ISSN 2072-8670 (Print) **НАУКА І ПРАВООХОРОНА**
NAUKA I PRAVOOKHORONA
DOI (Issue): https: //doi.org/10.36486/np.2023.2(60) **Issue 2(60) 2023**
УДК 004.056

Демедюк Сергій Васильович,
кандидат юридичних наук,
заступник Секретаря Ради національної
безпеки і оборони України, м. Київ, Україна
ORCID ID 0009-0008-1359-5265

РОЗБУДОВА НАЦІОНАЛЬНОЇ КІБЕРСТІЙКОСТІ ТА ЗАХИСТ КРИТИЧНО ВАЖЛИВОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Статтю присвячено аналізу проблемних питань щодо розбудови національної системи кіберстійкості суспільства. Методологічно зосереджується увага на усвідомленні ключових напрямів: захисту критичної інформаційної інфраструктури, боротьби з кіберзлочинністю та розвитку спроможності реагування на кіберінциденти. Акцентовано увагу на тому, що національна кіберполітика має відношення до внутрішніх справ, безпеки оборони і зовнішньої політики, промислової та економічної політики, а також політики у сфері досліджень, освіти та технологічного розвитку. Розкрито особливості реалізації ключових вимог державної політики у розбудові стійкої національної кіберсистеми з особливим акцентом на побудові адекватних механізмів захисту критичної інформаційної інфраструктури.

Ключові слова: *кібербезпека, кіберінцидент, кіберзлочинність, критична інформаційна інфраструктура, кіберстійкість.*

Цифрова трансформація кидає виклик усім суспільствам і економікам і з урахуванням особливостей формує підґрунтя для критично важливих послуг та економічного зростання. Перед національними розробниками кіберполітики стоїть багато пріоритетів, серед яких захист критичної інфраструктури, зниження рівня кіберзлочинності, підвищення обізнаності та дотримання інтересів національної безпеки і зовнішньої політики. Захист критично важливих послуг та інфраструктури, боротьба з кіберзлочинністю, реагування на кіберінциденти та відновлення формують основу кіберстійкості країн в цифрову епоху [1].

Метою статті є проведення огляду щодо організації і забезпечення лідерства та ефективної національної системи кібербезпеки на рівні держави. А також аналіз ключових вимог державної політики у створенні стійкої національної кіберсистеми з особливим акцентом на побудові адекватних механізмів захисту критичної інформаційної інфраструктури; окреслення пріоритетів державної політики щодо інших національних кіберпроблем, оскільки ефективна система захисту критичної інформаційної інфраструктури пов'язана з функціонуванням різних однаково центральних елементів національної кіберсистеми.

Інформаційно-комунікаційні технології (далі – ІКТ) стали центральною основою для комунальних підприємств, фінансових послуг, закладів охорони здоров'я та урядових систем зв'язку. Оскільки ці технології призначені для полегшення економічних і

DOI (Article): https: //doi.org/10.36486/np.2023.2(60).8

суспільних функцій, вони автоматично формують взаємопов'язану основу для всіх критично важливих економічних секторів і систем зв'язку в усьому світі. Однак глобальна цифрова сфера, що швидко зростає, є менш захищеною, ніж можна було б припустити, зважаючи на її центральне значення для економіки та інших функцій. Вторгнення в інформаційні системи з різних мотивів стали рутинними побічними ефектами цифрової трансформації [2]. Серйозний технологічний або антропогенний збій в інформаційній інфраструктурі може мати далекосяжні і непередбачувані наслідки. Теоретично більшість критично важливих мереж в енергетиці, транспорті та інших життєво важливих секторах не мають бути безпосередньо підключені до інтернету, а отже, повинні бути здатні уникнути збоїв. На практиці навіть закриті об'єкти критичної інфраструктури або військові мережі можуть бути інфіковані і постраждати від наслідків кібервторгнення. Усвідомлюючи неминучість кібервразливостей, політики почали шукати відповіді на них, щоб убезпечити критично важливу інфраструктуру. Саме тому в Європі та США сформувався широкий консенсус щодо включення аспекту кіберстійкості в урядові та галузеві нормативні акти [3].

В умовах широкомасштабного вторгнення рф, швидкої цифрової трансформації, яка змінює всі економіки і суспільства, важливо підвищувати обізнаність про кіберзагрози як серед громадськості, так і у приватному та державному секторах. Кібербезпека є одним із ключових елементів обороноздатності держави. Сьогодні кібервійна в розпалі. Російські хакери здійснюють цілеспрямовані атаки на органи влади та інфраструктурні підприємства для того, щоб знизити або паралізувати економічну активність громади, підвищити соціальну напругу через відсутність або нестабільну роботу підприємств, які забезпечують роботу критичної інфраструктури [4].

Ефективне реагування на кіберзагрози вимагає цілісного, загальнонаціонального підходу, в якому кібербезпека буде інтегрована у багатьох сферах державної політики. Таким чином, можна створити середовище, яке буде відносно захищене від серйозних порушень, але це також буде тривалим процесом, який вимагає співпраці всіх основних зацікавлених сторін, включно з приватним сектором. Крім того, воно вимагає зміни мислення щодо того, наскільки впливовим стає цифрове підґрунтя та його незахищеність.

Особи, відповідальні за розробку кіберполітики, стикаються зі складним завданням прийняття рішень, у яких переплітаються питання економіки, внутрішньої та національної безпеки, а окремі варіанти розроблених політик у кожній з цих сфер можуть суперечити одна одній. Країни, які хочуть бути кіберзабезпеченими, отримують вигоду саме від комплексної моделі кіберуправління, яка, оцінюючи конкуруючі політичні пріоритети, здатна збалансувати національні інтереси в кіберпросторі. Національна кіберполітика має відношення до внутрішніх справ, безпеки і зовнішньої політики, промислової та економічної політики, а також політики у сфері досліджень, освіти та технологічного розвитку [5]. Для того, щоб збалансувати всі інтереси, політики також повинні регулярно консультуватися з приватним сектором. Національна кіберполітика має забезпечити стратегічне бачення, сформулювати варіанти політики і, що дуже важливо, виділити додаткові кошти для досягнення цілей кібербезпеки.

Оскільки кіберпростір розвивається зі швидкістю інноваційного зростання, що стимулюється приватними компаніями, уряди мають різний ступінь здатності повністю орієнтуватися в цій швидкозмінній сфері. Вони повинні швидко адаптуватися, щоб бути в змозі зрозуміти динаміку цифрової трансформації та йти в ногу з рівнем інновацій, навчання та інвестицій. Ключова сфера, з якою сьогодні стикаються національні розробники кіберполітики, є захист мереж ІКТ, які підтримують надання критично важливих послуг. Але їм також необхідно розвивати спроможність реагування на інциденти на національному рівні, що охоплює критично важливі організації приватного і державного секторів, а також розвивати спроможність розслідування кіберзлочинів та переслідування злочинців. Ці сфери політики формують базовий трикутник мінімальної національної кіберсистеми, здатної захищати критично важливі послуги, боротися з кіберзлочинністю та забезпечувати достатній потенціал реагування на інциденти [6].

У кожній добре скоординованій національній кіберсистемі повинна існувати керівна структура, яка бере на себе відповідальність за прийняття рішень на вищому рівні. Її мандат полягає в тому, щоб забезпечити бачення, нагляд і ресурси для національних зусиль у сфері кібербезпеки. Керівна структура, еквівалент Національної ради з кібербезпеки, в ідеалі повинна підпорядковуватися вищому органу, який приймає рішення з питань національної безпеки або врегулювання кризових ситуацій, в безпосередній близькості до уряду, щоб включити кібербезпеку до національних пріоритетів на найвищому рівні. Провідна структура також має взяти на себе відповідальність за розроблення та оновлення національних стратегій і політик, нагляд за реалізацією пріоритетів національної політики. До складу національної структури управління кіберпростором повинні входити не лише вищі державні службовці, які відповідають за реагування на кіберінциденти, захист критичної інформаційної інфраструктури та боротьбу з кіберзлочинністю, а й ширше коло вищих державних службовців [7]. Окрім правоохоронних органів, до неї, безумовно, мають бути залучені дипломати, представники оборонного відомства, політики у сфері науки та освіти, представники торговельної та промислової політики, а також, якщо це можливо, необхідно передбачити консультації з асоціаціями приватного сектору. Широке коло зацікавлених сторін сприятиме підвищенню обізнаності про різні елементи національної політики кібербезпеки і про їхнє значення для широкого спектру цифрових питань. Це також дозволить досягти консенсусу щодо низки пріоритетів національної кіберполітики.

Як зазначалося, реагування на кіберінциденти, боротьба з кіберзлочинністю та захист критичної інформаційної інфраструктури (далі – ЗКІІ) є ключовими компонентами національної кіберполітики. Як правило, на політичному рівні формується модель організації цих елементів у функціонуючу і добре скоординовану національну кіберсистему. Хоча всі згадані сфери політики однаково важливі для національної кіберстійкості, не завжди очевидно, де в різних країнах інституційно знаходиться центр реагування на кіберінциденти та ЗКІІ.

Боротьба з кіберзлочинністю зазвичай належить до компетенції Міністерства внутрішніх справ, яке разом з іншими органами правопорядку очолює цю сферу політики. Через наскрізний характер реагування на кіберінциденти та ЗКІІ країни знайшли дуже

різні рішення щодо того, де розмістити ці можливості у своєму інституційному ландшафті. В європейських країнах національна група реагування на кіберінциденти (далі – CERT) може належати різним установам, таким як регулятор телекомунікаційного сектору, IT-агентство, розвідувальна організація, міністерство внутрішніх справ, оборонна структура або офіс кабінету міністрів. Деякі країни створили спеціальне національне кібер-агентство, яке діє як координаційний центр для реагування на інциденти та ЗКІІ, а деякі країни мають таку можливість як частину свого апарату внутрішньої безпеки.

Зокрема, в Україні CERT-UA є спеціалізованим структурним підрозділом Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України та його діяльність врегульована законами України «Про Державну службу спеціального зв'язку та захисту інформації» [8] та «Про основні засади забезпечення кібербезпеки України» [9].

Насправді не так важливо, де саме знаходяться ці можливості, як те, що вони належать авторитетному органу, який здатен координувати національну кібердіяльність і може взяти на себе горизонтальну роль у скликанні всіх необхідних зацікавлених сторін, включно з приватним сектором. Сили реагування на інциденти та органи ЗКІІ також можуть бути розташовані в різних адміністративних одиницях, але через їхні специфічні оперативні функції та політичну компетенцію вони повинні працювати в тісній координації.

Здатність боротися з кіберзлочинністю є іншим не менш важливим компонентом національної кіберполітики. Вона передбачає наявність певного рівня законодавства для криміналізації кіберзлочинців, а також спроможність збирати електронні докази і розслідувати злочини у сфері високих технологій. Основні виклики включають підготовку поліцейських, які першими реагують на кіберзлочини, зважаючи на те, що традиційні злочини все частіше пов'язані з електронними доказами. Країни також повинні навчати суддів, прокурорів, слідчих та інших працівників судової системи щодо інструментів кіберзлочинності, які швидко розвиваються. Крім того, судові органи або поліцейські організації мають створити підрозділи кібер-криміналістики для розслідування кібер-злочинів, що іноді надто вартісно для менш розвинених країн. ЄС запустив мережу лабораторій кібер-криміналістики у країнах-членах, що є гарним прикладом для інших регіонів.

Важливе коло питань пов'язане з економічними аспектами кібербезпеки і охоплює промислову та торговельну політику. Недобросовісна торговельна практика та економічні збитки, спричинені від кіберкрадіжки інтелектуальної власності, – це виклик, з яким дедалі частіше стикаються державні політики. Знову ж таки отримання загального уявлення про масштаби втрат інтелектуальної власності є делікатним балансуючим актом. Для оцінки наслідків кіберкрадіжки необхідна тісна співпраця з великими промисловими гравцями. Крім того, інструментарій політичного реагування для протидії крадіжкам інтелектуальної власності все ще розвивається і потребує як національних, так і міжнародних елементів підтримки. Наприклад, покарання за кібер-крадіжку через відповідні механізми міжнародної торгівлі може бути одним зі способів реагування на таку недобросовісну торговельну практику [2].

Очевидною політичною метою має бути підтримка промислової політики, яка вимагає вищого рівня стандартів безпеки в галузі ІКТ та інновацій з використанням ІКТ в інших галузях, оскільки цей сектор відіграватиме значну роль у підтримці майбутнього економічного зростання саме в країнах з розвиненою економікою. Досягненню більшої довіри та безпеки до продуктів ІКТ може сприяти цільове фінансування досліджень і розробок у сфері кібербезпеки, заохочення інновацій у сфері безпеки та створення кластерів стартапів. Це особливо актуально в епоху інтернету речей, коли автомобілі, побутова техніка та інше обладнання будуть підключені до інтернету.

Для великих компаній все частіше постає питання про те, скільки їм потрібно інвестувати в кіберстійкість, щоб стати кіберзахищеними. Існує певний поріг інвестицій, який керівництво компанії вважає пропорційним сприйнятому рівню ризику. І, безумовно, є рівень вище цього порогу, який не може бути досягнутий без надмірних інвестицій, які можуть бути економічно невиправданими. Як логічний наслідок, страхова галузь долучилася до кібердебатів, додавши важливий елемент обґрунтованої оцінки ризиків для приватних підприємств. Страхові компанії можуть забезпечити вимірний вплив на зниження ризиків через механізм застосування фінансових наслідків за вжиття заходів безпеки промисловими організаціями. У США розпочалися ініціативи з визначення відповідних метрик кіберризиків та збитків за участю представників страхових компаній та керівництва галузі. Уряди повинні заохочувати зусилля щодо аналізу потенційного позитивного впливу страхових практик на плани ЗКІІ.

Дуже важливим елементом буде відпрацювання способів реагування на великі кібератаки, а також включення кібер-аспектів у національні навчання з врегулювання кризових ситуацій. Ідеальний сценарій кібернавчань охоплюватиме як технічні, так і стратегічні аспекти прийняття рішень, на додаток до кібернавчань, які проводяться в лабораторіях лише серед технічного персоналу. Хоча технічні навчання є цінними з оперативної точки зору, національні командно-штабні навчання мають включати різні відомства, відповідальні за надання критично важливих послуг, керівників приватного сектору і ключовий персонал органів державного управління. Уряди також повинні мати можливість відпрацювати національну кризу з кількома елементами, одним з яких може бути кіберпорушення життєво важливих мереж або послуг. Добре проведені навчання дозволять підготувати плани на випадок надзвичайних ситуацій і оцінити готовність національних кіберструктур. Навчання також нададуть інформацію політикам, куди слід спрямувати додаткові інвестиції, наприклад, на придбання альтернативних засобів зв'язку, посилення мережевого захисту в життєво важливих сферах тощо.

Важливим, у контексті широкомасштабного вторгнення рф на територію України, використання агресором усього спектру гібридних загроз, зокрема кібератак, також є врахування кібер-аспектів при плануванні політики оборони і безпеки. Сили оборони мають бути здатні захистити себе і діяти в умовах кібератаки; вони повинні мати спеціалізовані структури реагування на інциденти для пом'якшення наслідків кібервторгнень, і вони мають бути включені в національне планування дій на випадок надзвичайних ситуацій і визначення їх місця та ролі. Посилення кібербезпеки в системі національної безпеки, оборони, врегулювання кризових ситуацій та захист критичної інфраструк-

тури вимагатиме вдосконалених спроможностей з виявлення та аналізу кіберзагроз на національному рівні.

Наразі слід не забувати, що навчання та освіта в галузі кібербезпеки – це широка сфера, яка включає в себе підготовку персоналу з ІТ-безпеки та інших спеціалістів, а також інформування громадськості та керівників щодо кіберзагроз. Нестача експертів з ІТ-безпеки вже є критичною, і багато урядів розробляють складні механізми, щоб утримати найталановитіших кіберфахівців у себе вдома. Включення елементів комп'ютерної та інформаційної безпеки в усі навчальні програми з інформаційних технологій є вимогою часу, паралельно зі збільшенням інвестицій у спеціалізовану підготовку з ІТ-безпеки та мережевого захисту. Пріоритетом має стати фінансування прикладних і теоретичних досліджень в галузі інформатики, а також заохочення міждисциплінарних кібердосліджень для підготовки наступного покоління осіб, які приймають рішення, і аналітиків.

Нарешті центральна група проблемних питань пов'язана із занепокоєнням щодо глобальної кіберстабільності та необхідністю введення поняття відповідальності держави в кіберпросторі. У сфері міжнародної безпеки, пов'язаної з кіберпростором, існує кілька ініціатив, які сприяють покращенню глобальної кібербезпеки, зобов'язуючи провідні уряди дотримуватися правил і норм. ООН, ОБСЄ та інші міжнародні організації зробили кілька кроків для розробки кібернорм і заходів зі зміцнення довіри, спрямованих на запобігання кіберконфліктам і зниження напруженості між державними суб'єктами [10]. Дипломатичне співтовариство разом з агентствами розвитку також допомагає країнам, що розвиваються, боротися з кіберзлочинністю та створювати мінімальні можливості реагування на кіберінциденти.

Таким чином, в умовах сучасних викликів, задля використання усіх переваг цифрової трансформації, об'єктивною вимогою є активізація зусиль у сфері кібербезпеки та посилення кіберстійкості. Основною метою національних зусиль у сфері кібербезпеки має бути зміцнення кібербезпеки критично важливих служб і секторів економіки, що супроводжується адекватним реагуванням на інциденти та розслідуванням кіберзлочинів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Roger Hurwitz*. Keeping Cool: Steps for Avoiding Conflict and Escalation in Cyberspace. Georgetown Journal of International Affairs: Georgetown University. 2014.

2. *Myriam Dunn Cavelty, Manuel Suter*. The Art of CIIP Strategy: Taking Stock of Content and Processes. Springer, 2012.

3. *Heli Tiirmaa-Klaar.* Building national cyber resilience and protecting critical information infrastructure, Journal of Cyber Policy, 2016. 1:1. P. 94–106.

4. Національний саміт кібербезпеки. URL: https://www.myvin.com.ua/news/17100-u-vinnytsi-vidbuvsia-natsionalnyi-samit-kiberbezpeky (дата звернення: 01.06.2023).

5. *Kahan J. H.* Resilience Redux: Buzzword or Basis for Homeland Security. Homeland Security Affairs. 2015. Vol.11. URL: www.hsaj.org/articles/1308 (дата звернення: 01.06.2023).

6. *Prior T., Hagmann J.* Measuring resilience: methodological and political challenges of a trend security concept. J. Risk Research. 2014. Vol. 17. №. 3. P. 281–298.

7. Organizational Resilience – Concepts and Evaluation Method / *Robert B.* et al. Pressesinternationales Polytechnique, 2010. 46 p.

8. Про Державну службу спеціального зв'язку та захисту інформації: Закон України від 23.02.2006 № 3475-IV. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text (дата звернення: 01.06.2023).

9. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 01.06.2023).

10. Dunn Cavelty M., Kaufmann M., Søby Kristensen K. Resilience and (in)security: Practices, subjects, temporalities. *Security Dialogue*. 2015. Vol. 46. P. 3–14.

REFERENCES

1. *Roger Hurwitz* (2014). Keeping Cool: Steps for Avoiding Conflict and Escalation in Cyberspace. Georgetown Journal of International Affairs: Georgetown University [in English].

2. *Myriam Dunn Cavelty, Manuel Suter* (2012). The Art of CIIP Strategy: Taking Stock of Content and Processes. Springer [in English].

3. *Heli Tiirmaa-Klaar* (2016). Building national cyber resilience and protecting critical information infrastructure, Journal of Cyber Policy. 1:1, P. 94-106 [in English].

4. Natsionalnyi samit kiberbezpeky. "National Cybersecurity Summit". URL: https://www.myvin.com.ua/news/17100-u-vinnytsi-vidbuvsia-natsionalnyi-samit-kiberbezpeky. (Date of Application: 01.06.2023) [in Ukrainian].

5. Kahan J.H. (2015). Resilience Redux: Buzzword or Basis for Homeland Security. Homeland Security Affairs. Vol. 11. URL: www.hsaj.org/articles/1308. (Date of Application: 01.06.2023) [in English].

6. *Prior T., Hagmann J*. (2014). Measuring resilience: methodological and political challenges of a trend security concept. J. Risk Research. Vol. 17. №. 3. P. 281–298 [in English].

7. Organizational Resilience – Concepts and Evaluation Method / Robert B. et al. Presses internationales Polytechnique, 2010. 46 p. [in English].

8. Pro Derzhavnu sluzhbu spetsialnoho zviazku ta zakhystu informatsii. "On the State service for special communications and information protection": Law of Ukraine of 23.02.2006. №. 3475-IV. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text. (Date of Application: 01.06.2023) [in Ukrainian].

9. Pro osnovni zasady zabezpechenna kiberbezpeky Ukrainy. "On the basic principles of ensuring cybersecurity of Ukraine": Law of Ukraine of 05.10.2017 №. 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text. (Date of Application: 01.06.2023) [in Ukrainian].

10. *Dunn Cavelty M., Kaufmann M., Søby Kristensen K*. (2015). Resilience and (in)security: Practices, subjects, temporalities. Security Dialogue. Vol. 46. P. 3–14 [in English].

UDC 004.056

Demediuk Serhii,
Candidate of Juridical Sciences (Ph.D), Deputy Secretary of the National Security and Defense Council of Ukraine, Kyiv, Ukraine,
ORCID ID 0009-0008-1359-5265

DEVELOPMENT OF NATIONAL CYBER RESILIENCE AND PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURE

The article concentrates on the analysis of problematic issues concerning development of the national system of society's cyber resilience. Methodologically, the focus is on

awareness of key areas: protecting critical information infrastructure, combating cybercrime, and improving the ability to react in the face of cyber incidents. According to the author, at the political level, these areas require the formation of a model for organizing them into a functioning and well-coordinated national cyber system. The article argues that, in the face of modern challenges, increasing efforts in the area of cyber security and strengthening cyber resilience is an objective requirement for taking full advantage of the digital transformation.

The key requirements of the state policy in the field of establishing a sustainable national cyber system are reviewed, with particular attention paid to building adequate mechanisms for the protection of critical information infrastructure. The priorities of state policy regarding other national cyber problems are outlined, since an effective system of protection of critical information infrastructure is related to the functioning of various equally central elements of the national cyber system.

Attention focuses on the fact that national cyber policy links with internal affairs, defense security and foreign policy, industrial and economic policy, and research, education, and technological development policy. The peculiarities of the implementation of the key requirements of state policy in the development of a sustainable national cyber system are revealed, with a special emphasis on the construction of adequate mechanisms for the protection of critical information infrastructure.

Keywords: cyber security, cyber incident, cyber crime, critical information infrastructure, cyber resilience.

Отримано 06.06.2023