Котух Євген Володимирович,
к.т.н, доцент кафедри комп'ютерних наук,
Сумський державний університет,
м. Суми
ORCID 0000-0003-4997-620X

УДК 351.865 **doi: 10.34213/tp.21.02.19**

РЕАЛІЗАЦІЯ НАЦІОНАЛЬНИХ СТРАТЕГІЙ КІБЕРБЕЗПЕКИ: ЕКОНОМІКО-ПОЛІТИЧНИЙ АСПЕКТ

Статтю присвячено розгляду проблем захисту критичної інфраструктури та врегулювання кризових ситуацій на національному рівні. Три кроки присвячено захисту саме критичної інфраструктури. Доведено, що публічно-приватне партнерство є обов'язковою умовою досягнення цих цілей захисту критичної інфраструктури.

Встановлено, що захист критичної інфраструктури окремими державами не є достатньо ефективним без відповідної співпраці на міждержавному та міжнародному рівнях. Проаналізовано новий вид дипломатичних відносин – кібердипломатію, виокремлено її три основних пріоритети (безпека, економічне співробітництво та права людини).

Ключові слова: критична інфраструктура, кібербезпека, кіберпростір, інформаційні системи, кібердипломатія, стратегія.

Постановка проблеми. Питання підтримки безпеки критичної інфраструктури є справою національної безпеки – з урахуванням чи без урахування кіберскладника. Однак мережі, що використовуються в об'єктах критичної інфраструктури, не застраховано від зростання залежності від інтернет-технологій. Тому можна стверджувати, що кібербезпека поєднується з національною безпекою здебільшого в критичній інфраструктурі. І хоч держави не мають одностайності у визначенні того, які об'єкти слід вважати критичною інфраструктурою, загальне бачення вказує на те, що такими об'єктами є надавачі найважливіших послуг усередині держави в рамках національної безпеки.

Аналіз останніх досліджень і публікацій. Кібербезпеці в публічному просторі, визначенню її стратегічних цілей присвятили свої дослідження Дж. Гілі, А. Клімбург, Д. Сміт. Дж. Мелісен досліджував провадження кібердипломатії, її витоки та особливості. М. Мак-Міллан розглядав стратегію кібербезпеки Великобританії в контексті балансу свободи й управління в Інтернеті.

Метою статті є аналіз національних стратегій кібербезпеки семи країн світу з точки зору захисту критичної інфраструктури та ролі міжнародної співпраці в цій сфері.

Виклад основного матеріалу. Одне з найскладніших завдань у сфері підтримки кібербезпеки полягає в тому, що значною частиною об'єктів критичної інфраструктури в державах з ліберальною ринковою економікою керують суб'єкти приватного сектору, а не держава, незважаючи на те, що ці об'єкти вважаються невід'ємною частиною національної безпеки. Крім того, надання приватному сектору можливості пропонувати більш безпечні та стабільні послуги пов'язано з наданням приватним надавачам послуг державної допомоги [5].

Розробники Стратегії кібербезпеки США і відповідальні за прийняття рішень у сфері кібербезпеки в цій країні створили новий інституційний механізм реалізації процесу обміну інформацією між зацікавленими сторонами

приватного і публічного секторів шляхом запуску нової Національної команди реагування на комп'ютерні надзвичайні події (National computer emergency response team, CERT) [8]. Але при цьому останнє слово залишається завжди за президентом США, рішення якого дає право застосувати кіберзброю. І це є певним недоліком, оскільки безпрецедентна швидкість кібератак здійснює суттєвий тиск на такий механізм прийняття рішень.

Операційний центр із питань безпеки інформаційних систем Франції (Operational Center of the Security of Information Systems, COSSI), головний орган Франції для координації ініціатив у сфері кібербезпеки, є основним, хто відповідає за врегулювання кризових ситуацій на національному рівні, а також за приготування та реалізацію плану дій щодо врегулювання кризових ситуацій у кіберпросторі. Наголошуючи на великому значенні критичної інфраструктури, Франція у Стратегії національної безпеки звертає особливу увагу на заходи безпеки стосовно цього середовища [4].

Слідом за боротьбою з кіберзлочинністю, другою за важливістю метою стратегії національної безпеки Великобританія визначає захист об'єктів критичної інфраструктури. Її Стратегію кібербезпеки спрямовано на розвиток публічно-приватного партнерства та заохочення обох сторін до подальшої співпраці. Наприклад, у 2018 р. уряд Великобританії виділив 14,2 млрд фунтів для 20 найбільших приватних постачальників послуг, а державні служби мали найменший персонал після Другої світової війни [10].

Необхідність співпраці описано так: "Значна частина інфраструктури, котру ми повинні захищати, знаходиться у приватній власності та керується приватним сектором. Досвід та інновації, необхідні для адекватної відповіді на загрози, буде орієнтовано на бізнес" [7]. Саме з метою активізувати публічно-приватне партнерство та заохотити обидві сторони до кращого співробітництва Великобританія внесла кардинальні зміни до своєї Стратегії кібербезпеки. Ще однією важливою метою Стратегії кібербезпеки Великобританії є захист міжнародної критичної інфраструктури. Перша і головна причина цього – боротьба, яку держава веде з кіберзлочинністю.

За показник, який демонструє намір керівництва Нідерландів мати комплексний підхід, що поєднує всі суб'єкти у сфері кібербезпеки, у Стратегії кібербезпеки Нідерландів взято налагодження відповідного рівня співпраці всіх зацікавлених сторін держави та міжнародних суб'єктів; цей показник включено до найважливіших принципів реалізації Стратегії [2]. На цьому етапі надзвичайно важливо зазначити, що стратегія Нідерландів задіює як публічні, так і приватні міжнародні суб'єкти щодо вирішення питань національної безпеки. Загалом ця частина Стратегії є, імовірно, конструктивним зразком в аспекті заходів зі зміцнення довіри, що є визначальними для міжнародних кіберальянсів.

У Стратегії кібербезпеки Німеччини захист критичної інфраструктури посідає центральне місце. Існує 10-кроковий план дій щодо захисту кіберпростору, з якого три кроки присвячено захисту саме критичної інфраструктури. При цьому публічно-приватне партнерство у плані названо обов'язковою умовою досягнення цих цілей [9]. Також було створено Раду національної кібербезпеки Німеччини, завданням якої є координування співпраці правоохоронних органів, Конституційного суду, агентств розвідки, Федерального агентства новин і окремих міністерств. Це був крок Німеччини до створення ефективної системи врегулювання кризових ситуацій у випадку виникнення інцидентів у національному кіберпросторі, а також щоб вирішити питання

того, яка владна структура має право вимагати реалізації плану дій у разі кібератаки та інших пов'язаних із цим проблем.

Варто зауважити, що визначення критичної інфраструктури відрізняються залежно від рівня процвітання держави. У зв'язку з цим у Туреччині створено чіткий перелік об'єктів, що надають критично важливі послуги [12]. При цьому відповідно до плану дій Туреччини у сфері кіберпростору, що містить галузевий аналіз ризиків для критичної інфраструктури, перевагу у сфері захисту критичної інфраструктури мають публічні організації, відповідальні за регулювання й аудит критичних секторів, а також за розроблення галузевих планів дій у надзвичайних ситуаціях і для безперервного ведення бізнесу. Туреччина також досягла значного прогресу в інституціоналізації кібербезпеки, утворивши національну Команду реагування на комп'ютерні надзвичайні події (USOM) та плануючи створити подібні команди реагування для окремих секторів. Один із найважливіших пунктів стратегічного підходу Туреччини до захисту критичної інфраструктури пов'язано з визначенням правових санкцій у відповідь на порушення безпеки критичної інфраструктури.

Індія, своєю чергою, створила Національний центр захисту критичної інформаційної інфраструктури (National Critical Information Infrastructure Protection Centre, NCIIPC), який має повноваження для підвищення рівня захисту та стійкості цієї сфери [3]. Але при цьому Індія у своїх стратегічних документах не визначає чітко найважливіших об'єктів інфраструктури.

Проте захист критичної інфраструктури окремими державами не є достатньо ефективним без відповідної співпраці на міждержавному та міжнародному рівнях. Кібердипломатію, відому також як публічна дипломатія 2.0, здебільшого сконцентровано на упровадженні технічних інновацій зі сфери комунікації й інформаційних технологій до сфери дипломатії [6]. Загалом її пов'язано зі зв'язками з громадськістю, і вона відкриває новий вимір для традиційної дипломатії, інтегруючи нові засоби, що дозволяють державам взаємодіяти не лише з високоповажними представниками, але також із пересічними громадянами з різних країн. Імовірно через слабкий і неконтрольований зв'язок зі сферою безпеки багато стратегічних документів не містять окремої частини, присвяченої кібердипломатії.

Держави зазвичай вбачають у кібердипломатії основу для формування міждержавних зв'язків і налагодження міжнародної співпраці з питань кібербезпеки. Нідерланди у Стратегії кібербезпеки підкреслюють потребу міждержавної співпраці й обіцяють брати активну участь в Форумі з управління Інтернетом від ООН (UN Forum of Internet Governance). Німеччина так само підкреслює важливість міжнародної співпраці і обіцяє активно підтримувати такі організації, як ООН, НАТО і G-7 [8].

У контексті глобальної інтернет-спільноти набір механізмів для управління Інтернетом складається з громадських організацій включно з представниками приватного сектору. На цей час двома найвпливовішими організаціями у сфері управління Інтернетом є Рада з архітектури Інтернету (Internet Architecture Board, IAB) та Інженерна рада Інтернету (Internet Engineering Task Force, IETF). Втручання держав у діяльність цих організацій є значно обмеженим. Утім низка держав надає суттєвої уваги питанням, пов'язаним із кібердипломатією та управлінням Інтернетом як складниками кібербезпеки.

Зокрема, Підрозділ із питань міжнародної кібербезпеки є інструментом управління Інтернетом у Великобританії, що був сформований під керівництвом міністра закордонних справ у 2011 р. [5]. При цьому Стратегія кібербез-

пеки Великобританії здебільшого зосереджено навколо міжнародної співпраці з метою створення основи для міжнародного кіберзаконодавства, а також для розвитку двосторонніх відносин із впливовими суб'єктами кіберпростору. У Лондоні вважають, що більш активна участь ЄС у дискусіях з питань кібербезпеки могла б сприяти формуванню більш активній стратегії в цій сфері.

На відміну від Великобританії з її міжнародним орієнтуванням, Франція наполягає на пристосуванні національної правової бази до найновіших напрацювань у сфері кібербезпеки [4].

Сама назва Стратегії кібербезпеки США – "Міжнародна стратегія дій у кіберпросторі" – вказує на те, що США вважають кіберпростір сферою, до якої повинен застосовуватись міжнародний підхід. Через це кібердипломатія набуває важливого значення для американської кіберстратегії. Наочним прикладом стратегічних змін є стратегічний документ, опублікований ще у 2003 р. за назвою "Національна стратегія підтримки безпеки кіберпростору", у якому зазначається, що США надають вирішального значення зміцненню міжнародних зв'язків і наголошують на важливості збереження свободи слова та правових санкцій щодо управління Інтернетом за ліберальним зразком [11].

Аналіз стратегічних документів Німеччини в галузі кібердипломатії показує, що в її стратегії пропонується ефективна координація для підтримки кібербезпеки в усьому світі. Німецькі стратеги розуміють кіберпростір як "простір свободи, безпеки та справедливості" [1]. Під час головування в ОБСЄ в 2016 р. Німеччина визначила три пріоритети для кібердипломатії: безпека, економічне співробітництво та права людини.

Індія у своїй стратегії чітко говорить про налагодження двосторонніх та багатосторонніх відносин, а також про співпрацю з питань кібербезпеки з іншими країнами. Керівництво держави проводить двосторонні діалоги з питань кібербезпеки з Великобританією, США та Німеччиною. Це поєднується із запуском ініціативи Цифрова Індія (Digital India) – для її реалізації створюється багатосторонні зв'язки. "Кібердипломатія – це сфера, що надалі розвивається. Це вимагає складних знань з технологій, права, політики тощо. Уряд Індії зосереджується на цьому" [3].

Висновки з цього дослідження та перспективи подальших розвідок у цьому напрямі. Отже, виклики кібербезпеки стосуються всіх країн, і жодна з них не стикається з абсолютно однаковими проблемами, але більшість із них є подібними, що дає можливість виробляти спільні універсальні рішення, які потім можна адаптувати до умов конкретних держав. При цьому кіберпростір є невід'ємною частиною розвитку будь-якої сучасної держави, адже потужний кіберпотенціал має вирішальне значення для прогресу та розвитку держав в економічній, політичній та соціальній сферах.

Це зумовлює необхідність розроблення та реалізації національних стратегій кібербезпеки, які б висували на перший план і підкреслювали необхідність підвищення рівня обізнаності щодо питань кіберсфери всередині гетерогенних категорій, таких як публічні службовці, політики, бізнесмени, IT-спеціалісти, представники громадськості та ін. І залежно від використаних підходів кібербезпеку можна сприймати або як відповідальність приватного сектору, або як відповідальність окремих органів публічної влади – від правоохоронних органів до військових відомств, або як поєднання обох. І саме останній підхід, на нашу думку, має бути застосовано в Україні.

Kotukh Ye. V.,
PhD of Technical Sciences, Associate Professor of Computer Science Department, Sumy State University, Sumy

IMPLEMENTATION OF NATIONAL CYBERSECURITY STRATEGIES: ECONOMIC AND POLITICAL ASPECT

The issue of maintaining the critical infrastructure security is a matter of national security – with or without taking into account the cyber component. However, networks used in critical infrastructure are not immune to growing dependence on Internet technology. Therefore, it can be argued that cybersecurity is combined with national security mainly in critical infrastructure.

In many developed countries, government agencies have been set up to deal with the security of information systems and the response to computer emergency incidents.

The challenges of cybersecurity apply to all countries, and none of them faces exactly the same problems, but most of them are similar, making it possible to develop common universal solutions that can then be adapted to the conditions of specific countries. At the same time, cyberspace is an integral part of the development of any modern state, as powerful cyberspace is crucial for the progress and development of states in the economic, political and social spheres.

This necessitates the development and implementation of national cybersecurity strategies that highlight and emphasize the need to raise awareness of cyberspace issues within heterogeneous categories, such as civil servants, politicians, businessmen, IT-professionals, members of the public, and others. And depending on the approaches used, cybersecurity can be seen either as the responsibility of the private sector, or as the responsibility of individual public authorities – from law enforcement to military agencies, or a combination of both. And the last approach, in our opinion, should be applied in Ukraine.

Keywords: critical infrastructure, cybersecurity, cyberspace, information systems, cyberdiplomatics, strategy.

References

1. Bundesministerium des Innern (2011). Cyber-Sicherheitsstrategie fur Deutschland. URL: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OEDVerwaltung/Information sgesellschaft/ cyber.pdf.

2. De Nationale Cyber Security Strategie: Slagkracht Door Samenwerking (2011). Netherlands Ministry of Security and Justice, The Hague, Netherlands. URL: http://www.rijksoverheid.nl/ bestanden/documenten-en-publicaties/rapporten/2011/02/22/nationale-cyber-security-strategie-slagkracht-door- samenwerking/de-nationale-cyber-security-strategie-definitief.pdf.

3. Department of Information Technology, Ministry of Communications and Information Technology (2018). New Delhi, India. URL: http://www.mit.gov.in/sites/upload_files/dit/files/ncsp_060411.pdf.

4. French Network and Information Security Agency (2011). Information Systems Defense and Security France's Strategy. URL: http://www.ssi.gouv.fr/IMG/pdf/2011-02-15 Information system defence and security - France s strategy.pdf.

5. Klimburg, A. and Healey, J. (2012). Strategic Goals & Stakeholders. National Cyber Security Framework Manual. Alexander Klimburg (Ed.). NATO CCD COE Publication, Talinn.

6. Melissen, J. (2007). The New Public Diplomacy: Soft Power in International Relations. New York, Palgrave.

7. Macmillan Morse, A. (2013). The UK Cyber Security Strategy: Landscape Review. National Audit Office, London Oxford University Press.

8. Smith, David (2020). Why Cybersecurity Is Vital in the Public Sector. May 08, 2020. URL: https://www.acfeinsights.com/acfe-insights/why-cybersecurity-is-vital-in-the-public-sector.

9. The Dutch Ministry of Security and Justice (2011). The National Cyber Security Strategy. The Hague. URL: .https://www.enisa.europa.eu/media/news-items/dutch-cvber-securitv-strategv-2011.

10. The UK Cabinet Office (2019). The UK Cyber Security Strategy Protecting and promoting the UK in a digital world. URL: https://www.gov.uk/government/uploads/system/uploads/attachment data/file/60961/uk-cyber-security-strategy-final.pdf.

11. The White House (2011). International Strategy for Cyberspace, Prosperity, Security, and Openness in a Networked World. Washington. URL: .http://www.whitehouse.gov/sites/default/files/ rss viewer/international strategy for cyberspace.pdf.

12. Turkish Ministry of Transport, Maritime Affairs and Communication (2013). National Cyber Security Strategy and Action Plan 2013-2014. Ankara. URL : http://www.ccdcoe.org/strategies/TUR CyberSecurity.pdf.

Надійшла до редколегії 11.05.2021 р.