УДК 004.056.5:343.326(045)

ТРОФИМЕНКО Олена Григорівна
ПРОКОП Юлія Віталіївна
ЛОГІНОВА Наталія Іванівна
ЗАДЕРЕЙКО Олександр Владиславович

МОНІТОРИНГ РІВНЯ КІБЕРБЕЗПЕКИ УКРАЇНИ У СВІТОВИХ РЕЙТИНГАХ

Постановка проблеми. Реалії сьогодення свідчать про те, що кіберзагрози еволюціонують в прискореному темпі, вони стають досконалішими, краще організованими і транснаціональними. Це зумовлено тим, що інтернет, цифрові послуги, інформаційно-комунікаційні технології (далі – ІКТ) стали невід'ємною частиною економіки в усьому світі: від електронного документообігу, інтернет-магазинів та онлайн-банкінгу до систем Інтернету речей та інтелектуальних систем управління підприємствами. Зі зростанням залежності від використання ІКТ у бізнесі та підприємництві відповідно зростають кіберризики і кіберзагрози, що потребує завчасного реагування щодо їх запобігання або вирішення та обізнаності з факторами ризику всіх зацікавлених сторін. Система кібербезпеки має працювати в інтересах громадськості як для постачальників послуг, так і для користувачів послуг. Саме держава як гарант прав і свобод громадян має взяти на себе відповідальність за забезпечення доступу до стабільного безпечного цифрового простору, яким можуть скористатися всі громадяни, адже забезпечення належного рівня кібербезпеки є необхідною умовою розвитку інформаційного суспільства.

Аналіз останніх досліджень і публікацій. Важливості питань інформаційної безпеки нашої країни і формуванню механізму міжнародної кібербезпеки приділяли увагу численні науковці. Так, Г. А. Піскорська та Н. Л. Яковенко у своїй роботі [1] дійшли висновку, що забезпечення міжнародної безпеки в інформаційній сфері та у світовому кіберпросторі вимагає не лише зусиль окремих країн світу, а й розроблення та реалізації максимально ефективних міжнародних інструментів. І. В. Діордіца [2] пропонує для розроблення дієвого механізму протидії кіберзагрозам в Україні взяти за приклад наявну практику зарубіжних країн і міжнародної спільноти та привести її у відповідність до українських реалій. Аналіз останніх досліджень і публікацій свідчить про те, що певні аспекти вітчизняних проблем інформаційної безпеки досліджувались у наукових працях І. В. Арістова, І. Р. Березовської, О. П. Дзьобаня, Р. А. Калюжного, Б. А. Кормича, В. А. Ліпкана,

А. І. Марущака, В. С. Цимбалюка, О. К. Юдіна та інших. Проте ці дослідження здебільшого зосереджені на сфері правового регулювання та формування системи інформаційної безпеки України.

Нині побудова дієвої системи кібернетичної безпеки України в умовах гібридної війни вимагає чіткого аналізу вже реалізованих заходів у сфері захисту комп'ютерних і телекомунікаційних мереж від кібератак та визначення потрібних для реалізації заходів щодо створення умов для безпечного функціонування кіберпростору задля випереджального реагування на динамічні зміни, що відбуваються у кіберпросторі.

Метою статті є моніторинг рівня кібернетичної безпеки нашої країни, висвітлення основних проблем розбудови національної системи кіберзахисту та визначення напрямів їх вирішення.

Виклад основного матеріалу. Упродовж останніх років через кібератаки нашій країні були завдані значні матеріальні та репутаційні збитки [3; 4]. Наша держава дорогою ціною зрозуміла неприпустимість зневажання питаннями власної кібербезпеки, позаяк стала полігоном сучасної кібервійни. Лише у 2018 році українські спеціалісти з кібербезпеки змогли заблокувати понад 400 кібератак. Окремі з них, за інформацією СБ України, могли бути за наслідками не менші, ніж віруси Petya, WannaCry та BadRabbit [5]. Крім значних матеріальних збитків, через втрату або спотворення стратегічно важливої інформації, кібератаки можуть спровокувати техногенні катастрофи, збитки цивільної, фінансової та військової інфраструктури, аж до втрати суверенітету держави [6]. Саме тому гарантування кібербезпеки є надзвичайно актуальним для України, а заходи з протидії викликам і загрозам у цій царині мають носити комплексний характер, позаяк кібербезпека повинна бути невід'ємною частиною технічного прогресу.

Усвідомлюючи важливість боротьби з кіберзлочинністю, не лише Україна, а й більшість країн світу скоригували політику своїх урядів, розробили відповідні законодавчі акти і прийняли національні стратегії кібербезпеки [7; 8], адже кібервійни транснаціональні і не мають кордонів.

Різноманітні індикатори реалізованих заходів у сфері захисту комп'ютерних і телекомунікаційних мереж від кібератак та створення умов для безпечного функціонування кіберпростору оцінюються і використовуються для моніторингу та порівняння стану кібербезпеки різних країн світу у щорічних міжнародних рейтингах, найбільш авторитетними з яких є «Глобальний індекс кібербезпеки» (Global Cybersecurity Index, GCI) та «Національний індекс кібербезпеки» (National Cyber Security Index, NCSI). Зазначені індекси кібербезпеки є своєрідними показниками ризику для корпоративної, промислової та урядової інформаційної інфраструктури через спектр кіберзагроз.

Відповідно до даних рейтингу GCI-2018 Україна посіла 54 місце з-посеред 193 країн, піднявшись за останній рік на 5 позицій [9]. При цьому фахівці відзначили: прогресивні кроки у побудові законодавчої бази для гарантування кібербезпеки держави; стійкість державних ініціатив щодо підвищення кібербезпеки у сфері ІКТ; значне покращення кіберстійкості організацій за останній рік, незважаючи на збільшення більш ніж удвічі цілеспрямованих кібератак. Проте, якщо у цьому рейтингу порівняти показники України з показниками, наприклад, країн пострадянського простору, то стає зрозуміло, що чимало з них провели набагато кращу роботу з побудови кіберстійкості, позаяк вони суттєво випередили нас у цьому рейтингу. Так, Литва посіла 4 позицію загального рейтингу, Естонія – 5, Грузія – 18, Російська Федерація – 26, Казахстан – 40, Латвія – 44, Молдова – 53 і обійшли нас у рейтингу GCI-2018.

Рейтинг NCSI вимірює готовність країн до запобігання кіберзагрозам та керування кіберінцидентами і може бути використаний для вдосконалення національних можливостей кібербезпеки. Відповідно до показників глобального індексу NCSI-2018 Україна посіла 26 позицію. Країни пострадянського простору, які випередили нас у цьому рейтингу, зайняли такі місця: Естонія – 2, Литва – 4, Латвія – 17, Грузія – 21, Російська Федерація – 23 [10]. Експерти рейтингу NCSI зосереджували увагу на вимірюваних аспектах кібербезпеки, впроваджених центральними урядами країн. Щодо нашої країни було відзначено гарні напрацювання у сфері запровадження політики кібербезпеки, захисту персональних даних, боротьби з кіберзлочинністю. Проте слабкими зазначено позиції управління інцидентами та кіберкризами, захисту електронних сервісів, аналізу та інформування громадськості про кіберзагрози.

Фахівці обох наведених рейтингів відзначили те, що наша країна зробила значні прогресивні кроки для забезпечення кібербезпеки держави. Проаналізуємо реалізовані заходи у сфері створення умов для безпечного функціонування кіберпростору.

Задля поглиблення міжнародного співробітництва і гармонізації нормативних документів у сфері кібербезпеки, відповідно до міжнародних стандартів і стандартів ЄС та НАТО, Україна ратифікувала Конвенцію Ради Європи про кіберзлочинність та інші міжнародні договори, оскільки на міжнародному рівні кібербезпека є спільною відповідальністю, яка вимагає комплексного забезпечення безпечної і стійкої цифрової сфери.

За підтримки трастового фонду НАТО створено Ситуаційні центри [11] при СБУ та ДССЗЗІ, на які покладено завдання з виявлення, запобігання та нейтралізації акцій кібернетичного характеру проти України. Завдяки цьому в Національній поліції

України діє Національний контактний пункт формату 24/7 щодо реагування та обміну інформацією про комп'ютерні злочини.

З метою посилення стійкості критичної національної інфраструктури з кібербезпеки український Уряд бере участь у міжнародному співробітництві з реагування на кіберінциденти, маючи доступ до передового міжнародного досвіду та сучасних алгоритмів протидії кібератакам. Серед останніх заходів – участь у міжнародних навчаннях з кібероперацій CWIX-2018 [12]. Саме розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, участь у заходах зі зміцнення довіри у кіберпросторі, які проводяться під егідою ОБСЄ, та поглиблення співпраці України з ЄС та НАТО посилюють спроможності України у сфері кібербезпеки і відповідають національним інтересам. Так, у плані заходів на 2019 рік з реалізації Стратегії комунікації у сфері європейської інтеграції на 2018–2021 роки [13] заплановано проведення інформаційної кампанії з поглиблення співпраці з ЄС у сфері кібербезпеки.

У рамках взаємодії з міжнародними організаціями з питань реагування на кіберінциденти було організовано участь України у Форумі команд реагування на інциденти інформаційної безпеки FIRST (Forum for Incident Response and Security Teams), що об'єднує різні групи CERT (Computer Emergency Response Team – Команда реагування на надзвичайні ситуації) у країнах Європи.

Проте казати про достатність виконуваних нині заходів було б перебільшенням. Адже показники міжнародних рейтингів NCSI та GCI свідчать, що наша держава ще далеко не є лідером з першої десятки, хоча і є визнаним полігоном сучасної кібервійни [14].

Забезпечення кібербезпеки можливе тільки за рахунок комплексного і безперервного застосування організаційно-правових та технічних методів захисту на різних рівнях реалізації. З метою вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в протиправних та воєнних цілях країна має активізувати участь в організації спільних міжнародних проєктів з нарощування кібернетичного потенціалу.

Україна має продовжувати застосовувати європейські і міжнародні стандарти у сфері кібербезпеки, розвивати роботу відповідних органів, які здатні ефективно взаємодіяти з відповідними органами ЄС і НАТО. Досвід України дозволяє їй бути не лише реципієнтом допомоги від ЄС і НАТО, а й джерелом нових знань, навичок і способів протидії сучасним кіберзагрозам [15].

Важливо підвищувати рівень обізнаності щодо кібербезпеки на всіх рівнях: від діючих центрів комп'ютерної безпеки до розгортання відповідних освітніх програм. За умов небезпек, що склалися нині у кіберпросторі, організаціям потрібно змінити

ставлення до інформаційної безпеки. А для цього треба підвищувати обізнаність про важливість інвестування у кібербезпеку як невід'ємну складову будь-якої національної стратегії розвитку ІКТ.

У нинішній політичній ситуації вкрай важливо посилити кібербезпеку виборчих систем та критичної інфраструктури, сприяти реалізації Стратегії кібербезпеки України, посилювати реагування на кіберінциденти. Доцільно докласти більше зусиль для встановлення державно-приватного партнерства, розроблення та запровадження механізму обміну інформацією між державними органами, приватним сектором і громадянами стосовно загроз критичній інформаційній інфраструктурі. Задля своєчасного реагування на кіберінциденти і здійснення заходів зі зміцнення володіння ситуацією у кіберпросторі важливо організовувати проведення тренінгів з підготовки висококваліфікованих фахівців у галузі кібербезпеки та цифрової криміналістики із залученням міжнародних фахівців.

Потрібні координація та переорієнтація наукових досліджень і розробок у сфері комп'ютерної безпеки, в області вдосконалення інформаційних технологій, використання математичних методів багатовимірного аналізу даних, розробленні технологій комплексного захисту апаратних і програмних платформ, технологій виявлення ознак кібернетичного нападу з використанням активних і пасивних методів та датчиків спостереження, створення систем контролю, які визначатимуть факт скоординованого широкомасштабного нападу і формуватимуть ранні попередження про можливу атаку та локалізацію джерела загрози [16].

Приділяти увагу треба розвитку безпечної і повсюдної електронної ідентифікації, що полегшить транскордонне використання онлайн-послуг та створить умови для інтеграції України у світовий електронний інформаційний простір. Слід посилити контроль за дотриманням вимог законодавства щодо унеможливлення доступу зловмисників до конфіденційних даних споживачів та забезпечення анонімності при електронній ідентифікації за рахунок впровадження новітніх технічно-програмних рішень реалізації електронних транзакцій.

З масовим розповсюдженням технології Інтернету речей, переходом у хмарні сховища даних, формуванням обліку FinTech, зокрема цифрових та криптовалют, криптобірж, електронних виборів та «розумних контрактів», для зниження небезпечних вразливостей треба ретельно захищати метадані від можливого викрадення унаслідок зловмисних атак.

Організаціям доцільно фінансувати та впроваджувати проривні технології автоматизованого захисту, які підтримуватимуть автоматизовані можливості управління та розширену поведінкову аналітику. Прикладами таких технологій можуть бути засоби штучного інтелекту для аналізу біометричних ідентифікаційних даних,

складні алгоритми машинного навчання, здатні створювати профіль типової поведінки користувача, визначати незвичні закономірності діяльності та виявляти потенційні загрози в режимі реального часу, перш ніж зловмисники матимуть можливість реалізувати їх. Завдяки автоматичній ідентифікації підозрілих даних, увесь процес дотримання безпеки стане більш ефективним, а сама кібербезпека позбавиться потреби в кропіткому ручному огляді журналу даних. Досвід показує [17], що інвестиції у кібербезпеку окупаються і навіть дають своєрідні дивіденди, позаяк дозволяють уникнути неминучої шкоди і наслідків, завдяки чому організації виходять у бізнес-лідери, а завчасні витрати є нижчими, ніж активне інвестування після атак або злочинних дій.

Висновки. Проведений моніторинг рівня кібербезпеки України у світових рейтингах та аналіз заходів у сфері захисту кіберпростору показав, що проблема ефективного забезпечення кібербезпеки потребує комплексного вирішення і вимагає скоординованих дій на національному, регіональному та міжнародному рівнях для запобігання, підготовки, реагування та відновлення інцидентів з боку органів влади, приватного сектору та громадянського суспільства. Сучасні інформаційні загрози підкреслюють нагальну потребу у співпраці між державами для запобігання постійним загрозам в Інтернеті, забезпечення кращого розслідування, затримання і переслідування зловмисних агентів, подолання проблем кібербезпеки. Саме тому міжнародні зусилля у посиленні кібербезпеки та захисту критично важливих інформаційних інфраструктур мають бути узгоджені та діяти у відповідь на ці нові тенденції в глобальному русі до цифрової економіки та інформаційного суспільства.

Список використаних джерел

1. Піскорська Г. А. Сучасні виклики і загрози в кіберпросторі: формування механізму міжнародної інформаційної безпеки / Г. А. Піскорська, Н. Л. Яковенко // Міжнародні відносини. Серія «Політичні науки». – 2018. – № 18–19 [Електронний ресурс]. – Режим доступу : http://journals. iir. kiev.ua/index.php/pol_n/article/view/3389.

2. Діордіца І. Поняття і зміст кіберзагроз на сучасному етапі / І. Діордіца // Адміністративне право і процес. – 2017. – № 4. – С. 99–107.

3. Трофименко О. Г. Моніторинг стану кібербезпеки в Україні / О. Г. Трофименко // Правове життя сучасної України : матер. міжнар. наук.-практ. конф. : у 2 т. – Т. 1. – Одеса : Видавничий дім «Гельветика», 2019. – Т. 1. – С. 642–646.

4. Трофименко О. Г. Законодавча база забезпечення кібербезпеки держави / О. Г. Трофименко // Кібербезпека в Україні: правові та організаційні питання : матер. ІІ Всеукр. наук.-практ. конф. (17 листопада 2017 р.). – Одеса : ОДУВС. – С. 55–56.

5. Українські спеціалісти з кібербезпеки змогли заблокувати близько 400 кібератак у 2018 році [Електронний ресурс]. – Режим доступу : https://www.ukrinform.ua/rubric-technology/2638599-v-ukraini-torik-zablokuvali-majze-cotiri-sotni-kiberatak.html.

6. Трофименко О. Г. Щодо правового потенціалу безпечного функціонування кіберпростору / О. Г. Трофименко, Я. В. Дубовой // Кібербезпека в Україні: правові та організаційні питання : матер. III Всеукр. наук.-практ. конф. (30 листопада 2018 р.). – Одеса: ОДУВС. – С. 5–7.

7. National Strategies [Електронний ресурс]. – Режим доступу : https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx.

8. Трофименко О. Г. Еволюція поглядів на інформаційні війни в епоху інформаційного суспільства / О. Г. Трофименко, Я. В. Дубовой // Порівняльно-аналітичне право: електронне наукове фахове видання. – 2017. – № 1. – С. 189–192 [Електронний ресурс]. – Режим доступу : http://www.pap.in.ua/1_2017/58.pdf.

9. Global Cybersecurity Index (GCI) 2018 [Електронний ресурс]. – Режим доступу : https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf.

10. National Cyber Security Index (NCSI) 2018 [Електронний ресурс]. – Режим доступу : https://www.ncsi.ega.ee/ncsi-index/.

11. Співробітництво Україна – ЄС – НАТО з протидії гібридним загрозам у кіберсфері / Центр глобалістики «Стратегія XXI» [Електронний ресурс]. – Режим доступу : https://geostrategy.org.ua/images/kiber_UA_A5.pdf.

12. В рамках багатонаціональних навчань CWIX-2018 у польському місті Бидгощ відбувся День високоповажних гостей [Електронний ресурс]. – Режим доступу : http://www.mil.gov.ua/news/2018/06/27/v-ramkah-bagatonaczionalnih-navchan-cwix-2018-u-polskomu-misti-bidgoshh-vidbuvsya-den-visokopovazhnih-gostej/.

13. Про затвердження плану заходів на 2019 рік з реалізації Стратегії комунікації у сфері європейської інтеграції на 2018-2021 роки [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/83-2019-р.

14. Про «священну корову» української кібербезпеки: Наскільки дієва міжнародна кібердопомога? [Електронний ресурс]. – Режим доступу : https://www.ukrinform.ua/rubric-technology/2567808-pro-svasennu-korovu-ukrainskoi-kiberbezpeki-naskilki-dieva-miznarodna-kiberdopomoga.html.

15. Співробітництво Україна – ЄС – НАТО з протидії гібридним загрозам у кіберсфері. – Київ, 2019. – 28 с. [Електронний ресурс]. – Режим доступу : https://geostrategy.org.ua/ua/analitika/item/1565-cooperation-ukraine-nato.

16. Трофименко О. Г. Щодо правового потенціалу безпечного функціонування кіберпростору. / О. Г. Трофименко, Я. В. Дубовой // Кібербезпека в Україні: правові та організаційні питання: матер. III Всеукр. наук.-практ. конф. (30 листопада 2018 р.). – Одеса : ОДУВС. – С. 5–7.

17. Впровадження європейської кібербезпеки: загальний огляд. / ISACA [Електронний ресурс]. – Режим доступу : https://www.isaca.org/Knowledффge-Center/Research/Documents/European-Cybersecurity-Implementation-Overview_res_Ukr_1215.pdf.

Державна політика України у сфері забезпечення інформаційної безпеки людини, суспільства, держави

Рецензенти:
доктор фізико-математичних наук,
доктор юридичних наук, професор
М. Василенко,
доктор технічних наук, професор
О. Балтовський

Аннотация. Работа посвящена мониторингу уровня кибербезопасности Украины в мировых рейтингах. Внимание авторов было сосредоточено на анализе основных проблем построения национальной системы киберзащиты с учётом международного опыта. По мнению авторов, обеспечение кибербезопасности страны возможно только при комплексном и непрерывном применении организационно-правовых и технических методов защиты не только на национальном, но и на международном уровне. Международное сотрудничество позволит обеспечить надлежащий уровень кибербезопасности и защитить информационные инфраструктуры в современных условиях развития информационного общества.

Ключевые слова: кибербезопасность, кибератака, киберинциденты, киберугрозы, информационная безопасность, стратегия кибербезопасности.

Abstract. The article is devoted to monitoring of the level of cybersecurity of Ukraine in world rankings. The authors' attention was focused on analyzing the main problems of building a national cyber defense system, considering international experience. According to the authors, ensuring the cybersecurity of the country is possible only with the comprehensive and continuous use of legal and technical methods of protection not only at the national, but also at the international level. International cooperation will ensure an adequate level of cybersecurity and protect information infrastructures in modern conditions of the information society development.

Key words: cybersecurity, cyberattacks, cyber incidents, cyberthreat, information security, cybersecurity strategy.