УДК 342.9:004 *DOI: https://doi.org/10.32631/vca.2024.3.47*

Олександр Іванович ЧЕРВЯКОВ,
кандидат юридичних наук
(Інститут Служби безпеки України Національного юридичного університету імені Ярослава Мудрого, м. Харків)

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ЯК ПРОВІДНОЇ СКЛАДОВОЇ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

У статті наголошено на тому, що сучасне розуміння феномену національної безпеки постає у єдності декількох складових, які охоплюють воєнну безпеку, публічну безпеку, економічну безпеку, енергетичну безпеки, екологічну безпеку, інформаційну безпеку, державну безпеку та кібербезпеку. Остання виступає інтегруючою складовою по відношенню до всіх інших, адже у сучасних умовах використання відповідних технологій та комп'ютерних програм є основою здійснення операцій у будь-якій сфері суспільного життя.

Наголошено, що необхідно бути свідомими того, що в останні десятиліття проблема кібербезпеки суттєво трансформувалася з рівня окремого комп'ютера на рівень держави, окремих організацій, сфер економіки та об'єктів критичної інфраструктури. З огляду на це дана проблема тепер не є суто технічною, а має розглядатися саме з точки зору адміністративно-правового забезпечення функціонування цілісного механізму забезпечення кібербезпеки держави, створення відповідних інституцій, центральних органів виконавчої влади, відповідальних за даний напрямок, а також структурних підрозділів (посадових осіб) на рівні окремих підприємств, установ, організацій.

Зазначено, що до особливостей забезпечення кібербезпеки як провідної складової національної безпеки України доречно віднести формування нормативно-правової основи кібербезпеки, визначення її концептуального бачення та стратегії розвитку на рівні держави; тісний зв'язок між кібербезпекою та розвитком вітчизняної освіти; формування так званої кіберкультури як системи цінностей, стійких уявлень про сутність та значення кібербезпеки у повсякденній життєдіяльності людей, їх об'єднань та суспільства в цілому.

Ключові слова: *національна безпека України, особливості забезпечення кібербезпеки, адміністративно-правове забезпечення, кіберкультура.*

Постановка проблеми. Ми живемо в кіберпросторі з безпрецедентно швидким розширенням простору та його елементів. Уся інтерактивна інформація обробляється та обмінюється у цьому просторі. Очевидно, що добре побудована система кібербезпеки є життєво необхідною для

забезпечення безпеки кіберпростору. Однак визначення та обсяги як кіберпростору, так і кібербезпеки все ще не є чітко сформованими, і це ускладнює створення надійних моделей безпеки та механізмів для захисту цього простору[1]. Водночас сьогодні все більше банківських, торговельних та інших розрахункових чи логістичних операцій як усередині однієї країни, так і в міжнародних відносинах здійснюються з використанням сучасних комп'ютерних, телекомунікаційних та інших інноваційних технологій і пристроїв[2]. У таких умовах актуалізується осмислення кібербезпеки, як провідної складової національної безпеки України, яка постійно вдосконалюється, адаптуючись до нових викликів у кіберпросторі.

Дослідження комплексу питань, пов'язаних із забезпеченням національної безпеки держави, ставали сферою наукових пошуків таких провідних вітчизняних науковців у царині права, як В. О. Антонов, О. І. Безпалова, О. С. Бодрук, О. С. Власюк, Т. В. Вставська, О. П. Гетманець, І. І. Дейнега, П. В. Діхтієвський, О. В. Джафарова, В. П. Ємельянов, О. І. Миколенко, А. М. Михненко, А. Г. Мосейко, О. М. Музичук, В. П. Приходько, О. Ю. Салманова, В. В. Сокуренко та ін. Проте останнім часом національна безпека стає все більше пов'язаною з кібербезпекою, підходи до забезпечення якої постійно вдосконалюються в світлі актуальних кіберзагроз, що потребує проведення нових наукових пошуків, у тому числі в адміністративно-правовій доктрині.

Мета статті полягає в тому, щоб визначити основні особливості забезпечення кібербезпеки як провідної складової національної безпеки України. Для досягнення вказаної мети необхідно вирішити такі завдання: узагальнити думки вітчизняних і зарубіжних науковців щодо сутності кібербезпеки у сучасній державі; визначити та ретельно проаналізувати особливості забезпечення кібербезпеки як провідної складової національної безпеки України.

Виклад основного матеріалу. Сучасне розуміння феномену національної безпеки постає у єдності декількох складових, які охоплюють воєнну безпеку, публічну безпеку, економічну безпеку, енергетичну безпеки, екологічну безпеку, інформаційну безпеку, державну безпеку та кібербізпеку. Остання виступає інтегруючою складовою по відношенню до всіх інших, адже у сучасних умовах використання відповідних програм є основою здійснення операцій у будь-якій сфері суспільного життя. З огляду на це кібербезпека по праву може вважатися провідною складовою національної безпеки України.

Кібербезпека означає захист апаратного забезпечення, програмного забезпечення, масивів даних (інформації) від кібератак з боку зловмисників, підключених до всесвітньої мережі Інтернет систем, Забезпечення

[1] Le N., Hoang D. Can maturity models support cyber security? 35th IEEE International Performance Computing and Communications Conference (IPCCC). Las Vegas, 09–11 December 2016. URL: https://www.semanticscholar.org/paper/Can-maturity-models-support-cyber-security-Le-Hoang/2aff05eb3f7b453430ea3a60d79735b67ea1674f.

[2] Pchelina O. V., Skulysh Y. D., Buglak I., Myroniuk R. V. International experience of ensuring cybersecurity in the country and possibility of its application in Ukraine. *DIXI*. 2021. № 23 (2). P. 2.

кібербезпеки необхідне для захисту інформаційних технологій разом із комп'ютерними системами, а також захисту компаніями своїх систем та інформації від кібератак. Можливі кілька типів кібератак, як-от віруси, фішинг, троянські коні, хробаки, атаки на відмову в обслуговуванні (DDoS), незаконний доступ (наприклад, викрадення інтелектуальної власності чи конфіденційної інформації), а також атаки на систему керування[1].

Кібербезпека сьогодні є найважливішим аспектом нашого технологічно заснованого життя. Державні установи, банківський сектор, державні та приватні служби, атомні електростанції, оператори електромереж, постачальники води та очисні компанії використовують інформаційні технології у своїй повсякденній діяльності. Усе, що використовує технології, базується на комунікаційних та інформаційних системах, а це означає, що це залежить від кібербезпеки. Державний і приватний сектори щороку витрачають мільйони доларів на технології, програмне забезпечення безпеки та апаратні пристрої, які підвищують кібербезпеку в компаніях, але вони все ще вразливі. Основна проблема цієї ситуації полягає в тому, що кібербезпека все ще зазвичай розглядається як технічний аспект або технологія, яку можна легко впровадити всередині організації, і ця реалізація гарантуватиме кібербезпеку. Це ставлення має змінитися, тому що кібербезпека сьогодні – це щось більше, ніж просто технології[2].

Необхідно бути свідомими того, що в останні десятиліття проблема кібербезпеки суттєво трансформувалася з рівня окремого комп'ютера на рівень держави, окремих організацій, сфер економіки та об'єктів критичної інфраструктури. З огляду на це дана проблема тепер не є суто технічною, а має розглядатися саме з точки зору адміністративно-правового забезпечення функціонування цілісного механізму забезпечення кібербезпеки держави, створення відповідних інституцій, центральних органів виконавчої влади, відповідальних за даний напрямок, а також структурних підрозділів (посадових осіб) на рівні окремих підприємств, установ, організацій.

Американські дослідники S. Ganapati, M. Ahn, C. Reddick стверджують, що існує дихотомія у трактуванні кібербезпеки як технічної проблеми чи проблеми управління. Вчені з публічного управління вважали кібербезпеку, імовірно, технічною проблемою, хоча політика безпеки діє з середини 1980-х років. Технічні проблеми еволюціонували від проблем окремих комп'ютерів (наприклад, віруси) до проблем системної мережі (наприклад, атаки програм-вимагачів). Останні публікації демонструють розгляд кібербезпеки саме як проблеми управління[3].

---

[1] Srinivas J., Das A., Kumar N. Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems-The International Journal of Escience*. 2019. № 92. P. 178.

[2] Limba T., Pleta T., Agafonov K., Damkus M. Cyber security management model for critical infrastructure. *Entrepreneurship and Sustainability Issues.* 2017. № 4 (4). P. 559.

[3] Ganapati S., Ahn M., Reddick C. Evolution of Cybersecurity Concerns: A Systematic Literature Review. In: 24th Annual International Conference on Digital Government Research (DGO) – Together in the Unstable World - Digital Government and Solidarity. Gdansk, 11–14 July 2023. P. 90.

Окремі вітчизняні дослідники акцентують увагу на необхідності визначення ключових аспектів публічного управління для забезпечення кібербезпеки в сучасних умовах соціально-економічного розвитку. Для вирішення проблем кібербезпеки необхідна значна комунікація та координація між різними приватними та державними структурами різних країн та організацій. Метою кібербезпеки є досягнення та забезпечення того, щоб як організація, так і активи користувача залишалися в стані безпеки від загроз безпеці, ризиків у кіберсередовищі[1].

Щодо особливостей забезпечення кібербезпеки, як провідної складової національної безпеки України, то першою такою особливістю є формування нормативно-правової основи кібербезпеки, визначення її концептуального бачення та стратегії розвитку на рівні держави. Як зазначають О. Пчеліна, Є. Скулиш, Ю. Буглак, Р. Миронюк, формування надійної системи кібербезпеки держави, здатної захистити як саму державу, так і всіх без винятку суб'єктів її правовідносин, потребує вдалого поєднання кількох елементів. Так, має бути чітка та недвозначна стратегія (або план) для досягнення успіху в забезпеченні надійної системи кібербезпеки. Така стратегія має включати ряд успішних рішень, які функціонували в аналогічних стратегіях, прийнятих розвиненими країнами Західної Європи протягом останніх кількох років. Також необхідно створити відповідну нормативно-правову базу, головним завданням якої буде забезпечення ефективного та безперервного функціонування національної системи кібербезпеки. Розробку відповідних нормативно-правових актів слід доручати видатним вітчизняним правознавцям з обов'язковим залученням вітчизняних юридичних шкіл. Крім того, уряд має забезпечити належний рівень постійного зовнішнього та внутрішнього фінансування кіберсектору[2].

Ще однією важливою особливістю є тісний зв'язок між кібербезпекою та розвитком вітчизняної освіти. Так, обізнаність у кібербезпеці є темою, яка становить особливий інтерес у кібербезпеці. Люди є центральними фігурами в кібербезпеці, і спосіб зменшити ризик у кіберпросторі – це зробити людей більш обізнаними про безпеку. Хоча було проведено численні дослідження щодо різних аспектів обізнаності про кібербезпеку, вони непослідовні та залежать від середовища. Науковці виявили, що знання виявилися домінуючим фактором усвідомлення кібербезпеки, і хоча студенти є вихідцями з цифрових технологій, вони не почуваються в безпеці в кіберсередовищі; вони не поводяться безпечно та не мають належних знань, щоб захистити себе в кіберпросторі[3].

У цьому контексті S. Topor зазначає, що сфера кібербезпеки є і ще

[1] Kryshtanovych M., Andriyash V., Bondar H., Kushnir Y., Ozarko K. Public Administration Mechanisms for Ensuring Cybersecurity in Modern Conditions of Socio-Economic Development. *International Journal of Computer Science and Network Security*. 2022. № 22 (3). P. 606.

[2] Pchelina O. V., Skulysh Y. D., Buglak I., Myroniuk R. V. International experience of ensuring cybersecurity in the country and possibility of its application in Ukraine. *DIXI*. 2021. № 23 (2). P. 14–15.

[3] Kovacevic A., Putnik N., Toskovic O. Factors Related to Cyber Security Behavior. *IEEE Access*. 2020. № 8. P. 140.

довго буде міцним зв'язком між секторами освіти, промисловості та військовими[1]. Важливу роль у вивченні здобувачами основ кібербезпеки відіграють різноманітні продукти, які може надати заклад освіти, такі як: освітні курси, університетські програми, конференції, семінари, виставки, візити тощо[2]. Водночас здобуття освіти за курсами може охоплювати відповідні теми в широкому діапазоні: від стратегій і політики до суто технічних галузей. Деякі з тем, які S. Topor пропонує включити до початкової підготовки та орієнтаційних курсів з кібербезпеки, можуть охоплювати: структури та організації на національному рівні та в інституціях ЄС і НАТО, які мають відношення до сфери кібербезпеки та мають завдання у сфері кібербезпеки; планування та управління кібероперaціями під час кризи; технічні теми для тих, хто менше знайомий із різними рівнями кіберзахисту: від фізичної інфраструктури до віртуального домену чи «кіберідентичності»; деякі аспекти щодо можливостей кіберпростору, з акцентом на оборонні; законодавча база та політики, що застосовуються до кіберконфлікту тощо[3].

Незважаючи на те, що багато університетів запровадили програми отримання дипломів з кібербезпеки, основна увага цих програм зосереджена на розвитку технічних навичок, а деякі дослідницькі звіти вказують на те, що випускникам цих курсів не вистачає більш м'яких навичок і ділової хватки. Проте управління кібербезпекою є темою, де студенти можуть розвивати такі навички[4]. З огляду на це постає важливість розуміння освітніх програм із кібербезпеки як таких, коли їх напрямок залежить від адміністративно-правових основ, врахування організаційно-управлінських особливостей забезпечення кібербезпеки на рівні підприємства, установи та організації. У світлі такого бачення постає важливість забезпечення фінансування досліджень, спрямованих на аналіз адміністративно-правових засад кібербезпеки в різних сферах життєдіяльності, налагодження державно-приватного партнерства в даній сфері, надання стипендій та грантів на реалізацію ініціатив, спрямованих на вдосконалення адміністративно-правового забезпечення кібербезпеки у різних сферах та галузях, налагодження міцніших зв'язків у даній сфері між закладами вищої освіти та дослідницькими установами по всій країні.

Ще однією особливістю забезпечення кібербезпеки, як провідної складової національної безпеки України є формування так званої кіберкультури як системи цінностей, стійких уявлень про сутність та значення кібербезпеки у повсякденній життєдіяльності людей, їх об'єднань та суспільства в цілому. Одним із напрямків поширення високих стандартів

[1] Topor S. Education in the cyber security field and implications for national security. *Annals: Series on Military Sciences.* 2020. №12 (1). P. 94.

[2] Topor S. Education in the cyber security field and implications for national security. *Annals: Series on Military Sciences.* 2020. №12 (1). P. 95.

[3] Topor S. Education in the cyber security field and implications for national security. *Annals: Series on Military Sciences.* 2020. №12 (1). P. 96.

[4] Allison J. Devising a cyber security management module through integrated course design. *Journal of Further and Higher Education.* 2023. № 47 (10). P. 1389.

кіберкультури серед значної кількості населення є національні змагання з кібербезпеки. Такі змагання забезпечують широкомасштабну обізнаність про проблеми кібербезпеки та мотивують людей дотримуватися вимог кібербезпеки. На початку 2014 року ENISA (European Network and Information Security Argent) мотивувала європейські країни організувати змагання з кібербезпеки національного рівня, подібні до змагань національного рівня з футболу. Після цього ENISA організувала змагання європейського рівня, подібні до футбольної ліги УЄФА, в яких кілька країн брали участь зі своїми національними командами. Це змагання з кібербезпеки відоме як ECSC (European Cyber Security Challenge). Люди віком від 14 до 25 років намагаються вирішити різні проблеми кібербезпеки, пов'язані з Інтернетом, криптографією, OSINT (розвідкою з відкритим кодом) тощо[1].

Висновки. Сучасне розуміння феномену національної безпеки постає у єдності декількох складових, які охоплюють воєнну безпеку, публічну безпеку, економічну безпеку, енергетичну безпеки, екологічну безпеку, інформаційну безпеку, державну безпеку та кібербезпеку. Остання виступає інтегруючою складовою по відношенню до всіх інших, адже у сучасних умовах використання відповідних програм є основою здійснення операцій у будь-якій сфері суспільного життя. З огляду на це кібербезпека по праву може вважатися провідною складовою національної безпеки України.

Необхідно бути свідомими того, що в останні десятиліття проблема кібербезпеки суттєво трансформувалася з рівня окремого комп'ютера на рівень держави, окремих організацій, сфер економіки та об'єктів критичної інфраструктури. З огляду на це дана проблема тепер не є суто технічною, а має розглядатися саме з точки зору адміністративно-правового забезпечення функціонування цілісного механізму забезпечення кібербезпеки держави, створення відповідних інституцій, центральних органів виконавчої влади, відповідальних за даний напрямок, а також структурних підрозділів (посадових осіб) на рівні окремих підприємств, установ, організацій.

До особливостей забезпечення кібербезпеки як провідної складової національної безпеки України нами віднесено формування нормативно-правової основи кібербезпеки, визначення її концептуального бачення та стратегії розвитку на рівні держави; тісний зв'язок між кібербезпекою та розвитком вітчизняної освіти; формування так званої кіберкультури як системи цінностей, стійких уявлень про сутність та значення кібербезпеки у повсякденній життєдіяльності людей, їх об'єднань та суспільства в цілому.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Yamin M., Erdodi L., Torseth E., Katt B. Selecting and Training Young Cyber Talent: A Recurrent European Cyber Security Challenge Case Study. *Augmented Cognition*. 2022. № 13310. P. 304.

1. Allison J. Devising a cyber security management module through integrated course design. *Journal of Further and Higher Education.* 2023. № 47 (10). P. 1389–1403.

2. Ganapati S., Ahn M., Reddick C. Evolution of Cybersecurity Concerns: A Systematic Literature Review. In: 24th Annual International Conference on Digital Government Research (DGO) – Together in the Unstable World - Digital Government and Solidarity. Gdansk, 11–14 July 2023. P. 90–97.

3. Kovacevic A., Putnik N., Toskovic O. Factors Related to Cyber Security Behavior. *IEEE Access*. 2020. № 8. P. 140–148.

4. Kryshtanovych M., Andriyash V., Bondar H., Kushnir Y., Ozarko K. Public Administration Mechanisms for Ensuring Cybersecurity in Modern Conditions of Socio-Economic Development. *International Journal of Computer Science and Network Security*. 2022. № 22 (3). P. 606–610.

5. Le N., Hoang D. Can maturity models support cyber security? 35th IEEE International Performance Computing and Communications Conference (IPCCC). Las Vegas, 09–11 December 2016. URL: https://www.semanticscholar.org/paper/Can-maturity-models-support-cyber-security-Le-Hoang/2aff05eb3f7b453430ea3a60d79735b67ea1674f.

6. Limba T., Pleta T., Agafonov K., Damkus M. Cyber security management model for critical infrastructure. *Entrepreneurship and Sustainability Issues.* 2017. № 4 (4). P. 559–573.

7. Pchelina O. V., Skulysh Y. D., Buglak I., Myroniuk R. V. International experience of ensuring cybersecurity in the country and possibility of its application in Ukraine. *DIXI*. 2021. № 23 (2). P. 1–16.

8. Srinivas J., Das A., Kumar N. Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems-The International Journal of Escience*. 2019. № 92. P. 178–188.

9. Topor S. Education in the cyber security field and implications for national security. *Annals: Series on Military Sciences.* 2020. №12 (1). P. 81–98.

10. Yamin M., Erdodi L., Torseth E., Katt B. Selecting and Training Young Cyber Talent: A Recurrent European Cyber Security Challenge Case Study. *Augmented Cognition*. 2022. № 13310. P. 304–321.

Стаття надійшла до редакції 17.11.2024

Oleksandr Iv. CHERVYAKOV,
PhD in Law
(Institute of the Security Service of Ukraine, Yaroslav the Wise National Law University, Kharkiv, Ukraine)

PECULIARITIES OF ENSURING CYBER SECURITY AS A LEADING COMPONENT OF UKRAINE'S NATIONAL SECURITY

The article emphasizes that the modern understanding of the phenomenon of national security appears in the unity of several components, which include military security, public security, economic security, energy security,

environmental security, information security, state security and cyber security. The latter acts as an integrating component in relation to all others, because in modern conditions, the use of appropriate programs is the basis of operations in any sphere of social life.

It was emphasized that it is necessary to be aware of the fact that in recent decades the problem of cyber security has significantly transformed from the level of a single computer to the level of the state, individual organizations, spheres of the economy and objects of critical infrastructure. In view of this, this problem is now not purely technical, but should be considered precisely from the point of view of administrative and legal support for the functioning of an integrated mechanism for ensuring state cyber security, the creation of relevant institutions, central bodies of executive power responsible for this area, as well as structural subdivisions (official persons) at the level of individual enterprises, institutions, organizations.

It is noted that the formation of the regulatory and legal basis of cyber security, the definition of its conceptual vision and development strategy at the state level should be included among the peculiarities of ensuring cyber security as a leading component of Ukraine's national security; the close connection between cyber security and the development of domestic education; formation of the so-called cyber culture as a system of values, stable ideas about the essence and significance of cyber security in the everyday life of people, their associations and society as a whole.

Key words: *national security of Ukraine, features of cyber security, administrative and legal support, cyber culture.*