ISSN 2072-8670 (Print) **НАУКА І ПРАВООХОРОНА**
NAUKA I PRAVOOKHORONA
DOI (Issue): https://doi.org/10.36486/np.2023.3(61) **Issue 3(61) 2023**

АДМІНІСТРАТИВНЕ ПРАВО І ПРОЦЕС. ФІНАНСОВЕ ПРАВО

УДК 004.56

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

ЗАХИСТ КРИТИЧНО ВАЖЛИВИХ ПОСЛУГ У ЦИФРОВУ ЕПОХУ

Статтю присвячено аналізу проблемних питань щодо розбудови національної системи кіберстійкості суспільства. Методологічно зосереджується увага на усвідомленні ключових напрямів – захисту критично важливої інформаційної інфраструктури. Акцентовано увагу на моделях щодо розвитку системи захисту КВІІ та на основі характерних узагальнень визначено їх своєрідність. Розкрито особливості реалізації ключових вимог державної політики у розбудові стійкої національної кіберсистеми з акцентом на нормативно-правовому регулюванні системи кібербезпеки, необхідності розвитку дієвого державно-приватного партнерства суб'єктів, розбудови адекватної регуляторної політики на засадах взаєморозуміння та ефективності механізмів захисту критичної інформаційної інфраструктури.

Ключові слова: *кібербезпека, кіберстійкість, захист критично важливої інформаційної інфраструктури, ЗКІІ.*

Розвиток цифрових технологій формує принципові виклики глобальному світу та національним економікам, суттєво впливає на формування базових засад надання критично важливих послуг. Концептуально система кібербезпеки передбачає різні напрями реалізації: захист критичної інфраструктури, зниження рівня кіберзлочинності, підвищення обізнаності та дотримання інтересів національної безпеки і зовнішньої політики, що формує також основу кіберстійкості країни [1].

Метою статті є проведення аналізу ключових вимог щодо формування державної політики та розбудови адекватних механізмів захисту критичної інформаційної інфраструктури, що є одним з пріоритетів забезпечення кібербезпеки держави та забезпечення національної кіберстійкості.

Захист критично важливих національних кіберактивів є основою для зусиль країн у сфері кібербезпеки. Для політиків, перед якими стоїть завдання розвивати національну систему кібербезпеки, питання визначення і захисту критично важливої інформаційної інфраструктури (далі ЗКІІ) змістилося від переважно фізичного розуміння інфраструк-

DOI (Article): https://doi.org/10.36486/np.2023.3(61).3

тури до захисту критично важливих послуг. ЗКІІ використовується для узагальненого позначення захисту життєво важливих ІТ-сервісів, які підтримують надання критично важливих послуг як приватними, так і державними організаціями [2].

Якщо поглянути на історію ЗКІІ, то цей термін з'явився під час холодної війни, коли перед оборонним відомством було поставлено завдання наглядати за критично важливими цивільними об'єктами. Визнаючи зростаючу залежність сучасного суспільства від цифрової інфраструктури, Комісія з питань захисту критичної інфраструктури при Президентові США у 1997 році підготувала звіт, який став першим відомим публічним документом, що обговорював кібербезпеку цілої нації. У ньому зазначалося: "Одним з найважливіших є визнання того, що власники і оператори наших критично важливих об'єктів інфраструктури зараз знаходяться на передовій наших зусиль із забезпечення безпеки. Саме вони найбільш вразливі до кібератак. І ця вразливість ставить під загрозу нашу національну безпеку, глобальну економічну конкурентоспроможність і внутрішній добробут" [3].

Це питання, безумовно, є актуальним для багатьох країн і сьогодні через різке зростання залежності від цифрової складової сучасної економіки і суспільства. Тим не менш, обізнаність та ресурси, що виділяються на національну кібербезпеку, залишаються дуже нерівномірними навіть серед індустріальних країн.

У той же час, кількість суб'єктів, потенційно здатних до незаконної кіберактивності з різних мотивів, стрімко зростає. З появою мільйонів нових інтернет-користувачів на ринках, що формуються, і в країнах, що розвиваються, відбудеться стрибок з 2,5 мільярдів інтернет-користувачів у 2015 році до 5 мільярдів користувачів до 2025 року [4]. Тому проблема кібербезпеки стає загрозою економічному зростанню та національній безпеці не лише в розвинених індустріальних країнах, а й у країнах з економікою, що розвивається.

Для покращення кібербезпеки критично важливих послуг основна увага має бути зосереджена на організаційних аспектах, а необхідні технічні компоненти – на вдосконаленому управлінні кіберризиками. Через складність захисту кіберелементів критично важливих послуг, питання, на яке слід відповісти насамперед полягає в тому, як організувати це завдання і забезпечити необхідне лідерство уряду у протидії кібервикликам. Нещодавні рекомендації Організації економічного співробітництва та розвитку (ОЕСР) дійшли висновку: "Замість того, щоб розглядати цифровий ризик як технічну проблему, яка вимагає технічних рішень, до нього слід підходити як до економічного ризику; отже, він повинен бути невід'ємною частиною процесів управління ризиками та прийняття рішень в організації" [5].

Наразі має місце думка щодо певних проблем, пов'язаних з ідентифікацією ІТ-послуг, які підтримують найбільш критичні послуги. Наявність такого переліку критично важливих секторів є необхідністю, але насправді перелік критично важливої інфраструктури є досить загальними і теоретичними [6]. Тому таке завдання буде мати місце постійно з метою більш детального визначення найбільш важливих послуг у кожному секторі і регулярне оновлення цього переліку, включаючи також нові послуги, що з'являються в онлайн економіці. Результат такої роботи буде різним у кожній країні,

залежно від її економічної структури та інших факторів. Але існують базові підходи до вирішення проблеми. Наприклад, послуга може вважатися життєво важливою для нації, якщо вона займає 5% ринку або створює понад 5% ВВП.

Перелік компаній та організацій, що надають найбільш важливі послуги, має визначатися тим самим міжвідомчим механізмом, який визначає найбільш важливі послуги. Водночас такий перелік переважно є конфіденційним. Правило конфіденційності також слугує інтересам приватного сектору. Багато експертів можуть вважати, що формування переліку життєво важливих послуг та операторів забирає багато часу та коштів і не підходить для країн з великою кількістю критично важливих операторів. Але обмеження наприклад в 5% все ж формує певним чином помірний список найбільш важливих послуг. І якщо уряд вирішив розпочати державно-приватне партнерство, яке допоможе операторам критично важливих послуг захистити свої сервіси, чіткий поріг найбільш важливих допоможе спрямувати ресурси на центральні частини національної критично важливої інформаційної інфраструктури.

Компанії також можуть оцінити конкретний перелік послуг, оскільки він надає їм рекомендації щодо того, на чому слід зосередити зусилля з безпеки на додаток до їхніх ключових бізнес-операцій. Наприклад, компанії можуть дізнатися, що не всі послуги, які вони надають, вважаються критично важливими з національної точки зору, що дозволить їм не витрачати занадто багато коштів на заходи безпеки. По-друге, точний перелік також полегшить подальший аудит та управління ризиками критично важливих операторів, що допоможе підвищити їхню загальну стійкість та зменшити ризики для ІТ-систем та мереж, що підтримують критично важливі послуги.

Важливим елементом розвитку системи ЗКІІ є державно-приватне партнерство. У більшості країн постачальники критично важливих послуг належать до приватного сектору, тому уряди повинні прорахувати, на чому сконцентрувати свої зусилля, перш ніж звертатися до приватного сектору з проханням додати рівень додаткового захисту до певних послуг. Відомим є вислів у сфері кібербезпеки – "державно-приватне партнерство" працює лише тоді, коли обидві сторони домовилися про чіткий набір цілей і параметрів співпраці [2]. Для стратегічного лідерства уряд має визначити, що захищати і як визначити критичні послуги. Він також повинен зібрати разом ключових галузевих і міжгалузевих гравців і запропонувати перелік стимулів для співпраці. Ці стимули можуть включати спеціалізоване навчання, огляд взаємозалежності між критично важливими операторами, спільні навчання, ресурси для фінансування резервного копіювання та засобів відновлення, а також інші вимоги, які диктуються інтересами національної безпеки.

Стандартне занепокоєння приватного сектору полягає в тому, щоб мати чітке розуміння того, що очікується від нього в межах кіберпартнерства з урядом. Постачальники критично важливих послуг вже зобов'язані дотримуватися багатьох правил, а кібервимоги без чітких стимулів з боку уряду можуть не створити сприятливого клімату для покращення безпеки. Якщо компанії не помічають відповідних зусиль з боку урядів щодо інвестування в кіберстійкість, або якщо вони вважають, що всі кіберзадачі покладені виключно на них, це, ймовірно, не сприятиме кращому кіберзахисту нації.

Тому успішне державно-приватне партнерство починається з правильного ставлення з боку урядів, з чітко визначеного національного бачення того, як досягти захисту критично важливих послуг, і розуміння того, який внесок обидві сторони зроблять для досягнення цієї мети.

Одним із найбільш важливих аспектів національної системи ЗКІІ є пошук відповідної організаційної моделі, яка сприятиме ефективній та стабільній роботі в цій сфері. Достатньо глибокий аналіз акцентує увагу на різних моделях ЗКІІ, і хоча немає двох абсолютно однакових моделей, все ж є певні закономірності, що склалися в Європі. Початково такі системи сформувалися в невеликих європейських країнах і здебільшого базувалися на міцних довірчих відносинах в однорідних суспільствах, де основна група критично важливих компаній і національних кіберорганізацій розробили системи обміну технічною кіберінформацією та раннього попередження з критично важливими операторами. На початковому етапі було створено окремий орган ЗКІІ, який виконував лише політичні функції і діяв як національний координатор, здійснюючи нагляд і консультування критично важливих компаній і організацій. Водночас цей орган інформує політиків вищого рівня, проводить навчання, готує національні кібернавчання і підтримує зв'язок з ключовими державними установами. В ідеалі така установа повинна бути розташована разом з національною структурою реагування на інциденти (CERT), щоб мати технічну кіберкомпетентність, а також мати доступ до оперативної інформації з кібербезпеки.

У деяких європейських країнах модель базується на галузевих підходах до ЗКІІ і тому відіграють більш важливу роль. Галузеві регулятори не обов'язково є найбільш компетентними кіберорганами, але оскільки ЗКІІ часто організована на галузевій основі, регулятори також мають мандат на нагляд за виконанням вимог щодо управління кіберризиками та звітності про інциденти. Цілісний підхід до ЗКІІ, коли кібербезпека інтегрована з фізичною та кадровою безпекою, добре слугує загальним цілям управління ризиками операторів критично важливих послуг. Деякі національні агентства ЗКІІ також демонструють здатність брати на себе наглядову і консультативну роль з питань ЗКІІ [7].

Існує також модель централізованого змісту з сильним кіберорганом у центрі національних зусиль, який має мандат на нагляд за реалізацією цілей ЗКІІ. У цьому випадку центральний орган також повинен мати можливість надавати корисні рекомендації та певну технічну допомогу постачальникам критично важливих послуг, а також не нехтувати галузевими специфікаціями у вимогах до кібербезпеки.

У більшості країн галузеві регулятори повинні бути більш обізнаними щодо кіберризиків і з часом відігравати певну роль в управлінні та нагляді за управлінням кіберризиками постачальників критично важливих послуг. Однак, оскільки багато європейських країн є малими або середніми державами, вони можуть не мати достатньої кількості кіберспеціалістів у всіх галузевих регуляторних органах, і було б економічно доцільно зосередити завдання з управління кіберризиками в національній організації ЗКІІ, яка тісно співпрацює з галузевими органами влади. В ЄС багато галузевих вимог до безпеки визначаються загальноєвропейськими регуляторними органами. Ці

гармонізовані європейські вимоги сприяють функціонуванню внутрішнього ринку та операторів критично важливих послуг, але національні уряди все одно здійснюють нагляд за виконанням нормативних актів.

Важливо зазначити, що кожна країна повинна знайти власну модель захисту критично важливих послуг у цифрову епоху. Досвід європейських країн показує, що центральним осередком національних зусиль у сфері кібербезпеки, як правило, є сильна державна установа з солідним фінансуванням і політичним керівництвом, орієнтованим на безпеку. Оскільки національна організація ЗКІІ повинна мати можливість залучати широке коло зацікавлених сторін з державного і приватного секторів, вона виграє від приналежності до національної установи, яка має прямий доступ до вищого політичного керівництва і володіє певним ступенем повноважень для здійснення нагляду.

Розбудова певної моделі ЗКІІ, створення відповідних органів, передбачає і відповідні регуляторні ініціативи, що сприяють підвищенню кібербезпеки критично важливих послуг. З цього приводу тривалий час у розвинених країнах серед суб'єктів кібербезпеки відбувалася дискусія щодо того, чи варто здійснювати регуляторні функції у сфері кібербезпеки. Представники національної безпеки та правоохоронних органів виступали за регулювання, тоді як ІТ-розробники та приватний сектор іноді запекло протистояли цьому. Оскільки більшість індустріальних країн зробили вибір на користь кіберрегулювання, спільною позицією стало посилення управління ризиками ІТ-безпеки в компаніях та організаціях державного сектору, які забезпечують критично важливу інфраструктуру та послуги. Стало очевидним, що для боротьби зі стрімким зростанням кіберзагроз необхідне втручання держави.

Після кібератаки на Естонію у 2007 році багато технологічно розвинених урядів почали зміцнювати свою національну кіберстійкість, а рівень обізнаності в державній політиці стрімко зростав. Після атак Stuxnet і Saudi Aramco, а також зростаючої тенденції використання програм-вимагачів проти комунальних підприємств, на національному рівні з'явився новий чіткий політичний напрямок захисту критично важливих послуг [8, 9]. Однак у деяких країнах законопроєктні ініціативи щодо підвищення кіберстійкості зазнали серйозних невдач, зокрема у 2012 році Сенатом США був відхилений Закон Лібермана про кібербезпеку. Але у 2013 році Указом Президента США було визначено новий курс для галузевої практики управління кіберризиками [10].

Згодом Національний інститут стандартів і технологій (*National Institute of Standards and Technology – NIST*) підготував збірник найкращих галузевих практик під назвою "Концепція кібербезпеки" [11]. Концепція NIST сприяла збору цінних передових практик у сфері кібербезпеки, оскільки вона була розроблена із залученням найкращих галузевих експертів. Однак, оскільки вона залишається "добровільною", важко виміряти її ефективність. Наприкінці 2015 року США прийняли Закон про обмін інформацією з питань кібербезпеки як частину більш широкого законопроєкту [12]. Закон не лише сприяв обміну інформацією між приватним сектором та урядом, а й зосереджував увагу на превентивних та оборонних заходах для захисту критично важливої інфраструктури, федерального уряду та уряду штатів, а також установ охорони

здоров'я [13]. Закон також включає інші важливі елементи національної кібербезпеки і зобов'язує Міністерство внутрішньої безпеки (Department of Homeland Security) та інші урядові установи США вжити необхідних заходів для запобігання та реагування на кіберзагрози.

Водночас Європейський Союз наприкінці 2015 року погодив Директиву про мережеву та інформаційну безпеку (*Directive on Network and Information Security - NIS*). Втім, окремі європейські країни вже мали відповідне національне законодавство, що врегульовувало питання кібербезпеки. Наприклад, у 2009 році Естонія ухвалила закон, який містив детальний перелік критично важливих послуг, з обов'язковим управлінням кіберризиками та звітуванням про інциденти операторами критично важливих послуг [14]. На той час Естонія була першою європейською країною, яка включила в закон перелік детальних критично важливих послуг у різних секторах, що викликало багато запитань у більш ліберальних кіберколах. До 2015 року інші європейські країни підготували подібні закони, хоча і з різним рівнем деталізації. Франція визначила кібербезпеку своїм головним пріоритетом у кількох Білих книгах, починаючи з 2009 року; Німеччина ухвалила закон про ІТ-безпеку у 2015 році. Багато інших європейських країн прийняли комплексні національні стратегії кібербезпеки [2].

Директива ЄС про мережеву та інформаційну безпеку (NIS) базується на комплексному регулюванні кібербезпеки з багатьма елементами. Вона спрямована на створення рівних умов для країн-членів ЄС, встановлюючи вимогу щодо наявності компетентного кіберорган, а також технічної спроможності реагування на інциденти на національному рівні. Вона також заохочує до співпраці між державами-членами для полегшення обміну інформацією та оперативного співробітництва щодо інцидентів. Крім того, вона забезпечує впровадження заходів безпеки в ключових секторах у всіх країнах-членах ЄС, включаючи енергетику, транспорт, водопостачання, банківські, медичні та фінансові послуги. Директива також поширює заходи ІТ-безпеки на постачальників цифрових послуг, таких як онлайн-маркети.

Водночас важливим питанням залишалося те, як ці регуляторні кроки насправді вплинуть на стан кіберстійкості критично важливих об'єктів інфраструктури та послуг. Багато експертів приватного сектору попереджали уряди, що надмірно суворе регулювання може призвести до неналежних зусиль з дотримання вимог, які можуть бути малоефективними щодо посилення реальної кібербезпеки. На початковому етапі державного регулювання кіберпростору в цих країнах, навіть з розвиненою індустріальною економікою, ще було занадто рано оцінювати ефективність такого регулювання. Однак досвід європейських країн, які вже запровадили відповідне регулювання, вказував на досить позитивні результати. Наприклад, уряд Естонії розгорнув допомогу для багатьох компаній щодо поглиблення уваги управлінню кіберризиками, проведенню навчань та підвищення обізнаності про кіберризики. Ці кроки супроводжувалися "м'яким" регулюванням, а також було створено державне агентство з мандатом нагляду за реалізацією національних пріоритетів у сфері ЗКІІ. У Німеччині прийняття закону про ІТ-безпеку сприяло розвитку державно-приватного партнерства у сфері кібербезпеки.

Резюмуючи щодо Директиви NIS, варто зазначити, що вона зосереджується переважно на організаційних аспектах національних кіберзаходів, закликаючи країни-члени ЄС розробити національне бачення та розбудовувати кіберстійкість разом з приватним сектором. Вона не містить надто детальних технічних вимог, а зосереджується на створенні організаційних меж для національної кібербезпеки у ключових секторах.

Таким чином, в умовах цифрової трансформації, об'єктивною вимогою є активізація зусиль у сфері кібербезпеки та посилення кіберстійкості. Прикладом цього процесу є законодавчі ініціативи економічно розвинених країн, зокрема США та ЄС. Урядами цих країн ухвалено нормативно-правові акти з кібербезпеки, де обізнаність щодо кібербезпеки критично важливих послуг є найвищим пріоритетом для осіб, які приймають рішення. У європейських країнах, які вже обрали регуляторний підхід, рівень обізнаності з питань кібербезпеки серед вищого керівництва та керівників компаній є високим. Оскільки перші кроки в регулюванні здійснювалися на національному рівні і включали тісну співпрацю з приватним сектором, наразі не спостерігається очевидних невдач. Однак мають місце ризики щодо надмірного регулювання галузі, у випадку неналежних зусиль суб'єктів кібербезпеки, а також недостатніх інвестицій та лідерства урядів у цьому питанні. Водночас процес потребує постійного дослідження та пошуку найбільш адекватного рішення. Саме тому академічні установи та аналітичні центри повинні максимально зосереджувати свій потенціал на прогалинах і надавати обґрунтований аналіз щодо організації ЗКІІ на національному рівні.

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

3. Report to the President's Commission on Critical Infrastructure Protection, 1997. C. 36. URL: https://resources.sei.cmu.edu/asset_files/specialreport/ 1997_003_001_16538.pdf. (дата звернення: 14.04.2023).

4. Cyberspace 2025: Today's Decisions, Tomorrow's Terrain, Microsoft Report. June 2014. URL: https://query.prod.cms.rt.microsoft.com/cms/api/ am/binary/REXXtS (дата звернення: 14.04.2023).

5. Digital Security Risk Management for Economic and Social Prosperity: OECD Recommen dation and Companion Document, OECD 2015. URL: https://www.oecd.org/publications/digital-security-risk-management-for-economic-and-social-prosperity-9789264245471-en.htm (дата звернення: 14.04.2023).

6. Methodologies for the identi fication of Critical Information Infrastructure assets and services: Guidelines for charting elec tronic data communication networks. December 2014. P. 22–23. URL: https://www.enisa.europa.eu/ publications/methodologies-for-the-identification-of-ciis (дата звернення: 14.04.2023).

7. UK Centre for the Protection of National Infrastructure. URL: https://www.protectuk.police.uk/news-views/centre-protection-national-infrastructure-cpni-has-evolved-become-national-protective# (дата звернення: 14.04.2023).

8. Jon. R. Lindsay. Stuxnet and the Limits of Cyber Warfare. *Security Studies*. 2013. C. 365–404.

9. Bronk, C. and Tikk-Ringas, E. The Cyber Attack on Saudi Aramco. Survival–Apr–May 2013. Vol.55. Ed 2. P. 81–96.

10. US Executive Order 13636, Improving Critical Infrastructure Cybersecurity. 12 February. 2013. URL: https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/eo-13636 (дата звернення: 14.04.2023).
11. NIST Cybersecurity Framework. URL: http://www.nist.gov/cyberframework/ (дата звернення: 14.04.2023).
12. Consolidated Appropriations Act text. URL: http://docs.house.gov/billsthisweek/20151214/CPRT114-HPRT-RU00-SAHR2029-AMNT1final.pdf (дата звернення: 14.04.2023).
13. Cybersecurity Information Sharing Act 2015. URL: https://www.congress.gov/bill/114th-congress/ senate-bill/754 (дата звернення: 14.04.2023).
14. The State of Emergency Act 2009, Riigi Teataja I 2009, 39, 260. URL: https://www.riigiteataja.ee/en/eli/512052020002/consolide (дата звернення: 14.04.2023).

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. *Heli Tiirmaa-Klaar* (2016). Building national cyber resilience and protecting critical information infrastructure. Journal of Cyber Policy. Vol. 1:1. P. 94-106 [in English].
3. Report to the President's Commission on Critical Infrastructure Protection (1997). C. 36. URL: https://resources.sei.cmu.edu/asset_files/specialreport/1997_003_001_16538.pdf. (Date of Application: 14.04.2023) [in English].
4. Cyberspace 2025: Today's Decisions, Tomorrow's Terrain, Microsoft Report. June 2014. URL: https://query.prod.cms.rt.microsoft.com/cms/api/ am/binary/REXXtS. [in English].
5. Digital Security Risk Management for Economic and Social Prosperity: OECD Recommen dation and Companion Document, OECD 2015. URL: https://www.oecd.org/publications/digital-security-risk-management-for-economic-and-social-prosperity-9789264245471-en.htm. (Date of Application: 14.04.2023) [in English].
6. Methodologies for the identi fication of Critical Information Infrastructure assets and services: Guidelines for charting elec tronic data communication networks. December 2014. P. 22-23. URL: https://www.enisa.europa.eu/ publications/methodologies-for-the-identification-of-ciis. (Date of Application: 14.04.2023) [in English].
7. UK Centre for the Protection of National Infrastructure/ URL: https://www.protectuk.police.uk/news-views/centre-protection-national-infrastructure-cpni-has-evolved-become-national-protective#. (Date of Application:14.04.2023) [in English].
8. *Jon. R. Lindsay* (2013). Stuxnet and the Limits of Cyber Warfare. *Security Studies*. P. 365-404 [in English].
9. *Bronk, C. and Tikk-Ringas, E.* (2003). The Cyber Attack on Saudi Aramco. Survival–Apr–May 2013. Vol. 55. Ed 2. P. 81-96 [in English].
10. US Executive Order 13636. Improving Critical Infrastructure Cybersecurity. 12 February. 2013. URL: https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/eo-13636. (Date of Application: 14.04.2023) [in English].
11. NIST Cybersecurity Framework. URL: http://www.nist.gov/cyberframework/. (Date of Application: 14.04.2023) [in English].
12. Consolidated Appropriations Act text. URL: http://docs.house.gov/billsthisweek/20151214/CPRT114-HPRT-RU00-SAHR2029-AMNT1final.pdf. (Date of Application: 14.04.2023) [in English].
13. Cybersecurity Information Sharing Act 2015. URL: https://www.congress.gov/bill/114th-congress/ senate-bill/754. (Date of Application: 14.04.2023) [in English].
14. The State of Emergency Act 2009, Riigi Teataja I 2009, 39, 260. URL: https://www.riigiteataja.ee/en/eli/512052020002/consolide. (Date of Application: 14.04.2023) [in English].

UDC 004.56

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

PROTECTING CRITICAL SERVICES IN THE DIGITAL AGE

The article is devoted to the analysis of problematic issues related to the development of the national system of cyber resilience of society. Methodologically, attention is focused on the awareness of key areas of protection of critically important information infrastructure. It noted that awareness and resources devoted to national cyber security remain highly uneven even among industrialized countries. At the same time, the number of subjects potentially capable of illegal cyber activity for various reasons is growing rapidly.

Attention is focused on the models for the development of the critical infrastructure protection system and their features are determined on the basis of characteristic generalizations. It is noted that there is a fairly wide variety of solutions to these issues by different countries, but at the level of generalization, three approaches to model formation are distinguished: an approach based on a single national regulator; branch approach; and the development of appropriate direct partnership between private business entities and the state.

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 regulatory and legal regulation of the cyber security system, the need for the development of an effective public-private partnership of subjects, the development of an adequate regulatory policy based on mutual understanding and the effectiveness of mechanisms for protecting critical information infrastructure.

Keywords: cyber security, cyber resilience, protection of critical information infrastructure, CIIP.

Отримано 17.10.2023