.2019 р.