УДК 327.5:327.8:004
DOI 10.26693/ahpsxxi2021-2022.03.082

СТРАТЕГІЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В ГІБРИДНІЙ ВІЙНІ

Олеся Звездова,
e-mail: zvezdova-ir@ukr.net
ORCID: https://orcid.org/0000-0001-9664-5257
Чорноморський національний університет імені Петра Могили,
Україна, 54003, м.Миколаїв, вул.68 Десантників, 10

Олександр Вакалюк,
e-mail: ov.marine.ukr@gmail.com
ORCID: https://orcid.org/0000-0003-4712-6025
Чорноморський національний університет імені Петра Могили,
Україна, 54003, м. Миколаїв, вул.68 Десантників, 10

Стаття присвячена розгляду суті проблеми кібербезпеки виявлення загроз сьогодення, викликів та небезпеки високотехнологічної кіберзлочинності і кібертероризму у сучасних умовах гібридної війни. Висвітлюються пріоритети удосконалення кібербезпеки України на основі аналізу внутрішніх та зовнішніх чинників, європейських тенденцій та реакції в країнах світу на основні виклики в кіберпросторі. Розглянуті основні аспекти кібервійни та кібербезпеки. Було проаналізовано досвід США, Німеччини, Великобританії, Китаю та РФ у сфері боротьби із кіберзлочинністю.

Ключові слова: *кіберпростір, кібербезпека, інформаційна безпека, кібертероризм, кібервійна.*

Постановка проблеми. Одним з основних наслідків інформатизації, що виник у період формування сучасної інформаційної епохи, стало виникнення і швидкий розвиток нової сфери конфронтації між державами – конфронтації в кіберпросторі. Якщо на сьогодні між найбільш розвиненими у військовому та економічному відношенні державами до деякої міри склався стратегічний паритет у зброї масового знищення та звичайному озброєнні, то питання про паритет у кіберпросторі залишається відкритим. І, як наслідок, для будь-якої держави безпека в кіберпросторі (кібербезпека) стала найгострішою проблемою забезпечення національної безпеки.

Питання забезпечення кібербезпеки є вкрай важливими і для української держави на сучасному етапі, що, насамперед, обумовлено необхідністю протистояти протиправним посяганням на інформаційний простір України, збереження інформаційних ресурсів, захисту населення від негативного інформаційного впливу тощо. Окрім цього, стратегічно визнаним пріоритетом зовнішньої політики України є європейська інтеграція, що вимагає удосконалення нормативно-правової бази забезпечення інформаційної безпеки України, яке б відповідало не лише міжнародним стандартам, а передусім українським національним інтересам в інформаційній сфері.

Тому шляхи забезпечення захисту даних в інформаційно-обчислювальних та телекомунікаційних мережах, розробка стратегії комплексного аналізу стану національної телекомунікаційної мережі для забезпечення пропорційності та адекватності заходів кіберзахисту реальним і потенційним загрозам є на сьогодні надзвичайно актуальними.

Аналіз попередніх досліджень. На сьогодні наявні значні напрацювання в галузі інформаційної безпеки. Проблематикою походження поняття кібербезпеки, кіберпростору, «гібридної війни», національної безпеки, інформаційних атак у державних і недержавних структурах займалися такі провідні українські вчені, як В. Хорошко, Р. Грищук[1], А. Худавердова[2], В. Бурячок[3]. Відомий український політолог Є. Магда[4] акцентує увагу на феномені гібридної війни, яку Російська Федерація розпочала на Сході України. Автор визначає сутність гібридної війни, її характерні риси і складові. Серед західних дослідників слід виділити Дж. Ная[5], який розглядає кібербезпеку у межах своєї концепції м’якої сили.

Методи та прийоми дослідження. Дослідження ґрунтується на принципах наукової об’єктивності та достовірності. Автори використовували системний підхід для того, щоб розглядати проблему забезпечення кібербезпеки як невід’ємний елемент системи міжнародної безпеки. При аналізі документів і законодавчих актів різних держав у цій сфері у нагоді став метод контент-аналізу. Порівняльний метод надав можливість авторам виділити найбільш ефективні шляхи боротьби із кіберзлочинністю.

Викладення основного матеріалу. Протягом останньої чверті століття у світі відбувся глобальний сплеск розвитку інформаційних мереж, який можна вважати унікальним поєднанням комп’ютерів і комунікацій соціуму. Цивілізація вступила в еру інформаційного суспільства, в якому інформація стає вирішальним чинником у багатьох сферах життєдіяльності. Сьогодні практично неможливо знайти площину соціальної активності, яка б не зазнала впливу інформаційних технологій: політика, право, економіка, медицина, освіта, культура, релігія, сфера послуг і розваги. Потреба у засобах накопичення, систематизації, зберігання, пошуку, передачі інформації, забезпечення безпеки зростає.

На думку дослідників, наразі значну загрозу для всієї міжнародної спільноти становить саме кібертероризм. Це жахливе явище має два крила — кіберзлочинність та тероризм. Виходячи з цього проблема інформаційних загроз кіберпростору є наднаціональною. Свідченням цього є декларація, що була прийнята на саміті НАТО в Уельсі у 2014 р. (п.п. 72-73), згідно з якою «кібератаки можуть досягати такого рівня результатів, що загрожують євроатлантичному добробуту, безпеці і стабільності… Рішення про те, коли кібератаки потребують використати статтю 5, буде прийматися Північноатлантичною радою на індивідуальній основі»[6].

Гостроти проблематиці додає також те, що інформаційна складова є безумовним об’єктом маніпулювання в умовах гібридної війни, адже складна політична ситуація, в якій перебуває Україна останні шість років, постійне погіршання іміджу держави на міжнародній арені зумовлені низкою чинників, серед яких важливим фактором є неналежний стан системи інформаційної безпеки.

---

[1] Хорошко, В.О., Грищук, Р.В. (2016). Кібернетична зброя: класифікація, базові принципи побудови, методи та засоби застосування й захисту від неї. *Сучасна спеціальна техніка,* 4, 30-36.

[2] Худавердова, А.О. (2018). Кібербезпека як захист від інформаційної війни. *Інформаційна агресія Російської Федерації проти України,* 103-107.

[3] Бурячок, В. Л. (2015). Інформаційна та кібербезпека: соціотехнічний аспект: підручник. Київ: ДУТ.

[4] Магда, Є. В. (2014). Гібридна війна: сутність та структура феномену. *Міжнародні відносини. Політичні науки,* 4, 14-22.

[5] Nye, J. (2010). Cyber Power. *Center for Science and International Affairs*. Retrieved from: http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf

[6] Wales Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales on 05 Sep. 2014. *NATO*. Retrieved from: https://www.nato.int/cps/uk/natohq/official_texts_112964.htm

Дехто з фахівців навіть вважає, що в Україні фактично відсутня система інформаційної безпеки, яка б могла забезпечити виявлення, аналіз інформаційних загроз національній безпеці, а також протидію цим загрозам.

Розглянемо основні аспекти кібервійни та кібербезпеки. Кібервійна – це військові дії, що здійснюються в електронному просторі в електронному вигляді. Зброя в кібервійні – це інформація, інструменти – комп'ютери, театр військових дій – Інтернет. Мережа Інтернет стає потужною зброєю, яка суттєво підсилюється технологіями штучного інтелекту. Кіберзброя представляє собою широкий спектр технічних і програмних інструментів, які найчастіше спрямовані саме на використання вразливих місць у системах передачі даних[7]. Механізм дії кіберзброї може бути абсолютно різним. Наприклад, вірусні програми можуть заважати іншим програмам різними способами: відміняти команди або задавати свої, видаляти всі дані або змінювати їх. Однак у більшості випадків достатньо проникнути в чужу програму для того аби отримати необхідні дані. Інструментами кібератак є шкідливі програми і віруси, тому для того, щоб протистояти кібератакам, необхідно використовувати високоякісний захист і, безумовно, залучати компетентних фахівців.

Досліджуваний вид протистояння складається з двох етапів: шпіонажу та атак. Перший етап включає збір даних шляхом злому комп'ютерних систем інших держав. Атаки можуть бути розділені у відповідності з цілями і завданнями військових дій: вандалізм, пропаганда, збір інформації, порушення роботи комп'ютерного обладнання, атака інфраструктури і критичних об'єктів.

Завдання кібервійни полягає в досягненні певної мети в економічній, політичній, військовій та інших галузях. При цьому ставиться додаткове завдання щодо здійснення цілеспрямованого впливу на соціум і владу заздалегідь підготовленою інформацією. Тому кібервійна є ще й психологічною та одним із видів інформаційної війни в кібернетичному просторі. Адже комп'ютерні технології та Інтернет використовуються в усьому світі не лише в повсякденному житті людей, а й на підприємствах і державних установах. Маніпулювання даними, що отримуються із зазначених вище установ, створюють загрозу національній безпеці держави. Отже, кібербезпека є невід'ємною частиною захисту національної безпеки при даному протистоянні[8].

Мета кібервійни – порушення функціонування комп'ютерних систем, які відповідають за роботу ділових і фінансових центрів, державних установ, створення хаосу в житті держави. Тому перш за все страждають найбільш життєво важливі і функціональні системи. До них відносяться системи водо- і енергозабезпечення, транспорту, комунікаційні мережі тощо. Відзначимо, що найбільша кількість атак в Україні упродовж 2016-2017 рр. у критичній інфраструктурі прийшлася на енергетичний сектор та урядові установи.

Таким чином, у зв'язку з глобальним розповсюдженням інформаційних технологій у всі сфери нашого життя, аналогічна підривна діяльність, якщо вона успішна, може нанести збитки, які порівняльні з вибухом декількох атомних бомб. Це може деморалізувати й дезорганізувати противника, не застосовуючи при цьому звичайних озброєнь і жодного солдата.

Як засвідчили проведені дослідження, більшу частину кіберзлочинів здійснюють так звані хактевісти (37 %). Це хакери, що здійснюють атаки на сайти урядів держав, сервери великих компаній, використовуючи при цьому таємні бази даних. На думку

[7] Хорошко, В.О., Грищук, Р.В. (2016). Кібернетична зброя: класифікація, базові принципи побудови, методи та засоби застосування й захисту від неї. *Сучасна спеціальна техніка,* 4, 31.
[8] Указ Президента України №392/2020 Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України». Retrieved from: https://www.president.gov.ua/documents/3922020-35037

економістів, збитки світової економіки від такої діяльності кіберзлочинців становлять орієнтовно 114 млрд. доларів.

Забезпечення безпеки критичної інфраструктури (Critical Infrastrurture Protection, CIP) – це концепція готовності протистояти серйозним загрозам роботи важливих об’єктів інфраструктури та об’єктів підвищеної загрози в регіоні чи державі, особливо в умовах розповсюдження інформаційних технологій.

Історично першим кроком у цьому напрямі було створення в 1996 р. Комісії по захисту життєво важливої інфраструктури при Президенті США – було поставлене завдання розробити всеохоплюючу національну стратегію по захисту інфраструктури від фізичних і кібернетичних загроз. Подібна директива видана в ЄС у 2008 р. в Україні рішення Ради національної безпеки і оборони України від 27 січня 2016 р. «Про Стратегію кібербезпеки України» введено Указом Президента 15 березня 2016 року. Основні ж напрями державної політики по захисту критично важливих об’єктів інфраструктури прийняті Верховною Радою в Законі 5.10.2017 р. № 2997-VIII «Про основні засади забезпечення кібербезпеки України»[9]. Головною метою якого є сприяння безпеки об’єктів кібербезпеки та кіберзахисту. До таких об’єктів віднесено: комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси; об’єкти критичної інформаційної інфраструктури (перелік затверджується КМУ); комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу.

Відзначимо, що основна роль у забезпеченні кіберзахисту критичної інфраструктури належить телекомунікаціям – як у забезпеченні власної безпеки, так і всіх важливих об’єктів. На жаль, варто зазначити, що українські мережі зв’язку (глобальні, регіональні й локальні) побудовані в основному на базі іноземного обладнання (маршрутизатори, телекомунікаційні процесори, роутери, їх програмне забезпечення тощо).

Основними суб’єктами національної системи кібербезпеки є Державна служба спеціального зв’язку та захисту інформації, Національна поліція України, СБУ, Міністерство оборони України та Генеральний штаб ЗСУ, розвідувальні органи, Національний банк України, Державний комітет фінансового моніторингу України, ФАТФ (FATF)[10].

Розглянемо досвід США у сфері кібербезпеки. Загроза кібервійни привела до вражаючого факту: в США урядовий зв’язок відмовився від IP-телефонії. Поворотним моментом послужив теракт 11 вересня 2001 р. в Нью-Йорку, і як міра протиборства була сформована надпотужна структура – Міністерство внутрішньої безпеки, хоча боротьба з тероризмом розпочалася значно раніше. Було поставлено завдання розробити всеохоплюючу національну стратегію по захисту інфраструктури від фізичних і кіберзагроз. Спеціальна комісія із п’яти команд, що представляли 9 інфраструктур, виділила п’ять напрямів захисту: телекомунікації, ПЕОМ і програмне забезпечення, інтернет, супутники і оптоволокно; залізниці, повітряний і морський транспорт, трубопроводи; електроенергія, газ, нафта, виробництво, зберігання і транспортування; фінансові операції, фондові і ринки облігацій; вода, аварійні служби, державна служба.

У відповідності до вказаних напрямів був розроблений стандартизований опис критичної інфраструктури для полегшення контролю й підготовки до ліквідації надзвичайних ситуацій. Відпрацьована рамочна концепція, яка складається з п’яти функцій кіберзахисту: виявити – відпрацювати ризики й управління ними; захистити – розробити заходи по кіберзахисту об’єктів; виявити – впровадити відповідні заходи;

[9] Закон України «Про основні засади забезпечення кібербезпеки України» (2017). Retrieved from: https://zakon.rada.gov.ua/laws/show/2163-19#Text

[10] Худавердова, А.О. (2018). Кібербезпека як захист від інформаційної війни. *Інформаційна агресія Російської Федерації проти України,* 103.

відповісти – здійснити заходи кіберзахисту; відновити порушені функції і забезпечити стійкість роботи системи.

Ці 5 функцій складаються з 22 заходів та включають множину стандартів, методик, процедур і процесів, що детально описані й підлягають виконанню операторами критичної інфраструктури. Крім того, вони зобов'язані повідомляти про інциденти IT-безпеки. Невиконання приписів передбачає досить строгі покарання: до 20 років позбавлення волі – за розкрадання інтелектуальної власності американських компаній з використанням інформаційних технологій; до 30 років позбавлення волі без права дострокового звільнення – за проникнення в державні мережі, енергомережі, транспортні канали зв'язку або системи управління водоспоживанням; до 100 років позбавлення волі – за кіберзлочини[11].

Окрім того, Президент США Барак Обама в 2015 р. затвердив нову Стратегію національної безпеки держави і політику в інформаційній сфері, згідно якої військове керівництво США розглядає кіберпростір як одну зі сфер проведення військових операцій поряд із наземною, морською, повітряною і космічною операціями. В даному випадку потенційними противниками називають Росію, Китай, Північну Корею та Іран.

У Китаї, для прикладу, політика в кіберпросторі визначається з 2005 р. Стратегією розвитку інформатизації, яка просуває Інтернет у народне господарство з метою розвитку економіки. При цьому китайці застосовують обмежувальні заходи в кіберпросторі. Так, наприклад, користувачі не мають права реєструватися в соціальних мережах, використовуючи псевдонім. Окрім того, в рамках фільтрації інтернет-контенту «Вогняна стіна» в Китаї офіційно заборонені найбільша в світі соціальна мережа Facebook, відеохостингова компанія YouTube та соціальна мережа мікроблогів Twitter[12].

Великобританія прийняла Стратегію у сфері кібербезпеки в 2011 р. й реалізує інформаційну політику з метою виводу країни на перше місце по інноваціям, інвестиціям і якості сервісів у сфері IT-технологій[13].

У Німеччині відповідний документ по кібербезпеці був прийнятий у 2011 р. й передбачає створення внутрішньої системи звітності про інциденти IT-безпеки. Не виконання вимог про вказану звітність підлягає штрафу в розмірі 100 тис. євро, які можуть бути накладені на оператора критичної інфраструктури, який не зміг реалізувати вказані заходи IT- безпеки[14].

У Росії Доктрина інформаційної безпеки РФ була затверджена в 2016 р. До основних її положень належить стратегічне стримування і відвертання військових конфліктів, які можуть виникнути в результаті застосування інформаційних технологій. Росія відноситься до п'ятірки країн, що володіють потужними кібервійськами (в 2014 р. були створені війська інформаційних операцій РФ). До таких країн відносяться США, Китай, Росія, Велика Британія і Південна Корея[15].

Таким чином, розвиток інформаційних технологій обумовлює появу нових видів кібератак. Відповідно, однією з основних складових національної безпеки держави

[11] National cybersecurity strategy of the USA. President D.J. Trump, Washington (September 2018). Retrieved from: <https://d-russia.ru/wp-content/uploads/2019/01/National-Cyber-Strategy_USA_2018.pdf

[12] О современной политике Китая в киберпространстве (2021). *Отдел аналитики.* Retrieved from: https://d-russia.ru/o-sovremennoj-politike-kitaja-v-kiberprostranstve.html

[13] National strategy cyber security 2016-2021. Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643426/Russian_translation_-_National_Cyber_Security_Strategy_2016.pdf

[14] Кибербезопасность инфраструктуры Германии (2020). *Zarubezhnoe voennoe obozrenye,* 9. 10-16. Retrieved from: http://factmil.com/publ/strana/germanija/kiberbezopasnost_infrastruktury_germanii_2020/41-1-0-1789

[15] Указ Президента Российской Федерации об утверждении Доктрины информационной безопасности Российской Федерации (2016). Retrieved from: http://kremlin.ru/acts/bank/41460

стає забезпечення інформаційної безпеки. В Україні почалася активна робота в цьому напрямі. Для реалізації інформаційної безпеки необхідно застосовувати не лише інфраструктуру, стійку до кібератак (квантові комп’ютери можуть стати одним із компонентів вирішення цього завдання), водночас і забезпечувати цифровий суверенітет (розвивати українське програмне й апаратне забезпечення). Крім того, необхідно прискорити міжнародне співробітництво по напрямках протидії кібератакам з боку терористичних організацій і країн та застосування кіберзброї для боротьби з ними. Але на сучасному етапі найбільш перспективним напрямом вдосконалення інформаційної безпеки об’єктів управління і зв’язку та інформації в рамках існуючих технологій є багаторівневий багатопозиційний захист (ББЗ) з використанням апаратно-програмних засобів і способів захисту об’єктів та інформації.

Звичайно, що технічна основа ББЗ повинна базуватися на наступних основних принципах: 1) незалежно від фізичної природи потенційних загроз система захисту повинна протидіяти їх реалізації з певною (необхідною) мірою надійності; 2) в системі повинен здійснюватися моніторинг стану захищеності об’єкта захисту, основна функція якого своєчасне й достовірне виявлення небезпечних подій; 3) в системі повинна здійснюватися ідентифікація виявленої небезпечної події та прийняття заходів по її нейтралізації; 4) система в будь-якому випадку завжди реалізує умови припинення (нейтралізації) загрози; 5) система повинна забезпечувати припинення дій дестабілізуючих факторів із заданою мірою надійності.

У відповідності з розглянутими принципами ББЗ має містити наступні рівні: рівень безпосереднього захисту, що забезпечує відвертання фізичних чи логічних атак; рівень виявлення, що забезпечує своєчасне й достовірне виявлення небезпечної події і передачі інформації органу, який приймає рішення про її нейтралізацію; рівень збору й обробки інформації; рівень оперативного реагування системи захисту, що забезпечує створення своєчасних умов для нейтралізації небезпечної події; рівень нейтралізації небезпечної події.

Кожен із вказаних рівнів захисту може бути реалізований із використанням різних технічних і програмних засобів, які забезпечують високу логічну, технічну й оперативну стійкість роботи системи захисту. При цьому можливі наступні підходи для вирішення завдання ідентифікації. Перший заснований на використані додаткових спеціальних засобів, таких, як засоби відеоконтролю для систем фізичного захисту, вимірювальні прилади й апаратура для засобів захисту інформації від витоку та спеціальні програмні продукти для верифікації й ідентифікації комп’ютерних програм. Другий підхід базується на застосуванні шаблону ситуацій. Ці шаблони повинні містити параметри, які описують стан системи та об’єкта захисту, поведінку порушників, зовнішні фактори. Співпадіння ситуацій із заданим в одному із шаблонів вказує на наявність небезпечної події.

Далі здійснюється вироблення варіанта реагування на небезпечну подію. Його реалізація полягає в синтезі можливих варіантів, що задовольнять критерій виконання вимог до ефективності нейтралізації небезпечної події й процесів, які її реалізують. Завдання синтезу може формуватися як оптимізаційне. У цьому випадку відшукується єдине найкраще рішення.

На четвертому рівні здійснюється оперативне реагування на небезпечну подію з метою її нейтралізації (видалення). Реалізація процедур даного рівня залежить від організації управління захистом і від просторово-технологічних можливостей системи захисту по припиненню небезпечних подій. Заходи, які реалізуються на даному рівні, є обов’язковими лише для систем захисту інформації.

Останній п’ятий рівень захисту передбачає безпосередню нейтралізацію небезпечних подій. Складність заходів даного рівня полягає у вирішенні конфліктної

ситуації, яка вимагає використання спеціальних ресурсів. Завершує дану послідовність контроль результатів нейтралізації небезпечної події й оцінка по заданому критерію.

Основними складовими елементами інформаційної безпеки є як забезпечення якісного інформування громадян і вільного доступу до різних джерел інформації, так і захист від негативних інформаційних впливів, що у сукупності мають сприяти цілісності суспільства. Першочерговим завданням соціальних і державних інститутів має бути розробка термінових ефективних заходів щодо нейтралізації інформаційно-диверсійної діяльності РФ проти України та запобігання її подальшому розгортанню[16].

Вирішення цієї комплексної проблеми дозволить захистити інтереси суспільства і держави, сприяти реалізації права громадян на отримання всебічної та якісної інформації.

В умовах гібридної війни держава, що стала об'єктом агресії, неминуче наражається на широкий спектр інформаційних загроз, нейтралізація яких, з одного боку, вимагає вжиття надзвичайних правових і адміністративних заходів, а з іншого – може супроводжуватися істотним згортанням демократичних прав і свобод. Пошук балансу між інтересами національної безпеки й ідеями верховенства права – це стратегічно важливе завдання держави.

Мас-медіа є чи не найефективнішою зброєю, яка використовується в сучасних гібридних війнах. Зважаючи на це, державна політика в галузі інформаційного права має орієнтуватися на вибіркове застосування обмежень щодо конкретних ЗМІ, які зарекомендували себе недружніми, заангажованими та маніпулятивними. Такий підхід вимагає максимальної правової визначеності обмежувальних критеріїв, оскільки за їх відсутності існує ризик потрапляння під заборону незаангажованих і політично нейтральних мас-медіа (наприклад, у разі нецілеспрямованого поширення недостовірної інформації). Водночас широке коло громадських діячів та організацій наголошують, що встановлені заборони позбавлені фактичних підстав, не мають правового обґрунтування, суперечать Конституції, утискають демократичні права і свободи. Тому, будь-які обмеження в інформаційному середовищі повинні мати точковий характер і стосуватися лише тих ресурсів, які скомпрометували себе конкретними діями або є джерелом загроз для держави та суспільства.

В умовах проведення країною-агресором РФ деструктивного інформаційного впливу на цільову аудиторію України та інших держав світу можна визначити такі основні напрями вжиття заходів щодо захисту національного інформаційного простору і забезпечення національної системи інформаційної безпеки України: по-перше, удосконалити нормативно-правову базу у сфері інформаційної політики держави, яка б визначала взаємодію силових структур України з органами місцевого самоврядування, державними органами та громадськими інституціями; по-друге, створити єдиний міжвідомчий координаційний орган, який би здійснював керівництво, координацію та контроль заходів інформаційної безпеки, (його, наприклад, можна створити у вигляді міжвідомчої комісії при РНБО); по-третє, створити систему комплексного моніторингу популярних аудіовізуальних і друкованих ЗМІ, а також популярних Інтернет ресурсів; по-четверте, заохочувати подальші комплексні наукові дослідження у сфері інформаційної безпеки.

Отже, з наведеного вище можна зробити висновок, що кіберпростір має стати інструментом нашої асиметричної відповіді на агресію. Основними завданнями в цій сфері повинно стати: добиватися управління не лише своїми засобами, але й супротивником; створювати й удосконалювати інтелектуальний потенціал (де чільне місце займає підготовка кадрів), мислити по-новому; всі органи і системи управління

[16] Худавердова, А.О. (2018). Кібербезпека як захист від інформаційної війни. *Інформаційна агресія Російської Федерації проти України,* 107.

«тримати у формі» шляхом проведення впорядкованих тренувань з управління в кризових ситуаціях з охопленням усіх можливих варіантів розвитку подій; багаторівневий захист може використовуватися для вирішення завдань забезпечення інформаційної безпеки об’єктів різного призначення як для захисту самого об’єкта, так і для захисту інформації, яка в ньому циркулює.

Кібербезпека сьогодні набуває значення нової галузі в нашому ВПК і призначена забезпечити національну безпеку держави. Тому, своєчасне планування й реалізація заходів забезпечення кібербезпеки та інформаційного протиборства на глобальному й регіональному рівнях стає одним із пріоритетних завдань держави. Україна не просто може, а вимушена перестати концентруватися виключно на оборонних заходах. Маючи один із найкращих у світі людських потенціалів, фахівців з IT, здатність працювати швидко та ефективно, високу мотивацію до протистояння зовнішній агресії, держава повинна робити ставку не лише на оборонні технології, а й на наступальні, в тому числі кіберозброєння.

References

Buriachok, V.L. (2015). *Informatsiina ta kiberbezpeka: sotsiotekhnichnyi aspekt.* [Information and cybersecurity: socio-technical aspect]. Kyiv [in Ukrainian].

Khoroshko, V.O., Hryshchuk, R.V. (2016). Kibernetychna zbroia: Klasyfikatsiia, bazovi pryntsypy pobudovy, metody ta zasoby zastosuvannia i zakhystu vid nei [Cyber weapons: classification, basic principles of construction, methods and means of application and protection against it]. *Suchasna opertsiina tekhnika,* 4, 30-36. [in Ukrainian].

Khudaverdova, A.O. (2018). Kiberbezpeka yak zakhyst vid informatsiinoi viiny [Cybersecurity as protection against information warfare]. *Informatsiina ahresiia Rosiiskoi Federatsii proty Ukrainy,* 103-107. [in Ukrainian].

Kiberbezopasnost infrastrukturyi Germanii [Cybersecurity of Germany's infrastructure] (2020). *Zarubezhnoe voennoe obozrenye,* 9. 10-16. Retrieved from: http://factmil.com/publ/strana/germanija/kiberbezopasnost_infrastruktury_germanii_2020/41-1-0-1789 [in Russian].

Mahda, Ye.V. (2014). Hibrydna viina: sutnist ta struktura fenomenu [Hybrid war: the essence and structure of the phenomenon]. *Mizhnarodni vidnosyny. Politychni nauky,* 4, 14-22. [in Ukrainian].

National cybersecurity strategy of the USA. President D.J. Trump, Washington (September 2018). Retrieved from: https://d-russia.ru/wp-content/uploads/2019/01/National-Cyber-Strategy_USA_2018.pdf [in English].

National strategy cyber security 2016-2021. Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643426/Russian_translation_National_Cyber_Security_Strategy_2016.pdf [in English].

Nye, J. (2010). Cyber Power. *Center for Science and International Affairs*. Retrieved from: http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf [in English].

O sovremennoy politike Kitaya v kiberprostranstve [China's current cyberspace policy] (2021). *Otdel analitiki.* Retrieved from: https://d-russia.ru/o-sovremennoj-politike-kitaja-v-kiberprostranstve.html [in Russian].

Ukaz Prezydenta Ukrainy № 392/2020 Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 veresnia 2020 roku «Pro Stratehiiu natsionalnoi bezpeky Ukrainy» [Decree of the President of Ukraine №392 / 2020 On the decision of the National Security and Defense Council of Ukraine of September 14, 2020 «On the National Security Strategy of Ukraine»]. Retrieved from: https://www.president.gov.ua/documents/3922020-35037 [in Ukrainian].

Ukaz Prezidenta Rossiyskoy Federatsii Ob utverzhdenii Doktrinyi informatsionnoy bezopasnosti Rossiyskoy Federatsii [Decree of the President of the Russian Federation on Approval of the Doctrine of Information Security of the Russian Federation] (2016). Retrieved from: http://kremlin.ru/acts/bank/41460 [in Russian].

Wales Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales on 05 Sep. 2014. *NATO*. Retrieved from: https://www.nato.int/cps/uk/natohq/official_texts_112964.htm [in English].

Zakon Ukrainy Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy. [Law of Ukraine On Basic Principles of Cyber Security of Ukraine]. Retrieved from: https://zakon.rada.gov.ua/laws/show/2163-19#Text [in Ukrainian].

Olesia Zvezdova,
Petro Mohyla Black Sea National University, Mykolaiv, Ukraine
ORCID: https://orcid.org/0000-0001-9664-5257

Alexander Vakalyuk,
Petro Mohyla Black Sea National University, Mykolaiv, Ukraine
ORCID: https://orcid.org/0000-0003-4712-6025

Cyber security strategy in hybrid war

This article deals with the essence of today's cybersecurity problem by identifying threats, challenges and dangers of high-tech cybercrime and cyberterrorism in the current conditions of hybrid warfare and priorities of improving Ukraine's cybersecurity based on analysis of internal and external factors, European trends. The response to major challenges of different countries is considered.

The main aspects of cyber warfare and cybersecurity are underlined. The experience of the USA, Germany, Great Britain, China and Russia in the fight against cybercrime was analyzed. The main actors of the national cybersecurity system are the State Service for Special Communications and Information Protection, the National Police of Ukraine, the Security Service of Ukraine, the Ministry of Defense of Ukraine and the General Staff of the Armed Forces, intelligence agencies, the National Bank of Ukraine, the State Financial Monitoring Committee, and the FATF.

The author concludes that cyberspace should become a tool of our asymmetric response to aggression. The main tasks in this area should be: to manage not only our own means, but also the enemy`s ones; to create and improve intellectual potential (where training is paramount); to conduct orderly trainings on management in crisis situations with coverage of all possible variants of development of events for all bodies and systems of management. Multilevel protection can be used to solve the problems of information security of objects for various purposes, both to protect the object itself and to protect the information circulating in it.

Key words: *cyberspace, cybersecurity, information security, cyberterrorism, cyberwar.*