Медіафорум : аналітика, прогнози, інформаційний менеджмент : зб. наук. праць. – Чернівці : Чернівецький нац. ун-т, 2018. – Том 6. – С. 94-111

Mediarorum: Analytics, Forecasts, Information Management: Collection of Research Articles. – Chernivtsi: Chernivtsi National University, 2018. – Vol. 6. – pp. 94-111

УДК: 327.88:004.056.5

© *Яна Кибіч*[1]

ОСОБЛИВОСТІ ФОРМУВАННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

У статті проаналізовано проблему інформаційної безпеки України на сучасному етапі розвитку в умовах розгортання інформаційно суспільства. Розглянуто теоретичні підходи до визначення сутності поняття «кіберебезпека», «кіберпростір» вітчизняними та зарубіжними науковцями. Визначено, що ці поняття широко використовуються у сучасній науці, проте досі не існує чітко визначеного їх змісту, що, відповідно, ускладнює наукове осмислення та практичне подолання проблем і загроз в інформаційному просторі України та завдає шкоди національним інтересам держави. Охарактеризовано нормативно-правову базу України, що регулює сферу інформаційної безпеки, зокрема нормативно-правові акти, які були прийняті, починаючи із 2014 року. Доведено, що кібернетичні атаки на інформаційні ресурси держави стали невід'ємним компонентом гібридної війни, розв'язаною Росією. Вказано, що з початком російської військової агресії відбулася трансформація національного інформаційного законодавства в тому числі щодо кібербезпеки. Досліджено пріоритетні напрями державної політики у сфері забезпечення кібернетичної безпеки України в умовах гібридної війни.

Ключові слова: *інформаційна безпека України, інформаційні загрози, державна інформаційна політика, кіберпростір; кібербезпека, кіберзагроза, гібридна війна, захист інформаційного простору.*

Peculiarities of the cybersecurity of Ukraine formation in the conditions of hybrid war

In the article, the problem of information security of Ukraine at the present stage of development in the context of the information society evolution was analysed. The theoretical approaches to the definition of the essence of

[1] Здобувач кафедри міжнародної інформації Чернівецького національного університету імені Юрія Федьковича, Україна, E-mail: yana.nanana2702@gmail.com

the concept of "cybersecurity", "cyberspace" by Ukrainian and foreign scientists were discovered. It is determined that these concepts are widely used in modern science, but there is still no their clearly defined meaning, which, accordingly, complicates scientific comprehension and practical overcoming of problems and threats in the information space of Ukraine and harms the national interests of the state.

The legal framework of Ukraine, which regulates the sphere of information security, in particular, legal acts adopted since 2014, were described. It has been proved, that cybernetic attacks on state information resources have become an integral part of the hybrid war, unleashed by Russia. It is indicated that with the onset of Russian military aggression, the transformation of national information legislation, including the one on cybersecurity, took place. The priority directions of the state policy in the field of ensuring the cybernetic security of Ukraine in the conditions of hybrid war were researched.

Keywords: *information security of Ukraine, information threats, state information policy, cyberspace; cybersecurity, cyber threat, hybrid war, protection of the information space.*

Постановка наукової проблеми та її значення. Необхідність розбудови ефективної системи кібернетичної безпеки, як однієї із основних складових національної інформаційної безпеки в Україні нагадала про себе після захоплення Росією АРК і включення її до складу РФ (з 27 лютого до кінця березня 2014 року – перша фаза гібридної війни), вторгнення російських загонів на території українського Донбасу, серії проросійських виступів в Україні і проголошення «державних суверенітетів» ДНР та ЛНР та початку бойових дій (квітень–липень 2014 року). Гібридна війна, розгорнута Росією проти незалежної України, поряд з класичними воєнними діями та інформаційно-психологічними операціями, включає в себе й проведення кібернетичних операцій. В розпорядженні Кремля працює ціла армія хакерів для проведення атак у кібернетичному просторі.

В умовах сучасного гібридного протистояння України та РФ, поширення інформаційної експансії та агресії, захист національного інформаційного простору нашої держави та гарантування інформаційної безпеки є пріоритетними стратегічними завданнями української влади. Україні необхідно шукати шляхи та створювати дієві механізми забезпечення захисту національних інтересів України в національному та глобальному кіберпросторах від сучасних загроз.

Аналіз останніх досліджень і публікацій. Дослідження питань національної інформаційної безпеки та кібербезпеки як складової інформаційного захисту держави в сучасних умовах є актуальним для багатьох зарубіжних науковців: Дж. Най, С. Морган, М. Шмідт, А. Клімбург, М. Гедекер, М. Лібіцкі, І. Зубарєв, М. Безкоровайний. Слід зазначити, що з початком російської збройної агресії неабиякий інтерес до даної проблематики стали проявляти й українські вчені, зокрема М. Ожеван, Д. Дубов, В. Бурячок, В. Фурашев, В. Бутузов, В. Толубко, О. Довгань, В. Хорошко, С. Толюпа, М. Погорецький, К. Титуніна та інші науковці.

Проте, незважаючи на досить велику кількість досліджень та публікацій на тему інформаційної та кібербезпеки їх аналіз свідчить, що дослідниками розглянуті лише загальні питання розбудови національної системи кібернетичної безпеки як невід'ємного елементу системи інформаційної безпеки.

Водночас, розкриття проблем побудови національної кібернетичної системи дозволить правильно визначити пріоритети такої побудови та дасть змогу захистити вразливий вітчизняний інформаційний простір.

Метою даного дослідження є дослідження сучасного стану та проблем побудови кібернетичної безпеки України як складової національної інформаційної безпеки в умовах гібридної агресії Російської Федерації.

Виклад основного матеріалу. У даний час відносно нове поняття безпеки в кібернетичному просторі або кібернетичної безпеки все більше актуалізується та розглядається як стратегічна проблема держави. Усвідомлюючи сучасний стан та актуальність проблеми забезпечення кібернетичної безпеки, більшість країн світу акумулюють свої зусилля та проводять комплексні заходи щодо безпеки в кібернетичному просторі. Насамперед вони пов'язані з розробкою та вдосконаленням нормативно-правової бази, що регулює питання у сфері кібербезпеки. Відповідно створюються відомчі та державні структури, які несуть відповідальність за забезпечення кібернетичної безпеки.

Проблема дослідження кіберпростору та аналіз стану кібернетичної безпеки характеризується низкою невизначеностей в самій термінологічній основі та в нормативно-правовій сфері. Для подальшого здійснення досліджень у напрямку взаємозв`язку понять «інформа-

ційна безпека» та «кібернетична безпека» необхідно чітко сформувати суть понять «кібербезпека» та «інформаційний простір». А це, у свою чергу, можливо зробити лише у тому випадку, коли буде чітко сформульвано сутність поняття «кіберпростір».

Термін «кіберпростір» було введено у вжиток канадським письменником-фантастом американського походження Вільямом Гібсоном у 1982 р. у новелі «Палаючий Хром» («Burning Chrome»). У 1984 році це поняття було більш детально розкрито у творі «Нейромант» («Neuromancer»). На думку Гібсона, кіберпростір (cyberspace) – це злагоджена галюцинація, яку щодня зазнають мільярди звичайних операторів у всьому світі. Це логічне представлення відомостей, збережених у пам'яті та на магнітних носіях комп'ютерів всього розумного людства. Потоки даних, що протікають у просторі розуму; скупчення та сузір'я інформації (Gibson, 1994).

Уперше термін «кіберпростір» було використано в Окінавській хартії глобального інформаційного суспільства(Окінавська Хартія глобального інформаційного суспільства, 2000) та в Конвенції про злочинність у сфері комп'ютерної інформації від 23 листопада 2001 р. (Конвенція Ради Європи, 2001). Сфера його дії на той час перебувала під впливом загальних механізмів правового регулювання суспільних відносин, обмежуючись специфічними об'єктами й інтересами суб'єктів правовідносин, а також комп'ютерними мережами, за допомогою яких можна брати участь у відповідних правовідносинах.

У науковій літературі можна знайти чимало тлумачень поняття «кіберпростору». При цьому різновекторне розуміння даного поняття властиве і нормативно-правовій сфері: практично кожна країна в своєму законодавстві дає власне визначення. Наприклад: 1) відповідно до міжнародного стандарту(ISO/IEC 27032, 2012), кіберпростір – це середовище існування, що виникло в результаті взаємодії людей, програмного забезпечення і послуг в інтернеті за допомогою технологічних пристроїв і мереж, під'єднаних до них, якого не існує в будь-якій фізичній формі; 2) згідно з нормативною базою США (National Military Strategy, 2005), кіберпростір – це сфера, що характеризується можливістю використання електронних та електромагнітних засобів для запам'ятовування, модифікування та обміну даними через мережні системи та пов'язану з ними фізичну інфраструктуру; 3) відповідно до офіційних докумен тів Євросоюзу (European Commission, Glossary and Acronyms), кіберп ростір – це віртуальний

простір, в якому циркулюють електронні дані світових персональних комп'ютерів (ПК); 4) за версією офіційних документів Великобританії (Cyber Security Strategy, 2009), кіберпростір – це всі форми мережної, цифрової активності, що включають у себе контент та дії, здійснювані через цифрові мережі; 5) згідно з офіційними документами Німеччини (German Cyber Security Strategy, 2011), кіберпростір – це вся інформаційна інфраструктура, доступна через інтернет поза будь-якими територіальними кордонами.

Вітчизняні науковці також трактують поняття кіберпростору. Для прикладу, С. Мельник визначає кіберпростір як простір, сформований інформаційно-комунікаційними системами, в якому проходять процеси перетворення (створення, зберігання, обміну, обробки та знищення) інформації, представленої у вигляді електронних комп'ютерних даних (Мельник, 2011).

Д. Дубов дає таке визначення кіберпростору – це об'єкти інформаційної інфраструктури, що керуються інформаційними (автоматизованими) системами управління та інформації, що в них циркулює (Дубов та Ожеван, 2011, 12). С. Гнатюк вважає, що кіберпростір – це віртуальний простір, отриманий у результаті взаємодії користувачів, програмного та апаратного забезпечення, мережевих технологій (у т.ч. Інтернет) для підтримки та управління процесами перетворення інформації (електронних інформаційних ресурсів) з метою забезпечення інформаційних потреб суспільства (Гнатюк, 2013).

Загалом, більшість дефініцій зводяться до розуміння кібербезпеки як стану захищеності кіберпростору держави в цілому або окремих об'єктів її інфраструктури від зовнішніх впливів та ризиків, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання й нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним і/або національним інтересам (Бурячок, Толубко, Хорошко та Толюпа, 2015, 15).

Багато дослідників концентрують свою увагу на важливості кібермогутності держави як здатності забезпечувати та захищати національні інтереси в кіберпросторі. До розуміння суті цього поняття варто застосовувати комплексний підхід, оскільки, воно включає в себе важливі аспекти політологічної, військової, юридичної, телекомунікаційної та інших сфер і потребує подальшої розробки та вдосконалення.

З огляду на триваючу гібридну війну між РФ та Україною питання кібербезпеки держави набуває особливого значення.

Як відомо, гібридна агресія Росії проти України переросла в активну фазу на початку 2014 року, однак задовго до прямого воєнного втручання супроводжувалася тактичною інформаційною підтримкою, яка містила широкий спектр інформаційно-психологічних впливів на населення України та Росії, фактично починаючи після проголошення Україною незалежності у 1991 році. Такої думки дотримується більшість (51,4%) з 37 українських експертів, які взяли участь в опитуванні, що здійснювалось у період з 18 по 28 серпня 2017 року Центром глобалістики «Стратегія XXI» за підтримки ЄС і Міжнародного фонду «Відродження» (Сприяння розбудові, 2018). Оцінки українських експертів також свідчать про те, що Росія завжди працювала над ослабленням України, і ця діяльність особливо активізувалась з приходом до влади В.Путіна.

Основним напрямком ведення війни гібридного характеру Російської Федерації проти України є інформаційна сфера, однак, російський вплив здійснюється також на культурно-гуманітарну, військову, фінансово-економічну сфери, кібер-простір, енергетичну та дипломатичну сфери. Це доводить, що гібридна війна Росії проти України спрямована на невійськові сфери, а першочерговим напрямком є інформаційно-пропагандистський, де кіберагресія є ключовою складовою.

Український вчений Д. Дубов вважає, що усі кіберзагрози, які на сьогоднішній день, у тій чи іншій мірі використовуються для здійснення негативного впливу на кіберпростір України, можна поділити на дві умовні групи. До першої належать так звані «класичні» кіберзлочини – як абсолютно оригінальні, так і вже звичні для нас, для своєї реалізації вони потребують лише сучасних інформаційних технологій. Друга група об'єднує злочини, характерні для геополітичної боротьби (або такі злочини на місцевому рівні, які мають потенціал вплинути на політичне становище держави): хактивізм (використання комп'ютерних систем, соціальних мереж для просування певних політичних ідей, лозунгів, гасел тощо) кібершпигунство та кібердиверсії. Водночас техніки здійснення атак в обох випадках демонструють чимало спільного. Наприклад, фішингові техніки можуть бути використані як для заволодінням коштами громадян, так і з кібершпигунською метою. Хоча, звичайно, ціла низка кіберзлочинів має на

меті й може скоюватися виключно для збагачення злочинців (Дубов, 2014, 210).

Якщо говорити про кіберзагрози, віднесені до групи геополітичних чи міждержавних, механізмів боротьби (хактивізм, кібершпигунство та кібердиверсії), то у цілому можна констатувати, що наша держава вже активно залучається у протистояння хактивістів, в окремих випадках стає об'єктом кібершпигунських акцій (Дубов, 2014, 210).

Кібератаки з боку Кремля вже неодноразово вражали сайти органів державної влади України, українських компаній та бізнесу. Перші серйозні напади були здійснені під час проведення виборів президента України. 27 травня 2014 р. служба безпеки України (СБУ) встановила, що більшість хакерських атак, які здійснювалися проти сервера ЦВК у день виборів президента, організовували з території Росії. За інформацією прес-служби СБУ, атаки на сервер ЦВК здійснювались безперервно зі змінною динамікою потужності, а переважна кількість атак проводилася з території Російської Федерації з використанням бот-мереж (Головка, 2016, 334).

Авторитетне українське видання «Новое Время» (П'ять найвідоміших хакерських угруповань, 2017) опублікувало список п'яти найвідоміших хакерських угруповань, які здійснюють диверсії в інформаційному просторі України. Серед них 1) Anonymous Ukraine, найбільш відомі атаки групи – злом електронної пошти МЗС України в жовтні 2013 року, а також публікація листування і особистих даних Віталія Кличка в листопаді того ж року. Кібератаки групи на сайти країн Балтії під час навчань НАТО в листопаді 2013 року були проведені з російських IP-адрес; 2) APT28 впровадила вірус Snake/ Uroborus/Turla для отримання повного доступу до інформації, що зберігається на атакованих серверах держструктур, ЗМІ та фінансових компаній в 2013-2014 роках. Ця ж група намагалася викрасти дані про розслідування катастрофи рейса MH17; 3) APT29 (інші назви – Cozy Bear, The Dukes, Office Monkeys) Угруповання здатне здійснювати технічно складні і тривалі атаки, що свідчить про фінансування на рівні держави. В 2013 році вірус The Duke приходив в Україну під виглядом фальшивих pdf-документів, що імітують офіційні папери на актуальні теми політичного контексту; 4) SendWarm (діє також під назвою Electrum). Воно має відношення до розробки шкідливого ПО Crash Override, націленого на атаку енергосистем різних країн. Саме

SandWarm розробила вірус SendEnergy3, який атакував Прикарпаттяобленерго, Київобленерго і Чернівціобленерго в 2015-му. Аналогічній атаці в грудні 2016- го піддалася підстанція Північна в Києві; 5) CyberBerkut, основні кібератаки групи – створення перешкод у роботі українського ЦВК під час президентських виборів, DDoS-атаки на сайти МВС, Генпрокуратури і президента України. CyberBerkut взяв на себе відповідальність за публікацію розмови між міністрами закордонних справ Естонії та ЄС з коментарями, що дискредитують дії української опозиції на Майдані (Кобра та Верестюк, 2018).

Масштабні хакерські атаки проти України регулярно здійснюються з 2014 року. 4 лютого 2014 року анонімні хакери з угрупування CyberBerkut завантажили в YouTube телефонну розмову помічни ка держсекретаря США Вікторії Нуланд з послом США в Україні Джеффрі Пайєттом, в якій вона нецензурно відгукнулася про роль ЄС у врегулюванні української кризи (Меркель обурена, 2014). У березні 2014 року на початку окупації Криму російські спецслужби за допомогою IPтелефонної атаки блокували зв'язок між українськими нардепами і підрозділами СБУ в Криму. У червні 2014 року на серверах приватних компаній України і країн НАТО були виявлені шкідливі програми, які займалися шпигунством. Серед них такі як Turla/ Uroburos/ Snake, RedOctober, MiniDuke і NetTraveler (Найбільші кібератаки, 2017). Аналіз показав, що програми були розроблені в Росії. З 2014 року радіолокаційна розвідка терористів, які воюють на Донбасі, зламуючи бази даних про місцезнаходження телефонів і мереж Wi-Fi, отримувала дані про позиції українських Збройних сил. 23 грудня 2015 року за допомогою троянської програми BlackEnergy3, у використанні якої були раніше помічені російські хакери, було відключено близько 30 підстанцій Прикарпаттяобленерго, в зв'язку з чим більш 200 тисяч жителів Івано-Франківської області залишалися без електроенергії (Найбільші кібератаки, 2017). 6 грудня 2016 року відбулася хакерська атака на внутрішні телекомунікаційні мережі Мінфіну, Держказначейства, Пенсійного фонду, яка вивела з ладу ряд комп'ютерів, а також знищила критично важливі бази даних, що призвело до затримки бюджетних виплат на сотні мільйонів гривень. 15 грудня 2016 року українські хакери на замовлення невстановленої особи з Санкт-Петербурга здійснили DDOS-атаку на сайт Укрзалізниці, внаслідок чого протягом дня була повністю заблокована його робота. 27 червня 2017 року відбулася масштабна хакерська атака

за допомогою вірусної програми Petya.A, яка порушила роботу численних українських державних і приватних підприємств, зокрема аеропорту Бориспіль, Укртелекому, ЧАЕС, Укрзалізниці та інших, а також Кабінету міністрів і ряду ЗМІ. СБУ заявила про причетність до атаки російських спецслужб. «Атака, що отримала назву «NotPetya», швидко поширилася по всьому світу, завдаючи збитків у мільярди доларів у Європі, Азії та Америці. Це було частиною постійних зусиль Кремля, спрямованих на дестабілізацію України, і дедалі активніше демонструє участь Росії в поточному конфлікті. Це було також безрозсудною та невибірковою кібератакою, яка матиме міжнародні наслідки», – йдеться в заяві Білого дому 15 лютого (Statement, 2018).

Наведені приклади доводять недостатню ефективність сучасної системи кібербезпеки України і про нагальну потребу її удосконалення та модернізації.

Варто зазначити, що в Україні також існують хакерські об'єднання, головною метою діяльності яких є протидія російській кіберагресії. Серед них «Український кіберальянс» – об'єднання хакерів та кібер-активістів на основі «FalconsFlame», «Trinity», «RUH8» та «Кіберхунти»(Дрогомирецький, 2018). Відомі за зламом електронних скриньок російських активістів і ватажків терористів; кібератаками на пропагандистські ЗМІ («Анна Ньюз», «Перший Канал»), міністерства РФ та так звані «ДНР» і «ЛНР»; публікаціями електронного листування терористів та російських високопосадовців. «Українські кібервійська» – ініціатива, створена Євгеном Докуніним. Головною метою є проведення оборонних та наступальних операцій в Інтернеті, протидія сепаратизму, тероризму та інформаційній війні проти України. Відомі блокуванням мобільного зв'язку та близько 450-ти банківських рахунків терористів; хакерськими атаками на близько 150 вебресурсів та віддаленим захопленням веб-камер терористів у Криму. «ІнформНапалм» (Офіційна сторінка «ІнформНапалм», 2018) (англ. InformNapalm) – проводили незалежне розслідування катастрофи малайзійського Боїнга; мають базу даних російських підрозділів, які воюють в Україні. Основний метод діяльності базується на принципі Open source intelligence – зборі інформації з відкритих джерел, соціальних мереж. Сайт «Миротворець» – широко відомий завдяки ЗМІ через бази даних осіб, задіяних у сепаратизмі, незаконному відвідуванні тимчасово окупованого Криму, підтримці агресивної політики Кремля. Відзначилися розробкою автоматизованої системи аналізу

та розпізнавання облич Identigraf, що покликана обробляти масивні бази даних та виявляти порушників.

Реакцією української влади на кібератаки було утворення Департаменту кіберполіції Національної поліції України, який відповідно до законодавства України забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю, організовує та здійснює відповідно до законодавства оперативно-розшукову діяльність (Постанова КМУ, 2015).

У відповідь на політичну ситуацію, що склалась у кінці 2014 р. – на початку 2015 р. Президент України Петро Порошенко підписав указ «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України». Цим указом вводиться в дію розроблена спеціалістами з кібербезпеки та затверджена на засіданні РНБОУ Стратегія кібербезпеки України. Цей документ базується на положеннях Конвенції про кіберзлочинність, ратифікованої Законом України від 7 вересня 2005 року № 2824-IV, затверджений і набрав чинності 15 березня 2016 року. Метою створення стратегії було забезпечення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства та держави. Одним з перших кроків з втілення Стратегії, стало створення в червні 2016 року Національного координаційного центру кібербезпеки як робочого органу Ради національної безпеки і оборони України.

До того ж на державному рівні Україна вживає такі заходи: створення Команди реагування на комп'ютерні надзвичайні події – CERT-UA (англ. Computer Emergency Response Team of Ukraine) – спеціалізований структурний підрозділ Державного центру кіберзахисту та протидії кіберзагрозам Державної служби спеціального зв'язку та захисту інформації України, заснований у 2007 році. Діяльність CERT-UA передбачена Законом України «Про Державну службу спеціального зв'язку та захисту інформації», Законом України «Про телекомунікації», Законом України «Про основні засади забезпечення кібербезпеки України» та підзаконними актами. Відповідно до рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України», уведеного в дію Указом Президента України від 15 березня 2016 року № 96 утворено Національний координаційний центр кібербезпеки, що є робочим органом РНБО України (Президент України; Указ, 2016).

Однозначно позитивним зрушенням у формуванні державної політики в інформаційній сфері стала Доктрина інформаційної безпеки, що була введена в дію Указом Президента України від 25 лютого 2017 року № 47/2017. Метою Доктрини є уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни (Верховна Рада України. «Закон України, 2017). Головним недоліком Доктрини є те, що вона не є документом прямої дії і відповідно не може застосовуватися як інструмент правового регулювання.

7 листопада 2017 року Президент України підписав закон України «Про основні засади здійснення кібербезпеки України» (Закон 2163 – VIII набрав чинності 9 травня 2018 року). Закон виконує роль центрального акта в структурі законодавства стосовно кібербезпеки і спрямований на формування загальної державної політики кібербезпеки. Крім цього, ним передбачається розподіл ролей та функцій суб'єктів національної системи кібербезпеки, а також порядок їх взаємодії у цій сфері. Зокрема, він надає повноваження спецслужбам для здійснення кібернетичного захисту України. Згідно із нормами закону координацією дій у сфері кібербезпеки буде займатися президент України через РНБО. На Кабінет Міністрів України покладається затвердження нормативно-правових актів з аудиту інформаційної безпеки, порядку функціонування Національної телекомунікаційної мережі, критеріїв та порядку віднесення об'єктів до об'єктів критичної інфраструктури, переліку таких об'єктів та загальних вимог до їх кіберзахисту. Цим законом також передбачається створення Національної системи кібербезпеки, до якої увійдуть: Державна служба спеціального зв'язку та захисту інформації, Нацполіція, СБУ, Міністерство оборони і Генеральний штаб, Національний банк та інші органи (Кібербезпека в Україні, 2017). Головною перевагою є те, що закон нарешті вводить у правову площину поняття «кібератака», «кібербезпека», «кіберзахист», «кіберзлочин» тощо.

Як бачимо, офіційні документи вже існують, але їх замало, як і недостатньо конкретних кроків уряду України у вирішенні питань, пов'язаних з кібербезпекою. Вітчизняні реалії у кібербезпековій сфері свідчать про низку серйозних проблем, які заважають створенню ефективно діючої системи протидії загрозам в кіберпросторі. В першу чергу до таких проблем відносяться: термінологічна невизначе-

ність, відсутність належної координації діяльності відповідних відомств, залежність України від програмних та технічних продуктів іноземного виробництва, складнощі із кадровим наповненням відповідних структурних підрозділів.

Для успішного опору агресору та активної оборони від агресії гібридного типу експерти Центру глобалістики «Стратегія XXI» (Сприяння розбудові, 2018) визначили потреби у наступних діях: політичну волю до викорінення корупції та олігархічно-орієнтованої системи влади; викорінення російської агентури з державної системи; чітку ідентифікацію конфлікту з Росією відповідно до політичних реалій; покращення бізнесклімату в державі; реформування і професіоналізація Збройних Сил України; переформатування СБУ; посилення кібербезпеки і завдання кіберударів агресору; жорстка протидія агресору в інформаційній сфері; створення ефективної територіальної оборони; створення інтегрованої системи раннього попередження і відповіді на конфлікти; вступ України до НАТО; зменшення культурно-релігійних впливів з боку РФ; економічне зростання України; поєднання зусиль уряду і громадянського суспільства; підвищення свідомості, самоідентифікації та консолідації всього українського суспільства.

Висновки. Починаючи з 2014 року виклики українського безпекового середовища певною мірою знаходять своє відображення в кібернетичному просторі. Виникає потреба в якісному дослідженні явища кібертероризму з метою побудови комплексного механізму протидії, який в першу чергу має виконувати запобіжну функцію. Незважаючи на низький рівень стартової готовності до спротиву агресії, зокрема в інформаційній сфері, Україна досягла значних успіхів, про що свідчать наведені у статті дані. Втім, досягнуті позитивні трансформації не можуть гарантувати надійну захищеність національних інтересів України від майбутніх проявів російської інформаційної агресії, адже російська сторона має значну перевагу в засобах ведення інформаційної війни та постійно адаптує нові інструменти і технології підривної діяльності. Рівень кіберзахисту критичної інфраструктури держави на сьогоднішній день залишається недостатнім, що продемонстрували численні вдалі кібератаки на систему органів державної влади, енергетичного, економічного, інформаційного комплексу, ЗМІ та інші інфраструктури. Потрібно якнайшвидше систематизувати та оптимізувати основні напрями діяльності правоохоронних органів

із протидії використанню кіберпростору з терористичною метою, а також розширити застосування новітніх інформаційних технологій в інтересах антитерористичної діяльності.

Варто також розвивати та впроваджувати ефективну нормативно-правову базу, в якій в першу чергу були би чітко визначені поняття «кіберпростір», «кіберзагрози», «кібербезпека», утворити загальнодержавну систему забезпечення кібербезпеки та законодавчо закріпити права і обов'язки її суб'єктів, відшліфувати механізм координації та взаємодії між ними. Підкреслимо, що дії органів влади та побудова законодавства у цій сфері в Україні відбувається за принципом надолуження згаяного. Натомість необхідно стратегічно планувати та діяти наввипередки, щоб створити потужний механізм стримування зовнішньої кіберагресії з якої сторони вона не відбувалася.

Джерела та література:

1. Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space http://webarchive.nationalarchives.gov.uk/+/http:/www.cabinetoffice.gov.uk/media/216620/css0906.pdf (accessed June 15, 2018).

2. German Cyber Security Strategy, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/cybersecurity-strategy-for-germany/view (accessed June 16, 2018).

3. Gibson, W. 1994. Neuromancer. London: HarperCollins.

4. Glossary and Acronyms (Archived) / European Commission, https://ec.europa.eu/digital-single-market/#c (accessed June 15, 2018).

5. ISO/IEC 27032, «Information technology — Security techniques — Guidelines for cybersecurity», (2012) https://www.iso.org/standard/44375.html (accessed June 2018).

6. National Military Strategy for Cyberspace Operations, https://www.hsdl.org/?view&did=35693 (accessed June 16, 2018).

7. Statement from the Press Secretary». 2018. https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/?utm_source=link (accessed June 16, 2018).

8. Бурячок, В.Л., Толубко, В.Б., Хорошко, В.О., Толюпа, С.В. 2015. Інформаційна та кібербезпека: соціотехнічний аспект: підручник, Київ ДУТ, 2015: 15.

9. Верховна Рада України. «Закон України Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII

http://zakon5.rada.gov.ua/laws/show/2163-19 (accessed June 16, 2018).

10. Верховна Рада України. «Про Державну службу спеціального зв'язку та захисту інформації України

11. Верховна Рада України. «Про телекомунікації. Закон від 18.11.2003 № 1280-IV» http://zakon4.rada.gov.ua/laws/show/1280-15/ (accessed June 17, 2018).

12. Гнатюк, С.О. 2013. «Базові дефініції у галузі кібернетичної безпеки держави», 2013, Вісник Інженерної академії України, http://nbuv.gov.ua/UJRN/Viau_2013_3-4_11 (accessed June 17, 2018).

13. Головка, А.А. 2016. «Захист кіберпростору як складова інформаційної безпеки України в умовах гібридної війни», Молодий вчений, № 4, (2016): 334.

14. Дрогомирецький, Б. 2018. «Україно-російська кібервійна: невидимий фронт». https://www.pravda.com.ua/columns/2018/02/22/7172439/ (accessed June 15, 2018).

15. Дубов, Д.В. 2014. Кіберпростір як новий вимір геополітичного суперництва: монографія. Київ, НІСД, 2014: 210.

16. Дубов, Д.В., Ожеван, М.А. 2011. Кібербезпека: світові тенденції та виклики для України. Київ, НІСД, 2011: 12.

17. Сприяння розбудові можливостей України гарантувати безпеку суспільства в умовах гібридних загроз. Результати експертного опитування http://prismua.org/wp-content/uploads/2018/02/blok_XXIend_3001.pdf (accessed June 19, 2018).

18. Закон від 23.02.2006 № 3475-IV http://zakon4.rada.gov.ua/laws/show/3475-15 (accessed June 21, 2018).

19. Кібербезпека в Україні: перезавантаження? https://ckp.in.ua/events/19139 (accessed June 2018).

20. Кобра, Г., Верестюк, І. 2018. «Пов'язані з Росією хакери перетворили Україну на полігон для випробування кіберзброї, яку в подальшому Кремль готовий використовувати проти куди більш грізних опонентів — США і ЄС» https://magazine.nv.ua/ukr/journal/2558-journal-no-24/virus-vova.html (accessed June 19, 2018).

21. Конвенція Ради Європи про кіберзлочинність: від 23 листопада 2001 року, http://zakon2.rada.gov.ua/laws/show/994_575 (accessed June 20, 2018).

22. Мельник, С.В. 22 березня 2011. «До проблеми формування понятійно-термінологічного апарату кібербезпеки», Актуальні

проблеми управління інформаційною безпекою держави: зб. матер. наук.-практ. конф., (Київ, Вид-во НА СБ України, 2011).

23. Меркель обурена словами Нуланд про роль ЄС в українській кризі. Українська правда, 07.02.2014 https://www.pravda.com.ua/news/2014/02/7/7013123/ (accessed June 20, 2018).

24. Найбільші кібератаки проти України з 2014 року. Інфографіка. Новое Время https://nv.ua/ukr/ukraine/events/najbilshi-kiberataki proti-ukrajini-z-2014-roku-infografika-1438924.html (accessed June 17, 2018).

25. Окінавська Хартія глобального інформаційного суспільства, http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=998_163 (accessed June 19, 2018).

26. Офіційна сторінка «ІнформНапалм». 2018. https:// informnapalm.org/ua/ (accessed June 22, 2018).

27. Офіційний портал Верховної Ради України: «Указ Президента України Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України», 15.03.2016, http://zakon3.rada.gov.ua/laws/show/96/2016 (accessed June 20, 2018).

28. Постанова Кабінету Міністрів України від 13.10.2015 № 831 «Про утворення територіального органу Національної поліції», Урядовий кур'єр, № 195, 21.10.2015.

29. Президент України; Указ. «Про Національний координаційний центр кібербезпеки. Положення від 07.06.2016 № 242/2016, http:// zakon2.rada.gov.ua/laws/show/242/2016 (accessed June 17, 2018).

30. Президента України. Указ №47/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» http://www.president.gov.ua/documents/472017-21374 (accessed June 17, 2018).

31. П'ять найвідоміших хакерських угруповань, що діють проти України. Інфографіка Новое Время, https://nv.ua/ukr/ukraine/ events/ p-jat-najvidomishih-hakerskih-ugrupovan-shcho-dijut-proti-ukrajiniinfografika-1439392.html (accessed June 22, 2018).

References:

1. Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space http://webarchive.nationalarchives.gov.uk/+/ http:/www.cabinetoffice.gov.uk/media/216620/css0906.pdf (accessed June 15, 2018).

2. German Cyber Security Strategy, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/cybersecurity-strategy-for-germany/view (accessed June 16, 2018).

3. Gibson, W. 1994. Neuromancer. London: HarperCollins.

4. Glossary and Acronyms (Archived) / European Commission, https://ec.europa.eu/digital-single-market/#c (accessed June 15, 2018).

5. ISO/IEC 27032, «Information technology — Security techniques — Guidelines for cybersecurity», (2012) https://www.iso.org/standard/44375.html (accessed June 2018).

6. National Military Strategy for Cyberspace Operations, https://www.hsdl.org/?view&did=35693 (accessed June 16, 2018).

7. Statement from the Press Secretary». 2018. https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/?utm_source=link (accessed June 16, 2018).

8. Buriachok, V.L., Tolubko, V.B., Khoroshko, V.O., Toliupa, S.V. 2015. Informatsiina ta kiberbezpeka: sotsiotekhnichnyi aspekt: pidruchnyk, Kyiv DUT, 2015: 15.

9. Verkhovna Rada Ukrainy. «Zakon Ukrainy Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy» vid 05.10.2017 № 2163-VIII http://zakon5.rada.gov.ua/laws/show/2163-19 (accessed June 16, 2018).

10. Verkhovna Rada Ukrainy. «Pro Derzhavnu sluzhbu spetsialnoho zviazku ta zakhystu informatsii Ukrainy

11. Verkhovna Rada Ukrainy. «Pro telekomunikatsii. Zakon vid 18.11.2003 № 1280-IV» http://zakon4.rada.gov.ua/laws/show/1280-15/ (accessed June 17, 2018).

12. Hnatiuk, S.O. 2013. «Bazovi definitsii u haluzi kibernetychnoi bezpeky derzhavy», 2013, Visnyk Inzhenernoi akademii Ukrainy, http://nbuv.gov.ua/UJRN/Viau_2013_3-4_11 (accessed June 17, 2018).

13. Holovka, A.A. 2016. «Zakhyst kiberprostoru yak skladova informatsiinoi bezpeky Ukrainy v umovakh hibrydnoi viiny», Molodyi vchenyi, № 4, (2016): 334.

14. Drohomyretskyi, B. 2018. «Ukraino-rosiiska kiberviina: nevydymyi front». https://www.pravda.com.ua/columns/2018/02/22/7172439/ (accessed June 15, 2018).

15. Dubov, D.V. 2014. Kiberprostir yak novyi vymir heopolitychnoho supernytstva: monohrafiia. Kyiv, NISD, 2014: 210.

16. Dubov, D.V., Ozhevan, M.A. 2011. Kiberbezpeka: svitovi tendentsii ta vyklyky dlia Ukrainy. Kyiv, NISD, 2011: 12.

17. Spryiannia rozbudovi mozhlyvostei Ukrainy harantuvaty bezpeku suspilstva v umovakh hibrydnykh zahroz. Rezultaty ekspertnoho opytuvannia http://prismua.org/wp-content/uploads/2018/02/blok_XXIend_3001.pdf (accessed June 19, 2018).

18. Zakon vid 23.02.2006 № 3475-IV http://zakon4.rada.gov.ua/laws/show/3475-15 (accessed June 21, 2018).

19. Kiberbezpeka v Ukraini: perezavantazhennia? https://ckp.in.ua/events/19139 (accessed June 2018).

20. Kobra, H., Verestiuk, I. 2018. «Poviazani z Rosiieiu khakery peretvoryly Ukrainu na polihon dlia vyprobuvannia kiberzbroi, yaku v podalshomu Kreml hotovyi vykorystovuvaty proty kudy bilsh hriznykh oponentiv — SShA i YeS» https://magazine.nv.ua/ukr/journal/2558journal-no-24/virus-vova.html (accessed June 19, 2018).

21. Konventsiia Rady Yevropy pro kiberzlochynnist: vid 23 lystopada 2001 roku, http://zakon2.rada.gov.ua/laws/show/994_575 (accessed June 20, 2018).

22. Melnyk, S.V. 22 bereznia 2011. «Do problemy formuvannia poniatiino-terminolohichnoho aparatu kiberbezpeky», Aktualni problemy upravlinnia informatsiinoiu bezpekoiu derzhavy: zb. mater. nauk.-prakt. konf., (Kyiv, Vyd-vo NA SB Ukrainy, 2011).

23. Merkel oburena slovamy Nuland pro rol YeS v ukrainskii kryzi. Ukrainska pravda, 07.02.2014 https://www.pravda.com.ua/news/2014/02/7/7013123/ (accessed June 20, 2018).

24. Naibilshi kiberataky proty Ukrainy z 2014 roku. Infohrafika. Novoe Vremia https://nv.ua/ukr/ukraine/events/najbilshi-kiberatakiproti-ukrajini-z-2014-roku-infografika-1438924.html (accessed June 17, 2018).

25. Okinavska Khartiia hlobalnoho informatsiinoho suspilstva, http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=998_163 (accessed June 19, 2018).

26. Ofitsiina storinka «InformNapalm». 2018. https://informnapalm.org/ua/ (accessed June 22, 2018).

27. Ofitsiinyi portal Verkhovnoi Rady Ukrainy: «Ukaz Prezydenta Ukrainy Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 27 sichnia 2016 roku «Pro Stratehiiu kiberbezpeky Ukrainy», 15.03.2016, http://zakon3.rada.gov.ua/laws/show/96/2016 (accessed June 20, 2018).

28. Postanova Kabinetu Ministriv Ukrainy vid 13.10.2015 № 831 «Pro utvorennia terytorialnoho orhanu Natsionalnoi politsii», Uriadovyi kurier, № 195, 21.10.2015.

29. Prezydent Ukrainy; Ukaz. «Pro Natsionalnyi koordynatsiinyi tsentr kiberbezpeky. Polozhennia vid 07.06.2016 № 242/2016, http://zakon2.rada.gov.ua/laws/show/242/2016 (accessed June 17, 2018).

30. Prezydenta Ukrainy. Ukaz №47/2017 «Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 29 hrudnia 2016 roku «Pro Doktrynu informatsiinoi bezpeky Ukrainy» http://www.president.gov.ua/documents/472017-21374 (accessed June 17, 2018).

31. Piat naividomishykh khakerskykh uhrupovan, shcho diiut proty Ukrainy. Infohrafika Novoe Vremia, https://nv.ua/ukr/ukraine/events/pjat-najvidomishih-hakerskih-ugrupovan-shcho-dijut-proti-ukrajiniinfografika-1439392.html (accessed June 22, 2018).