УДК 343.32 (477)
DOI: 10.26693/ahpsxxi2019.01.138

КІБЕРБЕЗПЕКА: СУЧАСНІ ВИКЛИКИ ПЕРЕД УКРАЇНОЮ

Анатолій Худолій,
e-mail: toliy65@yahoo.com
ORCID: https://orcid.org/0000-0001-8144-126X
Національний університет «Острозька академія»,
Україна, 35800, м. Острог, Рівненська обл., вул. Семінарська, 2

У статті розглянуто питання інформаційної безпеки України за останні кілька років, заходи здійснені урядом України і спрямовані на поліпшення її стану. Мета статті – висвітлити питання кіберзахисту України в світлі російської агресії проти України. Відсутність ґрунтовного законодавчого забезпечення кібербезпеки в Україні в умовах гібридної війни значно підвищує ризики руйнування національної системи. Проблема погіршується ще й тим фактом, що, сьогодні, в Україні відсутній єдиний центр координації роботи щодо законодавчого та нормативно-правового забезпечення ефективної системи кібербезпеки, яка б базувалась на комплексному реальному аналізі стану в зазначеній сфері, існуючих викликів, наявних і потенційних загроз, інтегрувалась в європейську та глобальну систему кібернетичної безпеки, мала б достатнє фінансове, організаційне, технічне та кадрове забезпечення. Автор розглядає основні документи, пов'язані з кібербезпекою в Україні, їхні сильні та слабкі сторони. Орієнтиром для створення законодавчої концептуальної основи у боротьбі з кіберзагрозами слугують документи прийняті СЄ та НАТО, які мають значно більше досвіду у кібернетичному протистоянні. Долучення України, її цивільних і військових органів до європейських і євроатлантичних ініціатив створює підґрунтя для цілеспрямованого процесу розвитку кібернетичної стратегії на державному та приватному рівнях.

Ключові слова*: кібербезпека, кіберзагрози, гібридна війна, кібератаки, Україна, інформаційна війна*

Вступ. Сучасний світ неможливо уявити без інформаційних технологій, однак такий стан речей має й протилежний бік, оскільки їх ефективно використовують для ведення інформаційних війн. Кіберпростір успішно використовує як держава, так і окремі громадяни, проте зворотній бік цифрових технологій несе руйнівну силу, загрозу та небезпеку як для суспільства, так і для держави загалом, про що свідчить досвід України у протистоянні із зовнішньою агресією.

Актуальність дослідження зумовлена швидким розвитком інформаційних технологій, які значною мірою визначають не лише розвиток сучасної держави, але й її існування. Цифрові технології наскільки широко використовуються в професійній сфері та повсякденному житті, що сьогодення неможливо уявити безе носіїв інформації, гаджетів тощо. Проте, попри позитив, такі технології несуть руйнівну силу, використання якої завдає вражаючої шкоди на різних рівнях функціонування держави, особливо коли держав в стані війни, як це ми спостерігаємо в Україні. Актуальність дослідження визначена не лише характером дослідження, але й власне відсутністю ґрунтовних досліджень, спрямованих на визначення лакун у кібербезпеці України, її цивільних і військових компонентах.

Мета дослідження полягає у висвітленні питання розвитку стратегії кібернетичної оборони України в світлі російської агресії проти України. Реалізація задекларованої мети передбачає низку питань, а саме:

– здійснити огляд сучасних досліджень проблеми кібербезпеки;

– розглянути офіційні документи, спрямовані на посилення кібернетичної безпеки України;

– здійснити аналіз шляхів розвитку кібербезпеки України з урахуванням останніх подій.

Аналіз останніх публікацій. Питанню кібербезпеки присвячені численні дослідження закордонних і порівняно невеликий відсоток досліджень вітчизняних науковців, які висвітлювали різні аспекти даного питання від безпекових особливостей інформаційних технологій і кіберзлочинів до інформаційних війн. Серед зарубіжних дослідників слід зазначити Р. Муді, Л. Стрельцова, Л. Керулуса, Е. Грінберга й інших.

Закордонні дослідники. Ребекка Муді[1] досить детально аналізує статистичні дані рейтингу країн світу з урахуванням низки факторів, безпосередньо пов'язаних з кібернетичною безпекою країни. Так Л. Стрельцов розглядає стан кібербезпеки в України упродовж 2015-2017 років, акцентуючи увагу на принципах кібербезпеки, суб'єктах, викликах та здобутках[2]. На жаль, стан кібербезпеки в Україні за останні два роки дещо змінився, проте окремі аспекти залишилися поза увагою науковця, дослідження якого було обмежене хронологічними межами. Л. Керулус[3] розглядає кібернетичну безпеку та стан її захисту та вразливості в контексті російської агресії, висвітлює особливості кібернетичної війни та деяких аспектів гібридної війни не теренах України, яка на передній лінії імперської політики Кремля. Е. Грінберг розглядає кібервтручання російських хакерів в Україні, від вимкнень світла до втручань у роботу багатьох секторів, від ЗМІ, фінансової сфери, транспорту, військової сфери до політичної та енергосистеми[4]. Західні дослідники та журналісти надають перевагу висвітленню кібервійни між Україною та Росією, точніше сказати, кібератакам російських хакерів проти цивільних і військових об'єктів України, оскільки Київ на даному етапі неспроможний завдати належного удару у відповідь.

Серед вітчизняних науковців немає єдиного підходу до аналізу актуальної проблеми – кібербезпеки України. Підходи варіюються від правових аспектів до стратегій силових відомств і військових ініціатив. Зокрема Ю. Семеній, С. Глущенко та О. Макаревич розглядають кібербезпеку України з точки зору законодавчого забезпечення, аналізу офіційних документів, зокрема стратегії кібернетичної безпеки, яка ґрунтується на законі про основні принципи кібербезпеки №2163-VIII від 5 жовтня 2017 року[5]. Практичні кроки втілення згадано стратегії залишилися поза увагою аналітиків. Низка експертів розграє кібербезпеки невіддільно від безпеки інформаційної та комунікаційної[6]. Досить збалансованим виявися аналіз рівня кібербезпеки України О. Янковського, який розглядає низку критеріїв оцінки ситуації з інформаційною безпекою, водночас доводячи, що застарілі підходи до вирішення проблеми сьогодення ситуацію не врятують, а слугують перепонами на шляху таких потрібних змін. І що найважливіше, відсутній системний зв'язок між владою, професійним товариством і бізнесом щодо питань кібербезпеки в Україні. Автор висловлює думку

[1] Moody, R. (2019, February 6). Which countries have the worst (and best) cybersecurity? *Comparitech*. Retrieved from https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/?fbclid=IwAR2vUYEilDvxl-ktToWiZohRygCw-q0q19IGSnKay-UbVbRbprB5P7jSfDg

[2] Streltsov, L. (2017). The System of Cybersecurity in Ukraine : Principles, Actors, Challenges, Accomplishments. *European Journal for Security Research*, *2* (2), 147-184. doi:10.1007/s41125-017-0020-x

[3] Cerulus, L. (2019, February 20). How Ukraine became a test bed for cyberweaponry. *Politico*. Retrieved from https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/

[4] Greenberg, A. (2017, June 20). *How an Entire Nation Became Russia's Test Lab for Cyberwar*. Retrieved from https://www.wired.com/story/russian-hackers-attack-ukraine/

[5] Semeniy, J., Glushchenko, S. & Makarevich, O. (2018, January 30). *Getting the Deal Through: Cybersecurity 2018*. Retrieved from https://www.asterslaw.com/press_center/publications/ getting_the_deal_through_cybersecurity_2018_ukraine/

[6] Кібербезпеку не треба відділяти від інформаційної та комунікаційної – експерт (2019, 12 грудня). Retrieved from https://www.ukrinform.ua/rubric-society/2836639-kiberbezpeku-netreba-viddilati-vid-informacijnoi-ta-komunikacijnoi-ekspert.html

низки фахівців, які критично оцінюють глибоко укорінену проблему кількох рівнів[7]. П. Біленчук і В. Кулик аналізують питання кібербезпеки з точки зору теоретичних і практичних підходів, акцентуючи увагу на в важливих аспектах проблеми, висвітлюючи недоліки вітчизняних підходів[8]. Заслуговує уваги стаття колишнього посадовця В. Горбуліна, який неупереджено оцінює кібербезпеки країни в світлі оборонної стратегії та інформаційної війни[9].

Основна частина. Як Україна реагує на виклики в царині кібербезпеки? Згідно з дослідженням, здійсненим «Лабораторією Касперського» (ITU, CSIS) у 2019 р. Україна зайняла десяте місце з кінця списку шістдесяти кран світу за низкою параметрів, зокрема: відсоток інфікованих телефонів, відсоток інфікованих комп'ютерів, кількості зловмисних фінансових атак; відсоток атак кіберзлочинців, країни найкраще підготовлені до кібератак та країни з найсучаснішим законодавством. Позаду нас – лише Іран, Білорусь, Пакистан, Узбекистан, Індонезія тощо. Наші сусіди значно нас випередили. РФ – на 38 місці (60-е місце – найвище), Польща обійняла 40, Угорщина – на 41, а найвище місце (60) у Японії[10]. Це змушує замислитись проте, наскільки Україна готова захищати себе не лише на фізичному, але й інформаційному рівні і що для цього робить президент та уряд? Критичний стан інформаційної безпеки особливо гостро виявився на тлі російської агресії 2014 р., яка виявила всі критичні недоліки в інформаційній обороні країни.

Які ж зміни відбулися в політичній, економічній та військовій сферах у зв'язку з кібернетичними загрозами Україні? На жаль, в Україні відсутнє ґрунтовне законодавче забезпечення кібербезпеки в умовах гібридної війни, що значно підвищує ризики руйнування національної системи. Такий підхід ставить під сумнів участь українських складових забезпечення кібербезпеки на європейському та світовому рівнях. Проблема погіршується ще й тим фактом, що, сьогодні, в Україні відсутній єдиний центр координації роботи щодо законодавчого та нормативно-правового забезпечення ефективної системи кібербезпеки, яка б базувалась на комплексному аналізі реального стану речей в зазначеній сфері, існуючих викликів, наявних і потенційних загроз, інтегрувалась в європейську та глобальну систему кібернетичної безпеки, мала б достатнє фінансове, організаційне, технічне та кадрове забезпечення[11].

Концептуальну основу кібернетичної безпеки України складають закони України «Про основи національної безпеки», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», Конвенція Ради Європи про кіберзлочинність, стратегія кібербезпеки України та інші. Як не прикро визнавати, проте всі згадані закони України носять декларативний характер, а війна, що триває потребує практичного застосування, дієвого та рішучого.

Конвенція Ради Європи про кіберзлочинність (Будапештська Конвенція) (2001 р.) є найбільш вагомим і визнаним міжнародно-правовим документом у сфері боротьби з міжнародною та національною кіберзлочинністю. Україна не лише підписала його, але й ратифікувала його 10 березня 2006 р. Київ долучився до реалізації проекту Ради Європи та ЄС «Кіберзлочинність@Східне партнерство» в 2011 р., мета якого поля-

---

[7] Янковський, О. (2019, 14 вересня). Україні потрібна нова кіберстратегія. *Українська правда*. Retrieved from https://www.pravda.com.ua/columns/2019/09/14/7226291/

[8] Біленчук, П. & Кулик, В. (2018). Стратегія забезпечення кібербезпеки в гібридній війні. *Юридичний вісник України, 1/2,* 18-19.

[9] Горбулін, В. (2015, 20 лютого). У пошуках асиметричних відповідей: кіберпростір у гібридній війні. *Дзеркало тижня*. Retrieved from https://dt.ua/internal/u-poshukah-asimetrichnih-vidpovidey-kiberprostir-u-gibridniy-viyni-_.html

[10] Moody, R. (2019, February 6). Which countries have the worst (and best) cybersecurity? *Comparitech*. Retrieved from https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/?fbclid=IwAR2vUYEilDvxl-ktToWiZohRygCw-q0q19IGSnKay-UbVbRbprB5P7jSfDg

[11] Кольцов, М., Приходько, О. & Аушев, Є. (2017, грудень). *Пропозиції до політики щодо реформування сфери кібербезпеки в Україні.* Київ: ГО «Лабораторія законодавчих ініціатив», 4-5. Retrieved from https://parlament.org.ua/wp-content/uploads/2017/10/Policy-Paper_Kiberbezpeka-1-1.pdf

гає в імплементації Будапештської конвенції, удосконалення національного законодавства в сфері боротьби з кіберзлочинністю та налагодження державно-приватного партнерства в цій сфері[12].

У вересні 2014 р. Верховна Рада України ратифікувала Угоду про Асоціацію між Україною та ЄС, Європейським Співтовариством з атомної енергії та їхніми державами-членами[13]. Одна з вимог згаданої Угоди – наблизити українське законодавство до права ЄС. У статті 3 додатку XVII зазначено, що, згідно зі статтями 114, 124, 133 та 139 Глави 6 «Підприємницька діяльність, торгівля послугами та електронна торгівля» Україна на постійній основі впроваджуватиме чинне законодавство ЄС у свою національну систему. У всіх відповідних документах ЄС вказується, що реформа правового регулювання захисту персональних даних має пряме відношення до врегулювання питань кіберзахисту та забезпечення мережевої та інформаційної безпеки. Стало відомо, що апарат Уповноваженого Верховної Ради України з прав людини готує неофіційні переклади документів щодо питання кібербезпеки в Україні і планує створювати Робочу групу з наближення українського законодавства до європейських стандартів сфері захисту персональних даних[14]. Важливість питання захисту персональних даних суттєво зросла після початку дії безвізового режиму. Слід зауважити, що існують елементарні заходи безпеки, які можуть забезпечити захист: 1) впровадження процесу управління персонального оновлення на всіх вузлах інфраструктури організації; 2) впровадження сегментації мережі (поділу мережі на різні сегменти); 3) створення, підтримка та тестування плану реагування на інциденти кібербезпеки; 4) впровадження процесу резервного копіювання даних (особливо на віддалений носій). Серед додаткових заходів безпеки слід здійснювати робочий процес моніторингу мережевих подій, впровадження обладнання з функцією IPS[15].

В Європі для всіх країн-членів ЄС була прийнята директива про загальні заходи безпеки мережевих та інформаційних систем у ЄС 2016/1148[16]. Директива зобов'язує держави-члени визначити об'єкт критичної інфраструктури в різних сферах.

У травні 2017 р. в українському парламенті розглядали законопроект № 2126а «Про основні засади забезпечення кібербезпеки України». Цей факт і зміст самого документа свідчить про актуальність питання кібербезпеки для країни. На жаль, стан кібернетичної безпеки в Україні, заходи протидії інформаційним загрозам свідчать про незадовільний стан вирішення проблеми, а всі ті заходи, що відбуваються не мають цілісного та комплексного підходу. Підтвердженням висловленої думки може слугувати кібератака 27 червня 2017 р., коли комп'ютерний вірус «Ransom:win32/Petya» вразив приватний і державний сектори української економіки, зокрема банки, аеропорти, державну залізничну компанію, телекомпанії, мережеві супермаркети, енергетичні компанії, державні фіскальні служби, органи державної влади та місцевого самоврядування[17]. Вірус зашкодив приватним і державним компаніям інших країн, проте найбі-

---

[12] Кіберзлочинність@Східне партнерство III: публічне / приватне співробітництво (Вірменія, Азербайджан, Білорусь, Грузія, Республіка Молдова, Україна). (2016, April). Retrieved from https://rm.coe.int/168065102e

[13] Верховна Рада України. (2014). *Закон України Про ратифікацію Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони*. Retrieved from https://zakon.rada.gov.ua/laws/show/1678-18

[14] Красний, А., Зимарин, А., Мягка, І. & Полєтаєва, М. (2018, 10 травня). *Безпека в мережі: як Україна регулюватиме кіберпростір*. Retrieved from https://mind.ua/openmind/20184620-bezpeka-v-merezhi-yak-ukrayina-regulyuvatime-kiberprostir

[15] Ibidem.

[16] Верховна Рада України. (2016). *Директива Європейського Парламенту і Ради (ЄС) 2016/1148 від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу*. Retrieved from https://zakon.rada.gov.ua/laws/show/984_013-16

[17] Грабовий, А. (2017). Закон про кібербезпеку та стратегія кібербезпеки України. *Юрист & Закон, 26*. Retrieved from http://uz. ligazakon.ua/ua/magazine_article/%20EA010553

льшої шкоди було завдано Україні, яка була і залишається вразливою перед лицем зовнішніх інформаційних загроз. Причиною стала відсутність відповідного програмного забезпечення, відповідних підрозділів і державної стратегії, розробленої та спрямованої на захист як громадянина, так і держави.

Слід зауважити, що проект закону має значні недоліки та дублює вже діюче положення Стратегії кібербезпеки України, затвердженої Указом президента України (від 15 березня 2016 р.) № 96. Недоліком законопроекту в тому, що не визначено єдиного органу, який здійснює керівництво суб'єктами кібербезпеки у мирний час, оскільки РНБ, МО України та Генеральний штаб ЗС України відповідають за оперативне управління у відповідний період. А без єдиного органу неможливо адекватно реагувати на кібернетичні загрози. У жовтні 2017 р. Верховна Рада ухвалила закон «Про основні засади забезпечення кібербезпеки України», який набрав чинності 9 травня 2017 р. В документі визначено основи забезпечення захисту національних інтересів України в кібернетичному просторі, повноваження державних органів влади, принципи координації їхньої діяльності задля кібернетичної безпеки. Проте захистити всіх користувачів нереально, тому, як зазначають фахівці, слід визначити пріоритети та способи захисту від кібератак[18]. Зрозуміло, що прийняті закони потребують уточнень, додаткових положень, визначеного чіткого алгоритму дій у тій або іншій ситуації.

Питання кібернетичних загроз є пріоритетом для Збройних Сил кожної держави. Підтвердженням висловленої думки є зустріч глав держав та голів урядів країнчленів НАТО, що відбулася в 2016 році у Варшаві, і на якій було вперше підписано Договір між ЄС та НАТО про співробітництво у сфері безпеки, зокрема в питаннях гібридних війн і кібератак. Було визначено кілька пріоритетних сфер діяльності,зокрема: 1) протистояння гібридним загрозам; 2) оперативне реагування та співробітництво в військово-морській сфері; 3) кібербезпека і оборона; 4) можливості захисту, оборонні промисловість та відповідні наукові дослідження; 5) тренування та узгодження дій партнерів[19].

Упродовж останніх років кібернетична безпека стала пріоритетним напрямком розвитку сучасної армії. Активна гібридна війна, яка супроводжує фізичну фазу воєнних дій, змушує українських військових активізувати зусилля в цьому напрямі. Агресор активно використовує кіберпростір не лише проти України, але й проти інших держав. Пригадаймо втручання Росії у вибори президента США, кібератаки проти балтійських держав, використання фейкових новин і відвертої пропаганди, численні кібератаки 2014-2019 рр. Основна мета РФ щодо України – розхитування ситуації в країні, створення хаосу та паніки як основи для захисту власних інтересів, політичних, економічних, безпекових, іміджевих тощо.

Гібридна війна (як новий тип війни) є прихованим способом ведення воєнних дій під прикриттям незаконних збройних формувань, так і одночасне використання широкого спектра політичних, економічних (енергетичних і торговельно-економічних), а також інформаційно-пропагандистських заходів, які її супроводжують упродовж усього періоду воєнних дій. За таких умов країна-агресор зазвичай залишається публічно-непричетною до розпаленого конфлікту та здійснює приховані військові операції[20]. Зразком широкомасштабної розвідувальної кібероперації стала операція під назвою BugDrop, мета якої полягала в тому, щоб отримати віддалений доступ до пер-

[18] Стан кібербезпеки в Україні. Кібербезпека в інформаційному суспільстві. (2019). *Інформаційно-аналітичний дайджест, 1*, 4.

[19] EU. General Secretariat of the Council. (2016, July 8). *Joint declaration by the President of the European Council, Donald Tusk, the President of the European Commission, Jean-Claude Juncker, and the Secretary General of NATO, Jens Stoltenberg, Warsaw*. Retrieved from https://www.consilium.europa.eu/media/21481/nato-eu-declaration-8-july-en-final.pdf

[20] Міністерство оборони України. (2018, 7 травня). *Кібербезпека як важлива складова всієї системи захисту держави*. Retrieved from http://www.mil.gov.ua/ukbs/kiberbezpeka-yak-vazhliva-skladova-vsiei-sistemi-zahistu-derzhavi.html

сональних комп'ютерів та інших гаджетів працівників різних структур, унаслідок чого персональні дані та паролі працівників об'єктів критичної інфраструктури, ЗМІ та наукових установ викрадалися й використовувалися.

Упродовж 2018 року Росія здійснила 190 провокацій з метою дестабілізувати українське суспільство. Таку кількість провокацій зафіксувало Міністерство з питань тимчасово окупованих територій та внутрішньо переміщених осіб в Україні[21]. У 2019 році російська влада додатково виділила своїм спецслужбам 350 млн. доларів для реалізації підривної діяльності в Україні. Кошти будуть спрямовані на оплату фейкових новин, підкуп, організацію провокацій, протестів, внутрішньополітичного тиску на керівництво країни, а також для підготовки кібератак[22]. Наведені факти свідчать про те що Росія від агресії не відмовилась, а навпаки нарощує темпи, щоб контролювати Україну в інформаційному просторі і Україна суттєво програє інформаційну війну.

Кроком у розвитку кібербезпеки став Закон України про національну безпеку України, прийнятий в червні 2018 р. Стаття 31 Закону присвячена стратегії кібербезпеки України. В ній зазначено, що згаданий документ є документом довгострокового планування, в якому визначено пріоритети національних інтересів держави у сфері кібербезпеки[23]. На жаль, викладено загальні положення, без конкретних заходів, доповнень тощо. Це свідчить про недооцінку важливості даного питання в сфері безпеки та оборони України, наслідком чого стають збоїв роботі державних органів влади, приватного бізнесу тощо. На численні кібератаки з боку РФ Україна слабко реагує.

Попри повільну реакцію керівництва країни та силових відомств спостерігаємо перші кроки в напрямку поліпшення. Так Міністерство Оборони України підтримало проект НАТО, спрямований на підготовку фахівців у сфері кібербезпеки. Зокрема, фахівці Альянсу розробили програму «Розширення освіти у сфері оборони» (DEEP), до якої долучилися не лише країни-члени НАТО, але й партнери, серед яких Україна. До проекту залучено дванадцять країн, значна частина яких з колишнього СНД. За умовами програми, експерти з союзних країн відвідали Житомирський військовий інститут імені Сергія Корольова з 24 по 28 вересня 2018 р., де провели заняття згаданого курсу з кібербезпеки. Курс викладали з урахуванням військового контексту з урахуванням досвіду канадської, польської та ірландської військових академій[24]. В програмі передбачено національну специфіку країни. Українські військові ознайомилися з різними засобами та практиками кібернетичної безпеки, здобули міжнародний досвід.

16 жовтня 2019 р. в Києві відбувся другий міжнародний Форум «Кібербезпека – найбільша проблема цифрової економіки» та перша Національна виставка «Кібербезпека 2019» (за підтримки РНБО України), яка засвідчила не лише інтерес до даного питання, але й підняла низку проблем, що існують і які слід терміново вирішувати, серед яких: надійність кібербезпеки в Україні; можливі кіберзагрози; уроки, які винесли влада та бізнес після масштабних кібератак; приватно-державні ініціативи, спрямовані на прискорення формування безпечного кіберпростору країни[25]. Учасники обговорили ключові теми, серед яких – кібербезпека у політиці, технологіях, освіті. Були напрацьовані пропозиції та рекомендації для президента України, уряду та парламенту.

---

[21] Російська агресія у кіберпросторі: за минулий рік Кремль здійснив майже 200 провокацій (2019). Retrieved from https://24tv.ua/rosiyska_agresiya_u_kiberprostori_za_minuliy_rik_kreml_zdiysniv_mayzhe_200_provokatsiy_n1101233?utm_source=rss

[22] Кібервійна проти України. Кібербезпека в інформаційному суспільстві. (2019). *Інформаційно-аналітичний дайджест, 1*, 7.

[23] Верховна Рада України. (2018). *Закон України Про національну безпеку України*. Retrieved from https://zakon.rada.gov.ua/laws/show/2469-19#n355

[24] NATO. (2018, October 29). *Enhancing cybersecurity in Ukraine*. Retrieved from https://www.nato.int/cps/en/natohq/news_159840.htm?selectedLocale= en

[25] Форум: Кібербезпека – найбільша проблема цифрової економіки (2019, 16 жовтня). Retrieved from https://cybersecurity.ciseventsgroup.com/

Висновки. Впровадження відповідних законів щодо кібербезпеки – лише перші кроки українських посадовців, які, на превеликий жаль, неспроможні ліквідувати значне відставання України не лише в технічному плані та кадровому забезпеченні, але й на рівні усвідомлення проблеми державної ваги. Інформаційна війна триває, проте, на даному етапі, Україна її програє.

REFERENCES

Bilenchuk, P. & Kulyk, V. (2018). Stratehiia zabezpechennia kiberbezpeky v hibrydnii viini [Strategy of providing cybersecurity in a hybrid war]. *Yurydychnyi visnyk Ukrainy, 1/2*, 18-19. [in Ukrainian]

Cerulus, L. (2019, February 20). How Ukraine became a test bed for cyberweaponry. *Politico*. Retrieved from https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/ [in English]

EU. General Secretariat of the Council. (2016, July 8). *Joint declaration by the President of the European Council, Donald Tusk, the President of the European Commission, Jean-Claude Juncker, and the Secretary General of NATO, Jens Stoltenberg, Warsaw*. Retrieved from https://www.consilium.europa.eu/media/21481/nato-eu-declaration-8-july-en-final.pdf [in English]

Forum. Kiberbezpeka – naibilsha problema tsyfrovoi ekonomiky. (2019, 16 zhovtnia). [Cyber security is the biggest problem of a digital economy]. Retrieved from https://cybersecurity.ciseventsgroup.com/ [in Ukrainian]

Greenberg, A. (2017, June 20). *How an Entire Nation Became Russia's Test Lab for Cyberwar*. Retrieved from https://www.wired.com/story/russian-hackers-attack-ukraine/ [in English]

Horbulin, V. (2015, 20 liutoho). U poshukakh asymetrychnykh vidpovidei: kiberprostir u hibrydnii viini. [Searching for asymmetric responses: cyberspace in a hybrid war]. *Dzerkalo tyzhnia*. Retrieved from https://dt.ua/internal/u-poshukah-asimetrichnih-vidpovidey-kiberprostir-u-gibridniy-viyni-_.html [in Ukrainian]

Hrabovyi, A. (2017). Zakon pro kiberbezpeku ta stratehiia kiberbezpeky Ukrainy [The Law about cybersecurity and a strategy of cybersecurity of Ukraine]. *Yuryst & Zakon, 26*. Retrieved from http://uz. ligazakon.ua/ua/magazine_article/%20EA010553 [in Ukrainian]

Kiberbezpeku ne treba viddiliaty vid informatsiinoi ta komunikatsiinoi. (2019, 12 hrudnia). [Cyber security shouldn't be separated from information and communicative security]. Retrieved from https://www.ukrinform.ua/rubric-society/2836639-kiberbezpeku-ne-treba-viddilati-vid-informacijnoi-ta-komunikacijnoi-ekspert.html [in Ukrainian]

Kiberviina proty Ukrainy. Kiberbezpeka v informatsiinomu suspilstvi. (2019). [Cyber war against Ukraine. Cybersecurity in the information society]. *Informatsiino-analitychnyi daidzhest, 1*, 6-7. [in Ukrainian]

Kiberzlochynnist@Skhidne partnerstvo III: publichne/pryvatne spivrobitnytstvo (Virmeniia, Azerbaidzhan, Bilorus, Hruziia, Respublika Moldova, Ukraina). (2016, April). [Cyber crimes and the Eastern Partnership III: public/private cooperation]. Retrieved from https://rm.coe.int/168065102e [in Ukrainian]

Koltsov, M., Prykhodko, O. & Aushev, Ye. (2017, hruden). *Propozytsii do polityky shchodo reformuvannia sfery kiberbezpeky v Ukraini* [Proposition to politics regarding reforming the sphere of cybersecurity in Ukraine]. Kyiv: HO «Laboratoriia zakonodavchykh initsiatyv». Retrieved from https://parlament.org.ua/wp-content/uploads/2017/10/Policy-Paper_Kiberbezpeka-1-1.pdf [in Ukrainian]

Krasnyi, A., Zymaryn, A., Miahka, I. & Polietaieva, M. (2018, 10 travnia). *Bezpeka v merezhi: yak Ukraina rehuliuvatyme kiberprostir*. [Security in the net: how Ukraine is going to regulate cyber space]. Retrieved from https://mind.ua/openmind/20184620-bezpeka-v-merezhi-yak-ukrayina-regulyuvatime-kiberprostir [in Ukrainian]

Ministerstvo oborony Ukrainy. (2018, 7 travnia). *Kiberbezpeka iak vazhlyva skladova vsiiei systemy zakhystu derzhavy*. [Cybersecurity as an important component of the whole system of a state defense]. Retrieved from http://www.mil.gov.ua/ukbs/kiberbezpeka-yak-vazhliva-skladova-vsiei-sistemi-zahistu-derzhavi.html [in Ukrainian]

Moody, R. (2019, February 6). Which countries have the worst (and best) cybersecurity? *Comparitech*. Retrieved from https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/?fbclid=IwAR2vUYEilDvxl-ktT0WiZ0hRygCw-q0q19IGSnKay-UbVbRbprB5P7jSfDg [in English]

NATO. (2018, October 29). *Enhancing cybersecurity in Ukraine*. Retrieved from https://www.nato.int/cps/en/natohq/news_159840.htm?selectedLocale= en [in English]

Rosiiska ahresiia u kiberprostori: za mynulyi rik kreml zdiisnyv maizhe 200 provokatsii. (2019). [Russian aggression in cyberspace: during last year the Kremlin organized almost 200 provocations]. Retrieved from https://24tv.ua/rosiyska_agresiya_u_kiberprostori_za_minuliy_rik_kreml_ zdiysniv_mayzhe_200_provokatsiy_n1101233?utm_source=rss [in Ukrainian]

Semeniy, J., Glushchenko, S. & Makarevich, O. (2018, January 30). *Getting the Deal Through: Cybersecurity 2018*. Retrieved from https://www.asterslaw.com/press_center/publications/getting_the_deal_through_cybersecurity_2018_ukraine/ [in English]

Stan kiberbezpeky v Ukraini. Kiberbezpeka v informatsiinomu suspilstvi. (2019). [State of cybersecurity in Ukraine. Cybersecurity in information society]. *Informatsiino-analitychnyi daidzhest, 1*, 4-5. [in Ukrainian]

Streltsov, L. (2017). The System of Cybersecurity in Ukraine : Principles, Actors, Challenges, Accomplishments. *European Journal for Security Research*, *2*(2), 147-184. doi:10.1007/s41125-017-0020-x [in English]

Verkhovna rada Ukrainy. (2014). *Zakon Ukrainy Pro ratyfikatsiiu Uhody pro asotsiatsiiu mizh Ukrainoiu ta Yevropeiskym Soiuzom, Yevropeiskym Spivtovarystvom z atomnoi enerhii i ikhnimy derzhavamy-chlenamy* [Law of Ukraine «About the Ratification of the Treaty of the Association between Ukraine and the European Union, European Community on Nuclear Energy and their State-members»]. Retrieved from https://zakon.rada.gov.ua/laws/show/1678-18 [in Ukrainian]

Verkhovna rada Ukrainy. (2016). *Dyrektyva Yevropeiskoho Parlamentu i Rady (YeS) 2016/1148 vid 6 lypnia 2016 roku pro zakhody dlia vysokoho spilnoho rivnia bezpeky merezhevykh ta informatsiinykh system na terytorii Soiuzu* [A Directive of the European Parliament and a Council of the EU about measures for a high level of common security of a net and information systems on the territory of the European Union]. Retrieved from https://zakon.rada.gov.ua/laws/show/984_013-16 [in Ukrainian]

Verkhovna rada Ukrainy. (2018). *Zakon Ukrainy Pro natsionalnu bezpeku Ukrainy*. [Law of Ukraine «About the national security of Ukraine»]. Retrieved from https://zakon.rada.gov.ua/laws/show/2469-19#n355 [in Ukrainian]

Yankovskyi, O. (2019, 14 veresnia). Ukraini potribna nova kiberstratehiia [Ukraine needs a new cyberstrategy]. *Ukrainska pravda*. Retrieved from https://www.pravda.com.ua/columns/2019/09/14/7226291/ [in Ukrainian]

Anatoliy Khudoliy,
National University of Ostroh Academy, Ostroh, Ukraine
ORCID: https://orcid.org/0000-0001-8144-126X

Cybersecurity: modern challenges of Ukraine

The article deals with information technologies, especially their application as war instruments. Cyber space, used by a state and its people, has a reverse side of it which is of a ruinous character, a threat and a danger for existence of a state, its functioning and survival. Ukraine is one of the countries which are suffering from cyber threats and danger is posed by its close neighbor – the Russian Federation.

The purpose of the article is to highlight the issue of cybernetic defense of Ukraine in the light of the Russian information threat. The author has observed and analyzed the researches related to the topic of the article. Along with it he tried to answer the question about the measures taken by Ukrainian Government and Ukrainian state bodies in order to get ready to confront an information aggression and cybernetic attacks organized and launched against Ukraine, its state and private companies. The author draws attention to documents officially accepted by state bodies which lay the foundation for effective strategy in order to suppress cyber attack launched against Ukraine. He also managed to analyze cyber strategy of Ukrainian state bodies developed to protect Ukraine from modern style information war.

As a matter of fact Ukraine is quite sensitive to cybernetic attacks. According to the research conducted by «Kaspersky Laboratory» (ITU, CSIS) in 2019, Ukraine ranged tenth from the bottom in the list of sixty countries. Certain criteria were applied for arrangement of the list. Among them: a percentage of virus infected phones, a percentage

of virus infected computers, a number of malware financial attacks, a percentage of attacks of cyber criminals, countries best prepared for cybernetic attacks and countries with up to date laws. Unfortunately, Ukraine is behind many countries, even the neighboring ones, such as Russia, Poland, and Hungary. This fact pushes to think about the level of readiness to protect itself not only on physical, but also on information level and whether the President and the Government of Ukraine do their utmost to make the country strong enough.

Cybernetic security is a hot issue not only in a civil sphere, but also in the sphere of military activity. And the cybernetic attack launched by aggressor have made Ukrainian militaries take measures to protect the country, strengthen cyber security and defense. And the standards set by NATO countries serve as a target to pursue in the near future.

Hybrid war is one of the wars waged against Ukraine by the Russia Federation. It is a hidden style of war which combines a wide range of means such as political, economic, information and propaganda that accompany it for the whole period of war actions. So, to survive Ukraine has to change not only its military planning, but also information protection, improving security standards and taking protection measures in order to secure the state bodies and the people from cyber attacks, malware and the flow of dirty waters of propaganda, hatred and lies.

***Keywords**: cyber security, malware, hybrid war, cyber attacks, Ukraine, information war*