УДК 32.019.2
DOI https://doi.org/10.32782/app.v74.2024.8

Ю. В. Завгородня
orcid.org/0000-0003-3500-8638
кандидат політичних наук, доцент,
доцент кафедри політичних теорій
Національного університету «Одеська юридична академія»

ДЕРЖАВНА ПОЛІТИКА В СФЕРІ КІБЕРБЕЗПЕКИ В УМОВАХ ПОВНОМАСШТАБНОЇ ВІЙНИ

Державна політика України у сфері кібербезпеки формується на міжнародній нормативній базі ратифікованій Україною та внутрішніми правовими документами. Повномасштабна війна прискорила ряд політичних рішень, які не визначались першочерговими, проте повномасштабна війна сприяла актуалізації безпекових питань в усіх сферах та площинах.

З початку російського вторгнення в 2022 році, кіберпростір став ареною інтенсивних атак, що вражають як корпоративну, так і персональну та державну безпеку.

13–14 січня 2022 року відбулася масова атака на українські урядові веб-сайти з повідомленнями про нібито витік особистих даних. Невдовзі був виявлений шкідливий програмний комплекс WhisperGate, націлений на знищення файлів на урядових, неприбуткових та IT-організаціях. 19 січня група хакерів Gamaredon намагалася скомпрометувати урядову установу в Україні з метою кібершпіонажу. З 6 березня зросла кількість атак проти цивільних, особливо фішингу та шкідливого ПЗ для особистих пристроїв (Адамов, 2024).

Такі активні кібератаки були звісткою про початок кіберпротиборства направленого на підтримання вторгнення наземного, проте існувала хибна думка про те, що через бажання ворога залякувати в кіберпросторі, повномасштабного вторгнення не буде, що зменшувало напругу у суспільстві. Проте, повномасштабне вторгнення розвіяло будь-які ілюзії щодо сприйняття агресором добросусідського існування та визнання територіальної цілісності України.

З розвитком боротьби повномасштабного вторгнення виникає актуальність щодо переоцінки значимості кіберпросторових атак та злочинів, які мастабувались на кіберпростір країн-партнерів України та необхідності у спільних діях. Тому, дослідження заходів, які вживає Україна під час агресії РФ, дуже важлива в аспекті кібернетичного досвіду кібербезпеки держави в умовах війни.

Наявна сукупність нормативно правових документів щодо кібербезпезпеки свідчить про, те усі закони та міжнародні договори були погоджені ще до повномастабного вторгнення. Так, на міжнародному рівні ключовими документами є Будапештська конвенція та Директива ЄС про мережеву та інформаційну безпеку (NIS). Відповідно, у національному законодавстві повинні бути враховані зобов'язання, які Україна взяла на себе як підписант міжнародних угод і конвенцій, а також ті, які можуть виникнути в процесі інтеграції до Європейського Союзу. Основними національними нормативними актами, що регулюють сферу кібербезпеки, є Закон України № 2163-VIII від 5 жовтня 2017 року «Про основні засади забезпечення кібербезпеки України» (Закон, 2017) та Національна стратегія кібербезпеки України (Стратегія, 2021).

У 2005 році Україна ратифікувала Будапештську конвенцію (Конвенція, 2005) – єдиний юридично обов'язковий міжнародний документ у галузі кібербезпеки, що визначає спільну кримінально-правову політику захисту від кіберзлочинності шляхом прийняття відповідного національного законодавства та сприяння міжнародному співробітництву. Проте не всі положення конвенції були інтегровані в українське законодавство, а повна імплементація вимагає внесення суттєвих змін до Кримінального процесуального кодексу.

У 2016 році Європейський Парламент ухвалив першу частину єдиного законодавства ЄС у сфері кібербезпеки – Директиву NIS. Оскільки Україна не є членом ЄС, положення Директиви NIS не є обов'язковими, але вони слугують орієнтиром для належної практики. Деякі

з положень цієї директиви були добровільно запроваджені в українському законодавстві, тоді як інші залишаються без належної уваги.

Останні роки перед повномасштабним вторгненням Україна ухвалила низку нормативних актів, що формують національну правову базу у сфері кібербезпеки. Так, Стратегія кібербезпеки України 2021 року визначила цілі та пріоритети кібербезпеки та проаналізувала реалізацію Стратегії кібербезпеки 2016 року, яка стала основою для прийняття Закону України «Про основні засади забезпечення кібербезпеки України» і вдосконалила потреби у сфері кібербезпеки.

Прийняття Закону про кібербезпеку є значущим кроком уперед, однак для його повної імплементації необхідно додати ще значних зусиль. таким чином, уряд не затвердив підзаконні акти, передбачені Законом про кібербезпеку, особливо ті, що стосуються захисту та аудиту об'єктів критичної інфраструктури (КІ), включно з конкретними апаратними та програмними засобами, що є її частиною та підтримують її функціонування.

Адаптуючись до процесу функціонування органів державної влади в умовах війни Кабінет міністрів України починаючи з 2023 року приймає підзаконні нормативно-правові акти для реалізації Закону України «Про основні засади забезпечення кібербезпеки України» (Закон, 2017), а саме:

− Постанова КМУ від 17 лютого 2023 р. № 142 «Про представника Державної служби спеціального зв'язку та захисту інформації в Об'єднаному центрі передових технологій з кібероборони НАТО» (з метою вдосконалення механізму взаємодії основних суб'єктів національної системи кібербезпеки з компетентними органами іноземних держав для вирішення питань, що стосуються реалізації державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, активної протидії агресії у кіберпросторі, кіберзахисту об'єктів критичної інформаційної інфраструктури та здійснення державного контролю у цих сферах);

− Постанова КМУ від 24 березня 2023 р. № 257 «Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури» (з метою реалізації ст. 6 Закону України «Про основні засади забезпечення кібербезпеки України» затверджено Порядок проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури);

− Постанова КМУ від 04 квітня 2023 р. № 299 «Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі» (з метою забезпечення реалізації пункту 37 Плану реалізації Стратегії кібербезпеки України, схваленого рішенням Ради національної безпеки і оборони України від 30 грудня 2021 р. «Про План реалізації Стратегії кібербезпеки України» затверджено Порядок реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі);

− Постанова КМУ від 19 грудня 2023 р. № 1163-р «Про затвердження плану заходів на 2023–2024 роки з реалізації Стратегії кібербезпеки України» (з метою виконання Стратегії затверджено план заходів на 2023–2024 роки з реалізації Стратегії кібербезпеки України);

− Постанова КМУ від 08 березня 2024 р. № 276 «Про утворення Міжвідомчої робочої групи з питань залучення міжнародної допомоги для забезпечення кібербезпеки та кіберстійкості держави» (з метою сприяння забезпеченню координації дій органів виконавчої влади з питань організації взаємодії з урядами іноземних держав та міжнародним організаціями у частині залучення міжнародної допомоги для забезпечення кібербезпеки та кіберстійкості держави, а також у започаткуванні та реалізації проектів (програм) міжнародної технічної допомоги щодо підвищення рівня стійкості державних інформаційних ресурсів утворенно Міжвідомчу робочу групу з питань залучення міжнародної допомоги для забезпечення кібербезпеки та кіберстійкості держави).

Враховуючи умови повномасштабної війни динаміка нормотворчої діяльності щодо кіберзахисту та розвитку кібербезпеки видається достатньо низькою з вирішенням проблем, які кардинально не впливають на кіберзахист та кібернетично-інфраструктурну систему.

Серед основних проблем, які потребують рішення в правовій базі кібербезпеки України, виділяються такі: невідповідність національного законодавства міжнародним зобов'язанням;

відсутність положень щодо проведення аудитів інформаційної безпеки КІ; обмеження державного бюджету, що зменшує можливості уряду щодо виплати конкурентоспроможних заробітних плат, найбільших для залучення та утримання кваліфікованих спеціалістів у сфері кібербезпеки тощо (Адамов, 2024).

Проте, в останні роки Україна зробила кілька важливих кроків для виконання міжнародних зобов'язань та вдосконалення законодавства у сфері кібербезпеки. Проте для досягнення повної відповідності міжнародним стандартам і забезпечення належного рівня захисту критичної інфраструктури потрібні подальші серйозні зусилля. Пріоритетними завданнями залишаються такі аспекти:

«вдосконалення кібербезпекового законодавства зокрема, забезпечення більш чіткого дотримання положення Будапештської конвенції та Директиви розробка та прийняття всеохоплюючого законодавства щодо питань кібербезпеки, котрі включають узгоджену термінологію та встановлення чітких вимог щодо обов'язкового інформування про кібербезпеку;

створення і затвердження законодавства щодо державно-приватного партнерства у сфері кібербезпеки;

прийняття нових підзаконних актів для встановлення уніфікованих критеріїв і методології класифікації об'єктів як критичної інфраструктури, а також процедур їх атестації, категоризації і аудиту;

чітке визначення ознак кіберзлочинів, які кваліфікують їх як кримінальні правопорушення, розтлумаченя та донесення до фахівців та суспільства;

розмежування юрисдикції та кримінальної відповідальності за кіберзлочини, які спрямовані проти державних інформаційних ресурсів, критичної інфраструктури та інших об'єктів;

оновлення Стратегії кібербезпеки та розробка нового Стратегічного плану кібербезпеки України не очікуючи терміну її дії, а реагуючи на виклики повномасштабної війни» (Адамов О., 2024).

Враховуючи усе вищезазначене можемо дійти до висновку, що основні напрямки державної політики у сфері кібербезпеки є: захист критичної інфраструктури (під час війни критична інфраструктура — такі як енергетика, транспорт, зв'язок та фінансова система — стоять мішенню для кібератак. Одним із завдань державної політики є забезпечення стійкості цих систем.) та розвиток кіберрезерву та кадрового потенціалу (у період війни кібербезпека потребує висококваліфікованих спеціалістів, здатних швидко реагувати на кіберзагрози та адаптуватися до нових викликів) .

Тому, важливої уваги потребує підготовка фахівців у сфері кібербезпеки через розширення освітніх програм та курсів з кіберзахисту в університетах і спеціалізованих навчальних закладах. А також, стимулювання приватного сектора до участі в підготовці кадрів, зокрема через державно-приватне партнерство, створення навчальних центрів та стажування для молодих спеціалістів.

Література

Адамов О. Кібербезпека під час повномасштабного вторгнення: неочікувані принципи кібергігієни**.** *GlobalLogic Ukraine*. 2024. URL: https://itcluster.lviv.ua/itid/kiberbezpeka-pid-chas-povnomasshtabnogo-vtorgnennya-neochikuvani-prynczypy-kibergigiyeny/

Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 5 жовтня 2017 року, URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» (втратила чинність) URL: https://zakon.rada.gov.ua/laws/show/96/2016#n11

Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text

Конвенція про кіберзлочинність, ратифікована Україною від 07.09.2005, підстава – 2824-IV, URL: https://zakon.rada.gov.ua/laws/show/994_575#Text

Постанова КМУ від 17 лютого 2023 р. № 142 «Про представника Державної служби спеціального зв'язку та захисту інформації в Об'єднаному центрі передових технологій з кібероборони НАТО» URL: https://zakon.rada.gov.ua/laws/show/142-2023-%D0%BF#Text

Постанова КМУ від 24 березня 2023 р. № 257 «Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури» URL: https://zakon.rada.gov.ua/laws/show/257-2023-%D0%BF#Text

Постанова КМУ від 04 квітня 2023 р. № 299 «Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі» URL: https://zakon.rada.gov.ua/laws/show/299-2023-%D0%BF#Text

Постанова КМУ від 19 грудня 2023 р. № 1163-р «Про затвердження плану заходів на 2023—2024 роки з реалізації Стратегії кібербезпеки України» URL: https://zakon.rada.gov.ua/laws/show/1163-2023-%D1%80#Text

Постанова КМУ від 08 березня 2024 р. № 276 «Про утворення Міжвідомчої робочої групи з питань залучення міжнародної допомоги для забезпечення кібербезпеки та кіберстійкості держави». URL: https://zakon.rada.gov.ua/laws/show/276-2024-%D0%BF#Text

References

Adamov O. (2024) Kiberbezpeka pid chas povnomasshtabnoho vtorhnennia: neochikuvani pryntsypy kiberhihiieny. [Cyber Security During a Full-Scale Intrusion: Unexpected Principles of Cyber Hygiene] GlobalLogic Ukraine. URL: https://itcluster.lviv.ua/itid/kiberbezpeka-pid-chas-povnomasshtabnogo-vtorgnennya-neochikuvani-prynczypy-kibergigiyeny/ [in Ukrainian]

Zakon Ukrainy (2017) «Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy» № 2163-VIII, [About the main principles of ensuring cyber security of Ukraine] URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text [in Ukrainian]

Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy (2016) «Pro Stratehiiu kiberbezpeky Ukrainy» (vtratyla chynnist) [About Cyber Security Strategy of Ukraine] URL: https://zakon.rada.gov.ua/laws/show/96/2016#n11 [in Ukrainian]

Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy (2021) «Pro Stratehiiu kiberbezpeky Ukrainy» [About Cyber Security Strategy of Ukraine] URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text [in Ukrainian]

Konventsiia pro kiberzlochynnist, (2005), [Convention on cybercrime] pidstava – 2824-IV, URL: https://zakon.rada.gov.ua/laws/show/994_575#Text [in Ukrainian]

Postanova KMU (2023) № 142 «Pro predstavnyka Derzhavnoi sluzhby spetsialnoho zv'iazku ta zakhystu informatsii v Obiednanomu tsentri peredovykh tekhnolohii z kiberoborony NATO» [About the representative of the State Service for Special Communications and Information Protection at the Joint Center for Advanced Technologies in NATO Cyber Defense] URL: https://zakon.rada.gov.ua/laws/show/142-2023-%D0%BF#Text [in Ukrainian]

Postanova KMU (2023) № 257 «Deiaki pytannia provedennia nezalezhnoho audytu informatsiinoi bezpeky na obiektakh krytychnoi infrastruktury» [Some issues of conducting an independent audit of information security at critical infrastructure facilities] URL: https://zakon.rada.gov.ua/laws/show/257-2023-%D0%BF#Text [in Ukrainian]

Postanova KMU (2023) № 299 «Deiaki pytannia reahuvannia subiektamy zabezpechennia kiberbezpeky na rizni vydy podii u kiberprostori» [Some issues of response by cyber security entities to various types of events in cyberspace] URL: https://zakon.rada.gov.ua/laws/show/299-2023-%D0%BF#Text [in Ukrainian]

Postanova KMU (2023) № 1163-r «Pro zatverdzhennia planu zakhodiv na 2023—2024 roky z realizatsii Stratehii kiberbezpeky Ukrainy» [On the approval of the action plan for 2023-2024 for the implementation of the Cybersecurity Strategy of Ukraine] URL: https://zakon.rada.gov.ua/laws/show/1163-2023-%D1%80#Text [in Ukrainian]

Postanova KMU (2024) № 276 «Pro utvorennia Mizhvidomchoi robochoi hrupy z pytan zaluchennia mizhnarodnoi dopomohy dlia zabezpechennia kiberbezpeky ta kiberstiikosti derzhavy» [On the formation of the Interdepartmental Working Group on attracting international assistance to ensure cyber security and cyber resilience of the state] URL: https://zakon.rada.gov.ua/laws/show/276-2024-%D0%BF#Text [in Ukrainian]

Анотація

Завгородня Ю. В. **Державна політика в сфері кібербезпеки в умовах повномасштабної війни.** – Стаття.

В умовах сучасної гібридної війни кіберпростір стає новим полем бою, де інформаційні технології використовують для досягнення військових і політичних цілей. Кіберзагроза є однією з головних проблем для державних інституцій, приватного сектора та громадян. Повномасштабна війна вимагає посилення кібербезпеки як невід'ємної складової національної безпеки. У цьому контексті державна політика у сфері кібербезпеки стає ключовим елементом для забезпечення стабільності та стійкості країни.

У статті актуалізована діяльність держави України в умовах повномасштабного вторгнення агресора щодо боротьби з кіберзагрозами та формуванням публічного політичного декламування стратегічних цілей, конкретних дій та заходів у напрямку формування колегіальної позиції (науковців, ІТ-спеціалістів та політиків) щодо вектору кіберполітики воюючої країни, яка зазнала найбільших атак за період незалежності.

Державна політика у сфері кібербезпеки по своїй суті відповідає викликам сучасних проблем, які виникають у суспільстві. В умовах повномасштабної війни велика кількість проблем, які назрівали у суспільстві та системі управління проявились гостро та актуально, а тому рішення мали бути невідкладними та рішучими.

У статті здійснений аналіз періоду повномастабного вторгнення агресора по теперішній час, прийняті політичні рішення та їх реалізація на практиці. Визначено пріоритетні вектори до подальшого вдосконалення системи кіберзахисту в воюючій країні та в повоєнний період.

Разом з сучасним вирішенням питань кіберзахисту назріли нормативні питання щодо реалізації державної політики кібербезпеки та кіберзахисту в сучасній воєнній Україні з пріоритетом на майбутні системи розвитку та захисту кіберпростору.

Ключові слова: державна політика, кібербезпека, політичний процес, суспільна свідомість, політичні інститути, форми протиборства.

Summary

Zavhorodnya Yu. V. **State policy in the field of cyber security in conditions of full-scale war. –** Article.

In the conditions of modern hybrid warfare, cyberspace is becoming a new battlefield where information technologies are used to achieve military and political goals. Cyber threat is one of the main problems for public institutions, private sector and citizens. All-out war requires strengthening cyber security as an integral component of national security. In this context, the state policy in the field of cyber security becomes a key element to ensure the stability and resilience of the country.

The article updates the activities of the state of Ukraine in the conditions of a full-scale invasion of the aggressor regarding the fight against cyber threats and the formation of public political recitation of strategic goals, specific actions and measures in the direction of the formation of a collegial position (scientists, IT specialists and politicians) regarding the cyber policy vector of a warring country that has experienced the greatest attacks during the period of independence.

State policy in the field of cyber security essentially meets the challenges of modern problems that arise in society. In the conditions of a full-scale war, a large number of problems that were brewing in society and the management system manifested themselves acutely and urgently, and therefore the decisions had to be urgent and decisive.

The article analyzes the period of the full-scale invasion of the aggressor until the present time, made political decisions and their implementation in practice. The priority vectors for the further improvement of the cyber defense system in the warring country and in the post-war period have been determined.

Together with the modern solution of cyber defense issues, regulatory issues regarding the implementation of the state policy of cyber security and cyber defense in modern military Ukraine with a priority on future systems of development and protection of cyber space have matured.

Key words: state policy, cyber security, political process, public consciousness, political institutions, forms of struggle.