УДК 004.056.5:343.326 (045)
DOI https://doi.org/10.32782/2524-0374/2023-5/55

КІБЕРБЕЗПЕКА ЯК ЧАСТИНА НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ ВІЙНИ

CYBER SECURITY AS A PART OF THE NATIONAL SECURITY OF UKRAINE IN THE CONDITIONS OF WAR

Лесько Н.В., д.ю.н., професор,
професор кафедри адміністративного та інформаційного права
Національний університет «Львівська політехніка»

Кіра С.О., студентка І курсу
Навчально-науковий інститут права, психології та інноваційної освіти
Національного університету «Львівська політехніка»

У статті актуалізується питання нарощення кіберпотужностей нашої держави як обов'язкового елемента національної безпеки України в умовах війни. Автори наголошують на необхідності створення вітчизняних кіберсил для побудови міцних кіберкордонів і успішного протистояння майбутнім кібератакам. Розглянуто основні законодавчі зміни в сфері інформаційної безпеки, проаналізовано всі «за» і «проти» створення офіцерів із кіберзахисту для запобігання, відбиття чи аналізу хакерських атак ворога.

В умовах глобалізації та стрімкого розвитку новітніх інформаційних технологій великого значення набуває питання про захист прав людини в інформаційному просторі. З початку повномасштабної війни росії проти України кількість кібератак на об'єкти критичної інфрастуктури та інформаційні ресурси нашої держави істотно збільшилася. Станом на сьогодні, можна чітко ствердити, що де-факто росія веде тотальну багаторівневу кібер війну проти нашої держави. З огляду на це важливого значення набуває кібербезпека в контексті як частини національної безпеки. І не просто викликом часу, а нагальною необхідністю в довготривалій перспективі є постійне вдосконалення систем кіберзахисту та реформування законодавства в означеній сфері.

Підкреслено, що національна система кібербезпеки України перебуває лише в процесі становлення, однак російським кіберзагарбникам досягти стратегічної мети й завдати значної шкоди критичній інфраструктурі нашої країни не вдається. Правда в тому, що росія недооцінила Україну не тільки у військовій, але й у кіберсфері. Створення кіберсил – це наступний важливий крок, навіть попри те, що ще з початку війни фахівці в сфері IT-технологій з усієї країни долучилися до кіберполіції, чим обумовили створення вже діючої кіберармії. Варто підкреслити, що виконання зазначених в цьому дослідженні рекомендацій стосовно нарощення кіберпотужностей гарантовано виведе Національний індекс кіберезпеки (NCSI) України у лідируючі позиції в світі. Однак, спершу варто докласти зусиль для реформування вітчизняного законодавства в кіберсфері, з метою наділення його здатністю гнучко адаптуватися до нових змін безпекового середовища, що в свою чергу, гарантуватиме злагоджене функціонування національного сегмента кіберпростору в цілому.

Ключові слова: кібербезпека, кібервійна, кіберсили, національна безпека, інформаційні технології, кібервійська.

The article updates the issue of building up the cyber capabilities of our state as a mandatory element of Ukraine's national security in wartime conditions. The authors emphasize the need to create domestic cyber forces to build strong cyber borders and successfully counter future cyber attacks. The main legislative changes in the field of information security are considered, all the "pros" and "againsts" of creating cyber security officers to prevent, repel or analyze enemy hacker attacks are analyzed.

In the conditions of globalization and the rapid development of the latest information technologies, the issue of protecting human rights in the information space is of great importance. Since the beginning of Russia's full-scale war against Ukraine, the number of cyber attacks on critical infrastructure and information resources of our state has increased significantly. As of today, it can be clearly stated that de facto Russia is waging a total multi-level cyber war against our state. Given this, cyber security in the context of national security becomes important. And it is not just a matter of time, but an urgent necessity in the long term is the constant improvement of cyber protection systems and the reform of legislation in this area.

It is emphasized that the national cyber security system of Ukraine is only in the process of formation, but Russian cyber invaders are unable to achieve their strategic goal and cause significant damage to the critical infrastructure of our country. The truth is that Russia underestimated Ukraine not only in the military, but also in the cyber sphere. The creation of cyber forces is the next important step, despite the fact that since the beginning of the war, specialists in the field of IT technologies from all over the country have joined the cyber police, which led to the creation of an already functioning cyber army. It is worth emphasizing that the implementation of the recommendations specified in this study regarding the increase of cyber capabilities is guaranteed to bring the National Cyber Security Index (NCSI) of Ukraine to the leading positions in the world. However, first efforts should be made to reform domestic legislation in the cyber sphere in order to give it the ability to flexibly adapt to new changes in the security environment, which, in turn, will guarantee the harmonious functioning of the national segment of cyberspace as a whole.

Key words: cyber security, cyber war, cyber forces, national security, information technology, cyber military.

Постановка проблеми. Сьогодення знаменується активним формуванням шостого технологічного укладу як цілісного і стійкого утворення відповідно до вимог часу і потреби споживача. Інакшими словами, так звані «перспективні технології» [1], котрі, очікувано, повинні змінити та покращити рівень технологічного і соціального розвитку людства. До яких роками раніше належали більшість IT-інновацій, що вже не складають об'єкта суспільного резонансу, ба більше того – реально працюють та стали буденністю для нового інформаційного суспільства. Очевидним видається те, що заразом із посиленням розвитку інформаційних технологій, останнє чинить також значний вплив на функціонування національних й транснаціональних структур управління, що, в свою чергу, формує нову безпекову ситуацію.

Саме за означених вище умов для більшості країн світу важливим стало створення й постійне зміцнення вітчизняних кіберкордонів, нарощення кіберсил та інформування власних громадян щодо застосування цифрової грамотності, дотримання цифрового етикету та правил кібергігієни. Реалізація цих та ряду інших завдань IT спрямованості в умовах воєнного стану набуло для України особливого стратегічного значення.

Аналіз дослідження проблеми. Практичні й теоретичні аспекти вдосконалення кібербезпеки України й, зокрема, питання захисту прав людини в інформаційному просторі були предметом дослідження таких українських науковців, як С. Онищенко, А. Глушко, О. Мережко, Ю. Яковенко, Ю. Заскока, Ю. Деркаченко, С. Кухтик, Д. Березовський, А. Бежевець.

Мета статті: дослідити ключові кібербезпекові зміни під час воєнного стану в Україні, запропонувати шляхи для вдосконалення безпеки національного сегмента кіберпростору.

Виклад основного матеріалу. В умовах глобалізації та стрімкого розвитку новітніх інформаційних технологій великого значення набуває питання про захист прав людини в інформаційному просторі. З початку повномасштабної війни росії проти України кількість кібератак на об'єкти критичної інфрастуктури та інформаційні ресурси нашої держави істотно збільшилася. Станом на сьогодні, можна чітко ствердити, що де-факто росія веде тотальну багаторівневу кібер війну проти нашої держави. З огляду на це важливого значення набуває кібербезпека в контексті як частини національної безпеки. І не просто викликом часу, а нагальною необхідністю в довготривалій перспективі є постійне вдосконалення систем кіберзахисту та реформування законодавства в означеній сфері.

Кіберправо як спеціальна частина, підгалузь інформаційного права являє собою один із найперспективніших векторів розвитку сучасного вітчизняного законотворення. Нормативно-правову базу вітчизняної кібербезпеки окрім Конституції України та Стратегії кібербезпеки України складають: Закон України (далі – ЗУ) «Про інформацію» від 2 жовтня 1992 року № 2657-XII, ЗУ «Про захист інформації в інформаційно-телекомунікаційних системах» від 5 липня 1994 року № 80/94-ВР, ЗУ «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII, ЗУ «Про захист персональних даних» від 1 червня 2010 року № 2297-VI, Постанова Кабінету Міністрів «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29 березня 2006 року № 373, Постанова Кабінету міністрів України «Про затвердження загальних вимог до кіберзахисту об'єктів критичної інфраструктури» від 19 червня 2019 року № 518 та ряд інших.

Окрім означених вище документів, про кібербезпеку міститься, зокрема, в ЗУ «Про національну безпеку України» в пп. 21 п. 1 ст. 1 цього закону визначено, що Стратегія кібербезпеки України – це документ довгострокового планування, який визначає загрози кібербезпеці України, пріоритети та напрями забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави [2]. Як відомо, основними суб'єктами національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України. При цьому, контроль за законністю заходів із забезпечення кібербезпеки України відповідно до статті 15 ЗУ «Про основні засади забезпечення кібербезпеки України» в сфері дотримання законодавства здійснюється Верховною Радою України. А контроль за діяльністю із забезпечення кібербезпеки суб'єктів сектору безпеки і оборони та інших державних органів здійснюється Президентом України та Кабінетом Міністрів України в порядку, визначеному Конституцією і законами України [3].

Кіберстійкість країни багато в чому залежить саме від злагодженої взаємодії означених вище суб'єктів національної системи кібербезпеки на всіх рівнях. Між іншим, новостворений 11 березня 2021 року Національний координаційний центр кібербезпеки (далі – ЦКЦК), як робочий орган Ради національної безпеки і оборони України, якраз таки покликаний вирішувати найбільш складні проблеми в означеній сфері. Однією з таких проблем є питання координації. ЦКЦК, в свою чергу, здійснює координацію діяльності суб'єктів національної безпеки і оборони України під час реалізації Стратегії кібербезпеки України. Водночас, наявність міцного законодавчого підґрунтя та вчасна адаптація останнього до нових кібервикликів сучасності, очікувано, підвищить спроможність України ефективно стримувати деструктивні дії в кіберпросторі. Ці та інші питання особливо актуалізуються для нашої держави зараз – у період війни, зокрема, кібервійни. Як пишуть дослідники Онищенко С. та Глушко А. з початку 2022 року, лише у січні було виявлено 6,8 млн підозрілих кіберподій в частині інформаційної безпеки, 25,5 тис. потенційних кіберінцидентів та зупинено 121 кібератаку. За січень-лютий 2022 року на об'єкти критичної інфраструктури та державні інформаційні ресурси України було здійснено 436 кібератак у порівнянні з 64 за такий же період 2021 року [4, с. 14].

Станом на 2 січня 2023 року, за даними Державної служби спеціального зв'язку та захисту інформації України від початку повномасштабного воєнного вторгнення росії в Україну Урядовою командою реагування на комп'ютерні надзвичайні події CERT-UA було зареєстровано та досліджено понад 1 500 кібератак, більшість із яких зафіксовано з боку держави-терористки. У період від вересня по грудень 2022 року в Україні діяло шість російських та проросійських хакерських угрупувань. Серед головних цілей хакерів: шпіонаж в частині отримання розвідданих щодо логістики, озброєння, планів та операцій Сил безпеки та оборони; спроби виведення з ладу об'єктів критичної інфраструктури; позбавлення доступу громадян до державних послуг та сервісів, банківського обслуговування, та ряд інших [5].

Реалії сьогодення зумовили створення та постійне нарощення вітчизняних кібервійськ з метою як захисту критичної інформаційної інфраструктури від кібератак, так і задля реалізації превентивних наступальних кібероперацій (до прикладу, DDoS-атаки на корпоративні, новинні та державні сайти противника, виведення з ладу критично важливих об'єктів інфраструктури росії, компроментація баз даних телекомунікаційних, роздрібних та урядових організацій, й інше). Вже з перших днів війни добровольча ІТ-армія України налічувала 175 тис учасників з усього світу: від білих хакерів та хактивістів до представників різних технологічних компаній, серед яких, зокрема, SpaceX, а також міжнародна сітка активістів і хакеристів Anonymous Collective. Парадокс ситуації, що склалася полягав у тому, що досі жодному уряду в світі не вдавалося завербувати названих незалежних іноземних суб'єктів (кандидатів) до настільки глобального волонтерського кіберутворення та ще й добровільно.

Незважаючи на те, що в Збройних силах України вже є кібервійська, котрі реально працюють, останні досі перебувають на етапі формалізації у правовому полі та складаються здебільшого із самоорганізованих добровольців та представників різних держорганів. Як зазначає Міністр оборони України з питань цифрового розвитку, цифрових трансформацій і цифровізації Олег Гайдук – станом на нині розробляються проєкти декількох законодавчих актів, котрі незабаром будуть внесені на розгляд до Верховної Ради України. І тут мова йде вже не стільки про кібервійська, скільки про створення кіберсил, адже саме поняття «кіберсили» – набагато ширше й більше відповідає функціоналу, і якраз про них йтиметься у «великому законопроєкті» [6].

Окрім цього, з метою покращення системи кібербезпеки у державі було прийнято рішення щодо внесення законодавчих змін до статей 361 та 361-1 Кримінального кодексу України [7], спрямованих на легітимізацію процедури Bug Bounty. Узаконення цієї програми на державному рівні дасть можливість залучити зовнішніх фахівців до пошуку помилок і вразливих точок у державних програмних продуктах, урядових сайтах та інших ресурсах. А в Держспецзв'язку зазначають, що найближчим часом в органах державної влади та на об'єктах критичної інформаційної інфраструктури заплановано створення посад «офіцерів із кіберзахисту», котрим підпорядковуватимуться служби захисту інформації [8]. Що, на нашу

думку, є справді необхідним, адже якщо навіть у маленьких ІТ-компаніях є хочаб один тестувальник ПЗ (фахівець, котрий тестує готове програмне забезпечення на наявність багів/помилок, та усуває їх), то цілком виправданою виглядає необхідність в створенні чогось схожого (офіцерів із кіберзахисту) для сайтійв кожного з відомств. Кіберофіцери були б також корисними для запобігання, відбиття чи аналізу хакерських атак ворога, однак питання основних функціональних обов'язків й розміру заробітної плати все ще залишається відкритим. Очевидним ж є те, що зарплатня повинна бути не нижче ринкової, інакше марно сподіватися на залучення справді компетентних фахівців в професію.

Варто додати, що діяльність Кіберполіції через російське вторгнення в Україну також зазнала чималих змін. Серед іншого, збільшилося число функціональних обов'язків та/або завдань кіберполіцейських. Окрім цього, в частині програмування та розумних ІТ-рішень кіберполіції спільно із волонтерами та іноземними партнерами вдалося розробити:

– телеграм-бот «Народний месник» – офіційний чатбот України для повідомлення про ворожі дії на території нашої держави. Спеціально створений для реагування Національної поліції та Збройних сил України на повідомлення громадян про: виявлені ворожі мітки, пересування техніки чи живих сил ворога, виявлення не розірваних боєприпасів, мародерів та диверсантів [9];

– телеграм-канал "StopRussiaChannel | MRIYA" [10] та телеграм чат-бот "StopRussia | MRIYA" [11]. Як складові частини екосистеми "MRIYA" – розроблені спеціально для перевірки та блокування диверсійних ресурсів тобто таких, котрі поширюють фейки та пропаганду. Окрім цього, на означених платформах можна знайти інструкції для боротьби з ворогом на інформаційному фронті та надсилати скарги на небезпечний, почасти, фейковий чи проросійський контент у соцмережах та месенджерах;

– он-лайн ресурс "DefenseUa" [12], що допомагає ворожим військовим-загарбникам знайти детальну інструкцію про те, як відмовитися від участі у кривавій війні проти України та/або вступити до лав Збройних сил України.

– інші офіційні сервіси, вебресурси, сайти, інструменти та ІТ-механізми зокрема, для накопичення інформації про публічних людей, котрі своїми діями підтримують російське вторгнення, окремо, для надання можливості здійснювати голосування громадянам з території російської федерації щодо припинення війни, для здійснення розпізнавання облич російських загарбників, тощо.

Висновок. Національна система кібербезпеки України перебуває лише в процесі становлення, однак російським кіберзагарбникам досягти стратегічної мети й завдати значної шкоди критичній інфраструктурі нашої країни не вдається. Правда в тому, що росія недооцінила Україну не тільки у військовій, але й у кіберсфері. Створення кіберсил – це наступний важливий крок, навіть попри те, що ще з початку війни фахівці в сфері ІТ-технологій з усієї країни долучилися до кіберполіції, чим обумовили створення вже діючої кіберармії. Варто підкреслити, що виконання зазначених в цьому дослідженні рекомендацій стосовно нарощення кіберпотужностей гарантовано виведе Національний індекс кіберезпеки (NCSI) України у лідируючі позиції в світі. Однак, спершу варто докласти зусиль для реформування вітчизняного законодавства в кіберсфері, з метою наділення його здатністю гнучко адаптуватися до нових змін безпекового середовища, що в свою чергу, гарантуватиме злагоджене функціонування національного сегмента кіберпростору в цілому.

ЛІТЕРАТУРА

1. Перспективні технології. URL : https://uk.wikipedia.org/wiki/Перспективні_технології.
2. Про національну безпеку України: Закон України від 21 червня 2018 року № 2469-VIII. URL : https://zakon.rada.gov.ua/laws/show/2469-19#Text.
3. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовтня 2017 року № 2163-VIII. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text.
4. Онищенко С., Глушко А. Аналітичний вимір кібербезпеки України в умовах зростання викликів та загроз. Economic security of the state and economic entities. Економіка і регіон. Національний університет ім. Юрія Кондратюка. № 1 (84). 2022 р. С. 13–20.
5. Які російські та проросійські хакери атакують Україну. Державна служба спеціального зв'язку та захисту інформації України. Державні сайти України. URL : https://cip.gov.ua/ua/news/yaki-rosiiski-ta-prorosiiski-khakeri-atakuyut-ukrayinu.
6. АрміяInform. У ЗСУ фактично вже є кібервійська, вони реально працюють – Олег Гайдук. URL : https://armyinform.com.ua/2022/11/22/u-zsu-faktychno-vzhe-ye-kibervijska-vony-realno-praczyuyut-oleg-gajduk/.
7. Кримінальний кодекс України: Закон України від 05 квітня 2001 року № 2341-III. URL : https://zakon.rada.gov.ua/laws/show/2341-14#top.
8. The Village Україна. В Україні узаконять процедуру Bug Bounty та створять посаду офіцера з кібербезпеки. URL : https://www.the-village.com.ua/village/city/city-news/321781-v-ukrayini-uzakonyat-protseduru-bug-bounty-i-stvoryat-posadu-ofitsera-z-kiberbezpeki?from=readmore.
9. «Народний месник». Офіційний чат-бот України для повідомлення про ворожі дії на території нашої держави. URL : https://t.me/ukraine_avanger_bot.
10. "StopRussiaChannel | MRIYA". Офіційний телеграм-канал України для перевірки і блокування ресурсів, які поширюють фейки та пропаганду. URL: https://web.archive.org/web/20220601090556/https://t.me/stoprussiachannel.
11. "StopRussia | MRIYA". Офіційний чат-бот України. URL : https://web.archive.org/web/20220601115228/https://t.me/stopdrugsbot.
12. DefenseUa. URL : https://www.defenseua.com.