УДК 351.865(477)
DOI https://doi.org/10.32782/app.v70.2022.16

А. В. Козьміних
orcid.org/0000-0002-5873-1178
кандидат політичних наук, доцент,
доцент кафедри політичних теорій
Національного університету «Одеська юридична академія»

А. М. Прохоренко
orcid.org/0000-0002-8662-9322
кандидат політичних наук,
старший викладач кафедри політичних теорій
Національного університету «Одеська юридична академія»

ЗАГАЛЬНА ХАРАКТЕРИСТИКА ОСОБЛИВОСТЕЙ ТА ПРОБЛЕМ КІБЕРБЕЗПЕКИ В СУЧАСНІЙ УКРАЇНІ

Інформаційно-комунікаційні технології, стали все більш важливим аспектом глобального соціального, політичного та економічного життя протягом останніх двох десятиліть і є основою глобального інформаційного суспільства сьогодні. Їх еволюція та розвиток є перевагою для окремих особи, а також безлічі державних і приватних установ і акторів. Однак інформаційно-комунікаційні технології також створили загрозу серйозних кібератак, що було продемонстровано в останні роки через акти кібершпигунства та кіберзлочинності (Cybersecurity in the European Union, 2016).

Кіберпростір та його базова інфраструктура вразливі до широкого спектру ризиків, що виникають від кіберзагроз і небезпек. Окремі досвідчені кіберзлочинці та національні держави використовують вразливі місця для викрадення інформації та грошей і розвивають можливості, щоб переривати, знищувати або створювати загрози для надання основних послуг. Кіберпростір особливо важко захистити через низку факторів: здатність зловмисників діяти з будь-якої точки світу, зв'язки між кіберпростором і фізичними системами, а також складність зменшення вразливості та наслідків у складних кібермережах. Дедалі більше занепокоєння викликає кіберзагроза для критично важливої інфраструктури, яка все частіше піддається складним кібервторгненням, що створює нові ризики (CISA's Role). Оскільки інформаційні технології все більше інтегруються в роботу фізичної інфраструктури, зростає ризик широкомасштабних або серйозних подій, які можуть завдати шкоди або порушити роботу послуг, від яких залежить економіка та повсякденне життя мільйонів американців. У світлі ризиків і потенційних наслідків кібернетичних подій існують окремі інститути, що зміцнюють безпеку та стійкість кіберпростору, що є важливою місією внутрішньої безпеки України.

Проблема поглибленого дослідження природи та сутності елементів і концептуальних засад кібербезпеки, її ефективності визначає необхідність розробки єдиного, комплексного підходу до формування ефективних систем і механізмів кібербезпеки, необхідність розробки та запровадити кібербезпеку (Бубнов, Гусейнова, 2022, с. 758).

Від початку війни стало відомо про велику кількість кібератак на українські ресурси. Атака на Україну російських хакерів почалася за кілька хвилин до масованого вторгнення армії. Як повідомляє Reuters, США, Велика Британія та Євросоюз офіційно звинуватили рф у здійсненні масової кібератаки 24 лютого 2022 року, яка призвела до збою в роботі супутникового інтернет-сервісу Viasat за годину до початку війна. Це спричинило знищення «десятків тисяч» супутникових терміналів (Війна росії проти України).

Також важливим фактом є те, що до початку бойових дій, після відомої кібератаки на сайти державних органів 14 січня 2021 року, виникла реальна потреба в термінових змінах та легалізації на рівні українського законодавства. Процедура Bug Bounty (залучення сторонніх спеціалістів для пошуку помилок та вразливостей у програмних продуктах, інформаційно-комунікаційних системах тощо) (Турчинов, 2022).

Сьогодні ІТ-спільнота може легально легко перевірити всі необхідні державні інформаційні системи на вразливості, а сама держава вживає термінових заходів для істотного підвищення ступеня захисту таких систем.

Зазначимо, що з початком війни в Україні активізувався неофіційний громадський рух кіберопору ворогу під назвою «Кіберармія» (Боротьба з кіберзлочинністю). Звичайні люди разом з ІТ-фахівцями завдають нищівного удару по ворогу в кіберпросторі, атакуючи, завдаючи шкоди та зриваючи плани. У військовій ситуації кожен повинен звернути увагу на такі контрольні точки: 1. Намагайтеся вивчати та активно аналізувати слабкі місця вашого кіберзахисту, щоб зміцнювати їх щодня. В Україні хакери завжди проводять багато спецоперацій.

Таким чином, вони знаходять найслабші місця в захисті наших компаній і атакують їх за допомогою цього. Немає такого поняття, як 100% безпечна система. Варто зауважити, що чим більше я обманюю, тим гіршою буде моя мотивація. Тим, хто перебуває в зоні кіберризику, слід обов'язково стежити за відповідними повідомленнями на різних офіційних ресурсах Держспецзв'язку та CERT-UA. Ці органи першими публікують офіційні попередження не лише про можливі кіберзагрози, а й про те, як мінімізувати їхні ризики (Комітет з питань цифрової трансформації).

Завжди потрібно пам'ятати про систему безпеки, яка залежить конкретно і абсолютно точно від кожного співробітника (Мальцева, Черниш, Штонда, 2022). Хакери можуть знищити компанію або створити її через співробітників різних компаній і викрасти їхні дані. Є особлива небезпека – військова, як і всі сили. Ця категорія людей повинна повністю звикнути до кіберпростору і прийняти його як норму повсякденного життя, щоб не мати серйозних наслідків.

Успішність запобігання кіберзлочинам, їх викриття та притягнення винних осіб до відповідальності наразі є «достатньо рідкісним явищем, якщо порівнювати з кількістю таких правопорушень» (Нікулеску, 2019).

Отже, науковий інтерес також має надання рекомендацій щодо переліку дії, необхідних для забезпечення кібербезпеки, до яких віднесено (Котух, 2020):

Створення довіри в Інтернеті. При розробці стратегії кібербезпеки рекомендують, щоб розробка політики була зосереджена на зміцненні довіри зацікавлених сторін у мережевому середовищі або на зміцненні довіри в Інтернеті. Це означає не лише надання зацікавленим сторонам (споживачам, підприємствам та уряду) довіри до онлайн-форми, але й забезпечення доступності інфраструктури. Цього можна досягти, наприклад, шляхом створення основи для захисту даних і регулювання конфіденційності, розробки національного плану управління надзвичайними ситуаціями в кіберпространстві, управління національними кризами та забезпечення захисту важливої інформації. Виникненню довіри в Інтернеті часто сприяють такі фактори: – збільшення цифрової переваги. – захист критичних активів (таких як конфіденційність, дані та інфраструктура) у кіберпросторі; – сприяння конфіденційності в Інтернеті: захист особистої інформації від несанкціонованого доступу та розголошення.

Координація, кооперація та співпраця. Враховуючи широкий спектр необхідних засобів захисту кібербезпеки, включаючи захист на індивідуальному, громадському, організаційному, національному та міжнародному рівнях, а також захист глобального кіберпростору, це не може бути виконано однією організацією. Такий захист вимагає співпраці кожного учасника, а кіберпростір вимагає колективного захисту. Це означає, що кожна організація повинна постійно працювати над підтримкою (і вдосконаленням) своїх кіберможливостей, щоб стати надійним гравцем у такій системі. Існує два типи дій, рекомендованих для координації, співробітництва та співпраці (ССС). Діяльність, пов'язану з організаційними відносинами, можна розділити на зовнішню і внутрішню. До першої категорії відноситься взаємодія з іншими організаціями через кооперацію та взаємодію. Адвокація може бути досягнута, наприклад, через альянси та партнерства з іншими організаціями, посилення можливостей кібердипломатії та м'якої сили, обміну інформацією щодо протидії загрозам, сприяння інтеграції та розподілу відповідальності шляхом посилення кіберможливостей сусідніх організацій (або впровадження третьою організацією партії). Друга категорія включає посилення внутрішньої координації в організаційній структурі організації. Цей тип діяльності призначений для

покращення зв'язку з усіма зацікавленими сторонами організації, узгодження всіх зацікавлених сторін організації з мандатом кібербезпеки та встановлення кіберуправління з чіткими ролями та обов'язками.

Профілювання кібердержави. Діяльність з профілювання передбачає встановлення цілей і відповідних ресурсів, необхідних для захисту кіберпростору, які є підготовчими діями перед наступною діяльністю. Профілювання кібердержави передбачає три дії: узгодження стратегії з основними цінностями; бюджетування та підготовка відповідних ресурсів; і формулювання припущень.

Стимулювання прогресу в напрямку підтримки впровадження Стратегії безпеки. Це означає розбудову кіберпотенціалу організації шляхом сприяння прийняттю принципів SKB. Окрім КТС, важливо враховувати діяльність, пов'язану з іншими суб'єктами кіберпростору. Обнадійливий прогрес можна розглядати як важливий аспект цих відносин, оскільки бути надійною організацією в кіберпросторі має фундаментальне значення для посилення кібербезпеки. Діяльність КТС і сприяння впровадженню взаємопов'язані. Незважаючи на те, що ССС представляє зовнішні дії у співпраці з усіма організаціями та зацікавленими сторонами, головною метою сприяння реалізації є внутрішньо орієнтовані стратегічні дії для зміцнення кібердовіри організації (WEF 2012b). Такі дії можуть приймати форму підвищення обізнаності, створення кіберкультури, інвестування в дослідження та інновації, використання інноваційних технологій, підвищення реакції на кіберпроцеси, а також навчання та навчання у сфері кібербезпеки.

Перегляньте та перегляньте. Існує також необхідність переглянути діяльність із захисту кіберпростору, щоб переконатися, що програма кібербезпеки виконує свою місію. Огляд призначений для коригування стратегії та реструктуризації програми для досягнення наміченої мети. Приклади такої діяльності включають створення аудитів і журналів, отримання відгуків, проведення самооцінювання та вдосконалення програми. Окрім створення аудитів і журналів, вам потрібно оцінити діяльність. Оцінка програми може бути проведена із залученням внутрішнього або зовнішнього аудитора.

Створення правового середовища. Правове середовище забезпечує основу для поведінки в кіберпросторі, яка проводить межу між тим, що прийнятно, а що ні. Для запобігання та припинення незаконної діяльності необхідні відповідні закони та правила. Багато ССВ консультують організації щодо визначення законної поведінки та створення правового середовища. Створення правового середовища передбачає створення законодавчої бази як основи розмежування законного та незаконного.

Для тих хакерів, які щоденно здійснюють небезпечні кібератаки на ворогів і займаються багхантингом з чітким планом покращення та зміцнення кібербезпеки України в умовах воєнного часу, щоб повністю уникнути невирішених проблем із послугами правоохоронних органів, це необхідно бути повністю готовими довести, що їх діяльність відповідає інтересам.

На думку І.Р. Мальцевої, Ю. О. Черниш, Р.М. Штонди доцільно визначено, що «мега ефективна та кваліфікована протидія загрозам національній безпеці у кіберсфері стає реальною тільки за певної умови щодо комплексного використання всього арсеналу правових засобів для найкращого забезпечення кібербезпеки. Це стосується пунктів, які діють за всіма структурованими елементами державного управління та на всіх етапах обігу інформації. Можемо сміливо стверджувати, що найкращий ефект полягає у повній взаємодії суб'єктів забезпечення кібербезпеки України.

Цього можливо досягнути шляхом використання цілісних та дієвих системних механізмів, адміністративно-правових методик та різноманітних засобів, завдяки яким здійснюються реалізації державної політики у сфері повного забезпечення кібербезпеки, як складових елементу національної безпеки України» (Мальцева, Черниш, Штонда, 2022).

Отже, державні органи, державні організації разом з українськими компаніями з кібербезпеки та найважливішими світовими виробниками рішень впровадили ешелоновий кіберзахист нашої держави та бізнесу загалом. Тим не менш, необхідно продовжувати докладати зусиль, аналізувати ситуації та шукати рішення.

Література

Боротьба з кіберзлочинністю в умовах дії воєнного стану. URL: https://www.lexology.com/library/detail.aspx?g=d37e1715-7526-4626-9cde-26d1f6982c17

Бубнов, Д. В., Гусейнова, К. С. (2022). Актуальні проблеми кібербезпеки у сучасному світі. *Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття» (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права)* Одеса : Видавничий дім, 758-761.

Війна росії проти України почалася з кібернападу на супутники. за годину до вторгнення були знищені «десятки тисяч» терміналів Viasat-itc.ua. *ITC.ua.* URL: https://itc.ua/ua/novini/vijna-rosiyi-proti-ukrayini-pochalasya-z-kibernapadu-na-suputniki-za-godinu-do-vtorgnennya-buli-znishheni-desyatki-tisyach-terminaliv-viasat/

Комітет з питань цифрової трансформації інформує як посилити кіберзахист підприємствам та установам. *Офіційний сайт Верховної Ради України*. URL: https://www.rada.gov.ua/news/razom/221800.html

Котух, Є. В. (2020). Формування систем кібербезпеки в органах публічної влади. *Державне управління: удосконалення та розвиток*. URL: http://www.dy.nayka.com.ua/pdf/3_2020/32.pdf

Мальцева, І.Р., Черниш, Ю.О., Штонда, Р.М. (2022). Аналіз деяких кіберзагроз в умовах війни. *Кібербезпека: освіта, наука, техніка,* 4(16). URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/362/300

Нікулеску, Д. (2019). Кібербезпека: вразливі моменти. *Юридична газета online*. URL: http//yurgazeta.com/publcations/practice/inshe/kiberbezpeka-vrazlivi-momenti.htmlc.

О. Турчинов: Національний координаційний центр кібербезпеки повинен мобілізувати весь наявний потенціал для забезпечення надійного кіберзахисту країни. *Офіційний сайт Ради національної безпеки і оборони України*. URL: https://www.rnbo.gov.ua/ua/Diialnist/2528.html?PRINT

CISA's Role in Cybersecurity. URL: https://www.cisa.gov/cybersecurity

Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy (2016). 1st ed. Edition Palgrave Macmillan

References

Borotba z kiberzlochynnistiu v umovakh dii voiennoho stanu [Fighting cybercrime under martial law]. URL: https://www.lexology.com/library/detail.aspx?g=d37e1715-7526-4626-9cde-26d1f6982c17 [in Ukrainian].

Bubnov, D. V., Huseinova, K. S. (2022). Aktualni problemy kiberbezpeky u suchasnomu sviti [Actual problems of cyber security in the modern world]. *Yevropeiskyi vybir Ukrainy, rozvytok nauky ta natsionalna bezpeka v realiiakh masshtabnoi viiskovoi ahresii ta hlobalnykh vyklykiv XXI stolittia» (do 25-richchia Natsionalnoho universytetu «Odeska yurydychna akademiia» ta 175-richchia Odeskoi shkoly prava)* [The European choice of Ukraine, the development of science and national security in the realities of large-scale military aggression and global challenges of the 21st century" (to the 25th anniversary of the National University "Odesa Law Academy" and the 175th anniversary of the Odessa School of Law)]. Odesa : Vydavnychyi dim, 758-761. [in Ukrainian].

Viina rosii proty Ukrainy pochalasia z kibernapadu na suputnyky. za hodynu do vtorhnennia buly znyshcheni «desiatky tysiach» terminaliv Viasat-itc.ua [Russias war against Ukraine began with a cyberattack on satellites. an hour before the invasion, "tens of thousands" of Viasat-itc.ua terminals were destroyed]. *ITC.ua.* URL: https://itc.ua/ua/novini/vijna-rosiyi-proti-ukrayini-pochalasya-z-kibernapadu-na-suputniki-za-godinu-do-vtorgnennya-buli-znishheni-desyatki-tisyach-terminaliv-viasat/ [in Ukrainian].

Komitet z pytan tsyfrovoi transformatsii informuie yak posylyty kiberzakhyst pidpryiemstvam ta ustanovam [The Committee on Digital Transformation informs enterprises and institutions how to strengthen cyber protection]. *Ofitsiinyi sait Verkhovnoi Rady Ukrainy* [Official website of the Verkhovna Rada of Ukraine]. URL: https://www.rada.gov.ua/news/razom/221800.html [in Ukrainian].

Kotukh, Ye. V. (2020). Formuvannia system kiberbezpeky v orhanakh publichnoi vlady [Formation of cyber security systems in public authorities]. *Derzhavne upravlinnia: udoskonalennia ta rozvytok*. URL: http://www.dy.nayka.com.ua/pdf/3_2020/32.pdf [in Ukrainian].

Maltseva, I.R., Chernysh, Yu.O., Shtonda, R.M. (2022). Analiz deiakykh kiberzahroz v umovakh viiny [Analysis of some cyber threats in the conditions of war]. *Kiberbezpeka: osvita, nauka, tekhnika* [Cyber security: education, science, technology], 4(16). URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/362/300 [in Ukrainian].

Nikulesku, D. (2019). Kiberbezpeka: vrazlyvi momenty [Cyber security: vulnerable points]. *Yurydychna hazeta online* [Legal newspaper online]. URL: http//yurgazeta.com/publcations/practice/inshe/kiberbezpeka-vrazlivi-momenti.htmls. [in Ukrainian].

O. Turchynov: Natsionalnyi koordynatsiinyi tsentr kiberbezpeky povynen mobilizuvaty ves naiavnyi potentsial dlia zabezpechennia nadiinoho kiberzakhystu krainy [O. Turchynov: The National Cyber Security Coordination Center must mobilize all available potential to ensure reliable cyber protection of the country].

Ofitsiinyi sait Rady natsionalnoi bezpeky i oborony Ukrainy [Official website of the National Security and Defense Council of Ukraine]. URL: https://www.rnbo.gov.ua/ua/Diialnist/2528.html?PRINT [in Ukrainian].

CISA's Role in Cybersecurity. URL: https://www.cisa.gov/cybersecurity [in English].

Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy (2016). 1st ed. Edition Palgrave Macmillan. in English].

Анотація

***Козьміних А. В., Прохоренко А. М.* Загальна характеристика особливостей та проблем кібербезпеки в сучасній Україні.** – Стаття.

В статті охарактризовано особливості та проблеми кібербезпеки в сучасній Україні. Визначено, що «мега ефективна та кваліфікована протидія загрозам національній безпеці у кіберсфері стає реальною тільки за певної умови щодо комплексного використання всього арсеналу правових засобів для найкращого забезпечення кібербезпеки. Це стосується пунктів, які діють за всіма структурованими елементами державного управління та на всіх етапах обігу інформації. Можемо сміливо стверджувати, що найкращий ефект полягає у повній взаємодії суб'єктів забезпечення кібербезпеки України. Завжди потрібно пам'ятати про систему безпеки, яка залежить конкретно і абсолютно точно від кожного співробітника. Хакери можуть знищити компанію або створити її через співробітників різних компаній і викрасти їхні дані. Є особлива небезпека – військова, як і всі сили. Ця категорія людей повинна повністю звикнути до кіберпростору і прийняти його як норму повсякденного життя, щоб не мати серйозних наслідків

Доведено, що можливо досягнути шляхом використання цілісних та дієвих системних механізмів, адміністративно-правових методик та різноманітних засобів, завдяки яким здійснюються реалізації державної політики у сфері повного забезпечення кібербезпеки, як складових елементу національної безпеки України». Зазначено, що оскільки інформаційні технології все більше інтегруються в роботу фізичної інфраструктури, зростає ризик широкомасштабних або серйозних подій, які можуть завдати шкоди або порушити роботу послуг, від яких залежить економіка та повсякденне життя мільйонів американців. У світлі ризиків і потенційних наслідків кібернетичних подій існують окремі інститути, що зміцнюють безпеку та стійкість кіберпростору, що є важливою місією внутрішньої безпеки України.

Ключові слова: кібербезпека, політика кібербезпеки, Європейський Союз, кіберпростір, кіберзлочин, кіберзагрози.

Summary

Kozminykh A. V., Prokhorenko A. M. General characteristics of the features and problems of cyber security in modern Ukraine. – Article.

The article describes the peculiarities and problems of cyber security in modern Ukraine. It was determined that "a mega-effective and qualified countermeasure against threats to national security in the cyber sphere becomes real only under certain conditions regarding the comprehensive use of the entire arsenal of legal means to best ensure cyber security. This applies to items that apply to all structured elements of state administration and at all stages of information flow. We can safely say that the best effect is the full cooperation of the subjects of Ukraine's cyber security. Always remember about the security system, which depends specifically and absolutely precisely on each employee. Hackers can destroy a company or create it through employees of different companies and steal their data. There is a special danger – military, like all forces. This category of people should fully get used to cyberspace and accept it as the norm of everyday life, so as not to have serious consequences

It has been proven that it is possible to achieve through the use of integral and effective system mechanisms, administrative and legal methods and various means, thanks to which state policy is implemented in the field of full cyber security, as a component of the national security of Ukraine." It noted that as information technology becomes increasingly integrated into the operation of physical infrastructure, the risk of large-scale or severe events that could damage or disrupt services on which the economy and daily lives of millions of Americans depend increases. In light of the risks and potential consequences of cyber events, there are separate institutions that strengthen the security and stability of cyberspace, which is an important mission of Ukraine's internal security.

Key words: cybersecurity, cybersecurity policy, European Union, cyberspace, cybercrime, cyber threats.