УДК 371.3
DOI https://doi.org/10.20535/2308-5053.2023.1(57).280780

ПОЛІТИЧНІ ВІЗІЇ КІБЕРОСВІТИ

Ананьїн В. О.,
доктор філософських наук, професор,
професор Спеціальної кафедри Інституту
спеціального зв'язку та захисту інформації
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»
ORCID ID: 0000-0002-4786-0011

Уваркіна О. В.,
доктор філософських наук, професор, завідувач
Спеціальної кафедри Інституту спеціального
зв'язку та захисту інформації
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»
ORCID ID: 0000-0001-9053-2016
uvarkinaev@ukr.net

У статті вперше проведений аналіз політичних візій нової Національної стратегії кібербезпеки США у питаннях кіберосвіти, яка у сучасної безпекової ситуації стає своєрідним габітусом світового інформаційного простору та започатковує нову довгострокову політику ключового українського міжнародного партнерства у гармонізації безпекових підходів. Визначення нових пріоритетів як глобального, так і національного безпекового середовища фокусує увагу Стратегії США на комплексному та скоординованому підходу державної політики у напрямку розширення доступу до кіберосвіти для задоволення потреб в експертних знаннях з кібербезпеки в усіх секторах економіки для продовження впровадження інновацій в безпечні та стійки технології наступного покоління.

Визначено, що необхідність актуалізації проблеми підготовки сучасних фахівців у сфері кібербезпеки обумовлена експоненціальною світовою цифровізацією, яка підвищила потребу у підготовці кібербезпекових спеціалістів у різних сферах діяльності суспільства.

Доведено, що у державних стратегічних документах з кібербезпеки приділяється увага до реформування кіберосвіти через оновлення та затвердження професійних стандартів, які є основою для вдосконалення освітніх програм та запровадження нових сучасних спеціалізації.

З'ясовано, що програма NATO DEEP в Україні продовжує адаптувати військову освіту до вимог НАТО, де кіберобізнаність військового фахівця в нової моделі військової освіти стає пріоритетною ознакою його професіоналізму.

Аналіз реалізації програми з кіберграмотності показав, що існує величезний попит на різноманітні заходи з кібергігієни для захисту молоді від деструктивного впливу дезінформації й маніпулятивної інформації в кіберпросторі з урахуванням появи нових кіберзагроз і викликів.

Ключові слова: стратегія кібербезпеки, фахівці з кібербезпеки, професійні стандарти, кіберграмотность, кібергігієна.

Постановка проблеми дослідження. Потреба екскурсу у політичні візії кіберосвіти обумовлена активізацією конотацій інновацій у сфері кібербезпеки, до яких долучилась майже вся світова інформаційна спільнота. Під впливом експоненційної світової цифровізації у суспільстві відчувається дефіцит фахівців з кібербезпеки у всіх сферах діяльності, а їх підготовка стає одним з пріоритетних завдань освітньої державної політики. Ураховуючи кардинальну зміну безпекової ситуації, яка

пов'язана з військовою агресією рф проти України, актуальність підготовки фахівців у сфері кібербезпеки також, безсумнівно, телеологічно зростає, трансгресує і темпорально вимагає політичної взаємодії з країнами-партнерами України. Тому визначення політичних візій на інтенцію сучасної кіберосвіти актуально для систематизації довгострокових програм та проектів у вітчизняних та світових стратегіях кібербезпеки.

Аналіз останніх досліджень і публікацій. Дослідженню концептуального каркасу української кіберосвіти присвячені сучасні праці військових фахівців (Ю. Даник, А. Зінченко, С. Мельник, В. Телелим та інші), науковців, які беруть участь у підготовці кадрів у сфері кібербезпеки (Л. Арсенович, О. Євсюкова, О. Матвійчук-Юдіна, О. Овчарук О. Юдін, та інші), а також компаративістів-дослідників з різних галузей знань науки і техніки, які змістовно збагачують та забезпечують кон'юкційну динаміку розвитку сучасних траєкторій становлення нової моделі інформаційної безпеки України (Б. Бистрова, А. Войцеховський, М. Гаврільцев, Т. Дзюба, Д. Дубов, Ю. Завгородня, Є. Таран та інші). Сумлінно оглядаючи динаміку дискурсів, визначаємо, що найвищий рівень конвенційної погодженості у фаховому середовищі притаманний тезі, згідно з якою «професійна підготовка фахівців у сфері кібербезпеки є одним із напрямів державної політики у сферах національної безпеки та оборони, без якої неможливий науково-технічний та соціально-економічний розвиток країни» (Арсенович, 2022). Разом з тим, на нашу думку, в українському науковому просторі немає повноцінного наукового дискурсу щодо політичних візій кіберосвіти та міжнародного партнерства у цієї галузі освіти. Постановка цього питання тим більш актуальна в умовах проактивної боротьби зі зловмисною діяльністю РФ у світовому кіберпросторі. Амплітуда концептуальних точок зору на проблемний горизонт кіберосвіти також підвищується під впливом нової Національної стратегії кібербезпеки США, яка актуалізує безпекову складову як у традиційних, так і в нових сферах.

Метою статті є визначення основних політичних візій кіберосвіти в умовах радикальних змін безпекової ситуації, пов'язаної з російською агресією проти України.

Виклад основного матеріалу дослідження. Основні політичні візії національної системи кібербезпеки були визначені у Плані реалізації Стратегії кібербезпеки України (далі – План реалізації), уведеного в дію Указом Президента України від 1 лютого 2022 року. Серед стратегічних цілей, особлива увага у Плані реалізації приділяється докорінної реформі системи підготовки та підвищення кваліфікації фахівців у сфері кібербезпеки, збереженню наявного кваліфікованого кадрового потенціалу суб'єктів кібербезпеки, а також координації заходів наукового співтовариства щодо стимулювання проведення наукових досліджень і розробок з реалізації державної політики у сфері кібербезпеки, з урахуванням появи нових кіберзагроз і викликів. Для потреб національної безпеки і оборони вважається необхідним визначення довгострокових напрямів проведення досліджень за програмою державної підтримки, «з урахуванням розвитку новітніх інформаційно-комунікаційних технологій, зокрема, технологій хмарних та квантових обчислень, 5G-мереж, Інтернету речей, штучного інтелекту з метою створення вітчизняних систем, платформ і продуктів у сфері кібербезпеки» (План реалізації , 2022).

Також, без перебільшень, вже можна констатувати, що Національна стратегія кібербезпеки США (далі – Стратегія США), яку 1 березня 2023 року оприлюднила адміністрація Президента США, започатковує нову довгострокову політику ключового українського міжнародного партнерства у гармонізації безпекових підходів. Російська агресія проти України змінила низку тенденцій в кібербезпековій політиці США та визначила нові пріоритети як глобального, так і національного безпекового середовища. У фокусі уваги Стратегії США (Ціль 4.6) зазначена національна стратегія комплексного та скоординованого підходу державної політики у напрямку розширення доступу до кіберосвіти. Розробку та впровадження Національної стратегії кібертрудових ресурсів та освіти доручено ONCD (Office of the National Cyber Director), який має задовольнити потребу в експертних знаннях з кібербезпеки в усіх секторах економіки для продовження впровадження інновацій в безпечні та стійки технології наступного покоління. Серед завдань політики кібербезпеки є залучення стратегічних державних інвестицій в інновації, науково-дослідні й дослідно-конструкторські роботи (НДДКР) через використання регіональної програми інноваційного розвитку Національного наукового фонду (NSF), довгострокових програм безпечного та надійного кіберпростору, нових грантових програм, включаючи Національну ініціативу з кіберосвіти (NICE), програму CyberCorps: стипендія для служби, програму Національних центрів академічної майстерності в галузі кібербезпеки, програму навчання та допомоги з питань кібербезпеки (Стратегія США, 2023).

Згідно аналітичної записки Національного Інституту стратегічних досліджень «Національна стратегія кібербезпеки США 2023: критична інфраструктура, координація, проактивність», українська кібербезпекова політика вже бере до уваги ідеї, використані в новій Стратегії США. Зазначається , що «як і більшість країн світу, Україна потребує більше фахівців з кібербезпеки – протягом цього та попереднього років вже було створено шість нових професійних стандартів кібербезпеки, гармонізованих

з положеннями NICE Framework, а відтак, впроваджуються найкращі міжнародні практики в освітній процес» (Дубов, 2023).

Дійсно на підсумковому у 2022 році засіданні Національного кластера кібербезпеки «Війна в кіберпросторі 2022: підсумки, здобутки та прогалини», який є координаційною платформою для об'єднання ресурсів, можливостей, компетенцій РНБО України та Фонду Цивільних досліджень на розвитку США (CRDF GLOBAL), урядових та міжнародних організацій, було зазначено, що національне агентство кваліфікацій проінформувало Адміністрацію Держспецзв'язку про внесення до Реєстру кваліфікацій відомостей професійних стандартів у сфері кібербезпеки:

– «Розробник систем захисту інформації»,
– «Адміністратор мереж і систем»,
– «Фахівець сфери захисту інформації»,
– «Аналітик з безпеки інформаційно-телекомунікаційних систем»,
– «Фахівець з питань безпеки (інформаційно-комунікаційні технології)»,
– «Інструктор-методист з інформаційної безпеки та кібербезпеки» (Cyber Digest, 2022).

Перші шість професійних стандартів були розроблені за підтримки Проєкту USAID Cybersecurity Activity «Кібербезпека критично важливої інфраструктури України», пройшли етапи публічного обговорення, дістали позитивні висновки експертизи Національного агенства кваліфікацій та були затверджені головою Держспецзв'язку Юрієм Щиголем. Затверджені стандарти відтепер є основою для запровадження нових спеціалізацій та оновлення освітніх програм вищої освіти за напрямками підготовки фахівців з кібербезпеки. Донині наявні у класифікаторі професії не відображали реалій сьогодення та не враховували стрімкого розвитку кіберпростору і тому у 2023 році Держспецзв'язку планує розробити професійні стандарти для 14 нових професій з кібербезпеки для посилення кіберзахисту країни (Cyber Digest, 2022).

Між іншим, слід нагадати. що в Україні запроваджена принципово нова програма NATO DEEP (Defence Education Enhancement Program) для підготовки спеціалістів військової сфери на основі передового досвіду країн-членів північноатлантичного альянсу (Jolicoeur, 2018). Програма не зосереджує увагу безпосередньо на підготовці військових фахівців з кібербезпеки, але допомагає у становленні системи професійної військової освіти та підготовці офіцерів сектору безпеки та оборони для спільної відсічі ворожим загрозам країнам НАТО у п'ятивимірної війні на суходолі, в морі, в повітрі, у космосі та кіберпросторі. Змістовне оновлення кредитних модулів та методики викладання навчальних дисциплін у визначених вищих військових закладах освіти має адаптувати українську освіту до вимог НАТО та оперативно, матеріально та інтелектуально змінити політику підготовки військових фахівців, не виключаючи і підготовку фахівців з кібербезпеки.

Безумовно, що розширення горизонтів трансформації української безпекової доктрини у напряму європейської і євроатлантичної інтеграції спрямовує фахівців з кібербезпеки на вирішення головного завдання розвитку системи кібербезпеки – «гарантування кіберстійкості та кібербезпеки національної інформаційної інфраструктури» (Про стратегію національної безпеки України, 2020) та врахування того, що «можливості комунікативного впливу на ворога зрівнялися й перевищили можливості збройного впливу» (Кулеба, 2022).

З'ясовуючи особливості кіберосвіти, чимало дослідників визнають необхідність організації системи освіти з питань кібербезпеки та пропонують «структурувати підготовку з питань кібербезпеки за етапами або рівнями освіти прийнятими у державі» (Даник, 2018). Принагідно зауважимо, що за фактом відторік у Плані реалізації (Ціль К.2.), зазначено про розробку Загальнонаціональної програми кіберграмотності, яка буде спрямована «на підвищення рівня цифрової грамотності населення України, зокрема, шляхом включення питань стосовно цифрових навичок, кіберобізнаності щодо сучасних кіберзагроз та протидії ним до навчальних програм загальної середньої, професійної (професійно-технічної), фахової передвищої та вищої освіти» (План реалізації, 2022).

Прикладом виконання зазначеного у Плані реалізації завдання є започатковані Інститутом спеціального зв'язку та захисту інформації КПІ ім. Ігоря Сікорського (Далі – Інститут) відкриті уроки на тему «Вступ до кібергігієни» в школах України. Ця соціальна ініціатива, яка була запланована на час проведення у жовтні щорічного Місяцю кібербезпеки, була продовжена і в умовах воєнного стану. Науково-педагогічні працівники Інституту спільно з курсантами проводять онлайн-уроки з кібергігієни та ознайомлюють учнів з основними принципами зменшення ризиків у інформаційному просторі та основам протидії негативному інформаційному впливу. Звернемо увагу, що в опублікованих Інститутом матеріалах конференції «Кібербезпека державних інституцій та подолання кризових станів» (2022) зазначається, що «за час проведення занять «Вступ до кібергігієни» було охоплено понад 15000 учнів» та уроки з кібергігієни виявили значний інтерес з боку педагогів та батьків (Пучков, 2022). Це, безперечно, один з напрямів Загальнонаціональної програми кіберграмотності, спрямованої на

захист від деструктивного впливу дезінформації й маніпулятивної інформації перед широким спектром безпекових загроз, зокрема в кіберпросторі.

Висновки. В умовах радикальної зміни безпекової ситуації та трансформаційних процесів глобального та національного безпекового середовища актуалізація концепту політичних візій кіберосвіти постає достатньо затребуваним та належить до нагальних питань підготовки сучасного фахівця у сфері кібербезпеки. Політичний праксис реалізації стратегічного курсу України на інтеграцію в євроатлантичний безпековий простір потребує оновлення нормативно-правових аспектів підготовки фахівців у сфері кібербезпеки та відкриває надзвичайно широкий горизонт для повноцінного наукового дискурсу. Когнитивні коди сучасності у кіберпросторі у своєму змісті мають бути спрямовані на гарантування кіберстійкості та кібербезпеки національної інформаційної інфраструктури з ознаками функцій ефективності, засвоюваності та адаптованості, що має забезпечити якісна кіберосвіта, використовуючи всі інструменти національної міці.

Ananin V., Uvarkina O. Political visions of cyber education

This article is the first to analyze the political visions of the new US National Cybersecurity Strategy in terms of cyber education, which in the current security situation is becoming a kind of habitus of the global information space and launches a new long-term policy of the key Ukrainian international partnership in harmonizing security approaches. The identification of new priorities in both the global and national security environment focuses the attention of the US Strategy on a comprehensive and coordinated approach of public policy towards expanding access to cyber education to meet the needs for cybersecurity expertise in all sectors of the economy to continue to innovate in secure and sustainable next-generation technologies.

It is determined that the need to actualize the problem of training modern cybersecurity specialists is due to the exponential global digitalization, which has increased the need for training cybersecurity specialists in various spheres of society.

It is proved that the state strategic documents on cybersecurity pay attention to the reform of cyber education through the updating and approval of professional standards, which are the basis for improving educational programs and introducing new modern specializations.

It has been found that the NATO DEEP program in Ukraine continues to adapt military education to NATO requirements, where cyber awareness of a military specialist in the new model of military education becomes a priority feature of his professionalism.

The analysis of the implementation of the cyber literacy program showed that there is a huge demand for various cyber hygiene measures to protect young people from the destructive effects of disinformation and manipulative information in cyberspace, taking into account the emergence of new cyber threats and challenges.

Key words: cybersecurity strategy, cybersecurity professionals, professional standards, cyberliteracy, cyberhygiene.

Література:

1. Арсенович Л. Удосконалення механізмів формування системи підготовки кадрів у сфері кібербезпеки в умовах державно-приватної взаємодії. *Науковий* вісник: Державне управління. 2022. №1 (11). С. 6–27. URL: https://doi.org/10.33269/2618-0065-2022-1(11)-6-27
2. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про План реалізації Стратегії кібербезпеки» : Указ Президента України від 1 лютого 2022 року № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/n0087525-21#Text (дата звернення: 22.03.2023).
3. The White House: National Cybersecurity Strategy. Washington. March 1, 2023. URL: https://www.whitehouse.gov/wp-content/uploads/2023/03/National- Cybersecurity-Strategy-2023.pdf
4. Дубов Д. Національна стратегія кібербезпеки США 2023: критичні інфраструктура, координація, проактивність. Аналітична записка / Національний інституту стратегічних досліджень. Київ, 2023. [Рукопис на 4 арк.].
5. Cyber Digest. Огляд подій в сфері кібербезпеки. Київ, грудень 2022. URL: https://www.rnbo.gov.ua/files/%D0%9D%D0%9A%D0%A6%D0%9A/%D0%9D%D0%9A%D0%A6%D0%9A-1/Cyber%20digest_December_2022.pdf
6. Pierre Jolicoeur. Defense Education Enhancement Program in Ukraine: The Limits of NATO's Education Program. Connections QJ, 2018. No 17(3) P. 109–119. URL: https://doi.org/10.11610/Connections.17.3.08.

7. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року « Про Стратегію національної безпеки України»: Указ Президента України від 14 вересня 2020 року № 37/2022. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення: 22.03.2023).
8. Кулеба Д. Війна за реальність: як перемагати у світі фейків, правд і спільнот. Київ : Книголав, 2022. 384 с.
9. Даник Ю., Зінченко А. Кіберосвіта та її особливості. Військова освіта. 2018. № 2(38). С. 67–84. URL: https://znp-vo.nuou.org.ua/issue/view/9559
10. Пучков О.О., Конюшок С.М. Роль обізнаності громадян у сфері кібербезпеки в умовах кризи: досвід ІСЗЗІ КПІ ім. Ігоря Сікорського. Матеріали І Міжнародної науково-практичної конференції «Кібербезпека державних інституцій та подолання кризових станів» Київ : ІСЗІІ КПІ ім. Ігоря Сікорського, 2022. С. 241–242.

References:

1. Arsenovych L. Udoskonalennia mekhanizmiv formuvannia systemy pidhotovky kadriv u sferi kiberbezpeky v umovakh derzhavno-pryvatnoi vzaiemodii [Improvement of the mechanisms of formation of the personnel training system in the field of cyber security in the conditions of public-private interaction]. Naukovyi visnyk: Derzhavne upravlinnia. 2022. №1 (11). S. 6–27. URL: https://doi.org/10.33269/2618-0065-2022-1(11)-6-27 [in Ukrainian]
2. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 30 hrudnia 2021 roku «Pro Plan realizatsii Stratehii kiberbezpeky» ["About the Cyber Security Strategy Implementation Plan"] : Ukaz Prezydenta Ukrainy vid 1 liutoho 2022 roku № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/n0087525-21#Text (data zvernennia: 22.03.2023). [in Ukrainian]
3. The White House: National Cybersecurity Strategy. Washington. March 1, 2023. URL: https://www.whitehouse.gov/wp-content/uploads/2023/03/National- Cybersecurity-Strategy-2023.pdf [in English]
4. Dubov D. Natsionalna stratehiia kiberbezpeky SShA 2023: krytychni infrastruktura, koordynatsiia, proaktyvnist. Analitychna zapyska [US National Cyber Security Strategy 2023: Critical Infrastructure, Coordination, Proactivity. Analytical note] / Natsionalnyi instytutu stratehichnykh doslidzhen. Kyiv, 2023. [Rukopys na 4 ark.] [in Ukrainian]
5. Cyber Digest. Ohliad podii v sferi kiberbezpeky [Overview of events in the field of cyber security]. Kyiv, hruden 2022. URL: https://www.rnbo.gov.ua/files/%D0%9D%D0%9A%D0%A6%D0%9A/%D0%9D%D0%9A%D0%A6%D0%9A-1/Cyber%20digest_December_2022.pdf [in Ukrainian]
6. Pierre Jolicoeur. Defense Education Enhancement Program in Ukraine: The Limits of NATO's Education Program. Connections QJ, 2018. No 17(3) P. 109–119. URL: https://doi.org/10.11610/Connections.17.3.08 [in English]
7. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 veresnia 2020 roku « Pro Stratehiiu natsionalnoi bezpeky Ukrainy» ["On the National Security Strategy of Ukraine"] : Ukaz Prezydenta Ukrainy vid 14 veresnia 2020 roku № 37/2022. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (data zvernennia: 22.03.2023). [in Ukrainian]
8. Kuleba D. Viina za realnist: yak peremahaty u sviti feikiv, pravd i spilnot [The War for Reality: How to Win in a World of Fakes, Truths, and Communities]. Kyiv : Knyholav, 2022. 384 s. [in Ukrainian]
9. Danyk Yu., Zinchenko A. Kiberosvita ta yii osoblyvosti [Cyber education and its features]. Viiskova osvita. 2018. № 2(38). S. 67–84. URL: https://znp-vo.nuou.org.ua/issue/view/9559 [in Ukrainian]
10. Puchkov O.O., Koniushok S.M. Rol obiznanosti hromadian u sferi kiberbezpeky v umovakh kryzy: dosvid ISZZI KPI im. Ihoria Sikorskoho. [The role of awareness of citizens in the field of cyber security in crisis conditions: experience of ISCIPof Igor Sikorsky Kyiv Polytechnic Institute]. Materialy I Mizhnarodnoi naukovo-praktychnoi konferentsii «Kiberbezpeka derzhavnykh instytutsii ta podolannia kryzovykh staniv» Kyiv : ISZII KPI im. Ihoria Sikorskoho, 2022. S. 241–242. [in Ukrainian]

Стаття надійшла до редакції 24.03.2023
Стаття рекомендована до друку 06.04.2023