УДК 351.865

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

DOI: 10.32702/2306-6814.2021.3.68

ОСНОВНІ ПІДХОДИ ДО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ: ДОСВІД КРАЇН ВИШЕГРАДСЬКОЇ ЧЕТВІРКИ

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

MAIN APPROACHES TO CYBERSECURITY PROVIDING: VISEGRAD COUNTRIES PRACTICE

У статті виокремлено базові стратегії у сфері кібербезпеки загалом, розглянуто конкретні стратегії країн Вишеградської четвірки (Польща, Словаччина, Угорщина, Чехія). Досліджено як співвідносяться державницька та економічна парадигма з реальним процесом реалізації стратегій кібербезпеки. Встановлено, що поділ підходів до кібербезпеки, може сприяти кращому розумінню кібербезпеки як явища і допомогти пояснити перешкоди для співпраці держав, що займаються питаннями кібербезпеки на міжнародному рівні. Крім цього, визначення особливостей різних підходів до кібербезпеки може пояснити конкретні дії держав у кіберпросторі. Доведено, що розуміння відмінностей у сприйнятті державами кіберзагроз, референтних об'єктів і потенційних противників становить основу для обговорення так званої кіберідентичності держав та недержавних суб'єктів.

The qualitative analysis of the cybersecurity policies of the four Visegrad countries shows that each of these countries has cybersecurity strategies and corresponding laws to address cybersecurity issues. All of the documents analyzed refer to higher-level national security or defense strategies and present the legislative environment, although there are significant differences in their profundity. Different cyberspace entities and the potential threats these entities generate are also addressed in the documents. In most national cyberspace security strategies, threats to critical infrastructure and cybercrime play a prominent role and indicate increasing economic damage wrought by cyberattacks. In the formal sense, the domain of cyberspace is already included in the security agendas of all states and could be called "securitized."

However, there are differences of securitization among countries. Cybersecurity differs by how countries (a) define a referent object (what should be protected), (b) perceive primary threats and risks, and (c) identify the sources of threats and risks. In accordance with these differences, countries can be classified into two categories. The first category, that of countries that militarize cybersecurity issues (like Poland). Such countries have militarized cybersecurity discourse are more precise in identifying specific referent objects and in articulating the defense of these objects as national priorities. This tendency elevates cybersecurity to the highest national security level and focuses on safeguarding ICT and governmental information resources. Poland tend to identify cybersecurity challenges as threats to the proper functioning of the state and identify attacks from foreign states as the most dangerous sources of such threats. Consequently, in such states, the responsibility of responding to cyber threats is handed over to military and defense institutions.

The second category of securitization discourse refers to the criminalization of cybersecurity issues. The Czech Republic, Slovakia and Hungary rely on a civil approach to maintain cybersecurity. Their referent objects are diffused and mainly related to the proper functioning of the state's economic system and private property. The ICT and governmental digital resources have no priority over other legitimate referent objects. As a result, countries with a prevailing civil approach are mostly concerned

with criminal activity conducted in cyberspace and describe cybersecurity issues as "risks". Potential sources of such risks are also fragmented and include not only external international actors but also internal actors such as hackers, hacktivists, criminal organizations, and even the unintentional disruption of networks. Civil institutions in the Czech Republic, Slovakia, and Hungary are charged with monitoring cybersecurity risks and coordinating state response to cyber incidents.

So, the categorization of cybersecurity approaches as civil or militarized may lead to a better understanding of cybersecurity as a phenomenon. It could contribute to the explanation of obstacles for cooperation between states dealing with cybersecurity issues on the international level. Furthermore, the identification of different approaches to cybersecurity could explain specific state's actions in cyberspace. Understanding states' differences in perceiving cyber threats, referent objects, and potential adversaries constitutes a background to discussions of the so-called cyber identities of states and nongovernmental actors.

Ключові слова: Інтернет, кібербезпека, кіберпростір, країни Вишеградської четвірки, стратегія.
Key words: Internet, cybersecurity, cyberspace, Visegrad countries, strategy.

ПОСТАНОВКА ПРОБЛЕМИ В ЗАГАЛЬНОМУ ВИГЛЯДІ

Кіберзагрози здійснили революцію в розумінні людьми безпеки, а також правил та методів підтримання національної безпеки. Сьогодні кібербезпека все частіше розглядається як питання національного масштабу, що стосується усіх рівнів суспільства [4]. Відповідно, підтримання безпеки кіберпростору стало невід'ємною частиною державних стратегій національної безпеки багатьох країн світу. Різні країни мають свої визначення кіберзагроз, але майже всі погоджуються з тим, що загрози і ризики для кіберпростору повинні належним чином бути представлені у стратегіях національної безпеки.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Питанням впливу кіберзагроз на економічний простір присвятили свої дослідження Р. Андерсен та Т. Мур. Дж. Свянтковська розглядала питання співпраці країн Вишеградської четвірки у кіберпросторі Л. Гансе, К. Дан, Г. Ніззенбаум, Дж. Стьювер опікувалися проблемами кібербезпеки як складової національної безпеки та об'єкта публічного управління.

МЕТА СТАТТІ

Метою статті є виокремлення підходів до реалізації стратегій кібербезпеки та визначенні основних відміннностей в діяльності держав у кіберпросторі.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Часто через низький рівень усвідомлення наявних проблем трапляються випадки тероризму, який також може мати значний вплив на стан кібербезпеки держави. Як заявляють Е. Салієч та ін. у сучасних умовах тероризм набирає нових форм та нового змісту. Водночас вони зазначають, що держави, що розвиваються, повинні краще співпрацювати з метою боротьби із сучасними формами злочинності [9].

У відповідь на наявні загрози держави у всьому світі розробляють стратегії кібербезпеки, зазвичай — шляхом створення певного національного правого акту або програми для реагування на кіберзагрози та захисту найважливіших мереж [11]. Однак пріоритети стратегій національної безпеки різних держав відрізняються. Деякі держави мають чітке уявлення про кіберсередовище та його головні референтні об'єкти, як-от: критична інфраструктура, і, відповідно, сформували комплексний підхід до сприйняття проблем, що становлять загрозу для кібербезпеки та національної безпеки, та визначили найважливіші джерела цих загроз. Унаслідок цього ключовою умовою для реалізації ефективних стратегій кібербезпеки у цих країнах є призначення державних відомств відповідальними за управління кібербезпекою. З іншого боку, держави, в яких переважає цивільний підхід до кібербезпеки, зосереджуються переважно на боротьбі з кіберзлочинністю. Потенційні джерела загроз кіберзлочинності не визначені чітко і пов'язані, переважно, з приватною власністю і належним функціонуванням сектору економіки. Ці два основоположні підходи спричинили появу конкуруючих доктрин для розгляду питань кібербезпеки.

Першою є так звана державницька (військова) парадигма національної безпеки, яка відображає традиційну роль держави в захисті кордонів та забезпеченні верховенства права [8]. Гаркнетт і Стівер висловлють думку, що питання кібербезпеки є унікальним і багатогранним, а її забезпечення вимагає зі сторони держави підтримання безпеки кібердіяльності на публічному, приватному та економічному рівнях [6]. У межах цієї парадигми кібербезпека вважається фундаментальним фактором воєнної та економічної безпеки держави, і тому до неї застосовуються традиційні аргументи національної безпеки, що базуються на захисті батьківщини [6]. Інакше кажучи, цей підхід підкреслює зв'язок між захистом критичної інфраструктури і тих державних та приватних систем, що є важливими для функціонування держави. Державницька парадигма національної без-

пеки відноситься до традиційного підходу до управління та запобігання ризикам з кібепростору у спосіб, що може спричинити зростання впливу військових сил у сфері стратегій кібербезпеки [3].

Другою є економічна парадигма, яка відображає зростання впливу інтернету на економічний добробут держави [8]. Тим часом як державницька парадигма національної безпеки виключає з процесів формування стратегій кіберпростору усі сектори, крім військового, економічна парадигма наголошує на важливості участі інших секторів та відомств у процесі формування стратегій кібербезпеки. За Т. Мур [7] економічна парадигма передбачає дві необхідні умови для реалізації стратегії національної кібербезпеки:

1) інтернет-провайдери мають бути відповідальними за видалення комп'ютерів, уражених шкідливим програмним забезпеченням, з їхніх систем;

2) компанії та інші агенції повинні мати зобов'язання виявляти витоки інформації та втручання в систему.

Економічна парадигма наголошує на децентралізованому підході в групах відомств та суб'єктів, відповідальних за управління кібербезпекою. Згідно з цим підходом тягар вжиття заходів щодо захисту систем розподіляється між окремими особами, надавачами послуг (провайдерами) та керівництвом держави.

Обидві парадигми — державницька та економічна — пропонують основи для теоретичного аналізу процесу створення і реалізації стратегій кібербезпеки. Між тим, на практиці, обидва підходи доповнюють один одного і не існують у "чистому вигляді". У цьому можна пересвідчитися на результатах кваліативного дослідження чотирьох держав Вишеградської групи (Польща, Чехія, Словаччина і Угорщина).

Порівняння державницького та економічного підходів в процесі реалізації державної політики щодо боротьби з кіберзагрозами представлено в таблиці 1.

Таблиця 1. Порівняння особливостей застосування державницького та економічного підходів у процесі реалізації державної політики щодо боротьби з кіберзагрозами

№	*Підходи*	*Економічний підхід*	*Державницький підхід*
1	Сприйняття кіберзагроз	Приватна безпека, інформаційно-комунікаційні технології (ІКТ)	Критична інфраструктура, ІКТ
2	Джерела кіберзагроз	Злочинці, недержавні суб'єкти, кіберзлочинці, хакери	Іноземні держави, шантажисти, терористи
3	Відомства, відповідальні за управління кібербезпекою	Міністерства внутрішніх справ, цивільні відомства та ін.	Міністерства оборони, інші військові відомства

Нижче узагальнимо практики боротьби з кіберзагрозами у різних країнах світу.

Польща провела багато комплексних змін у системі оборони кіберпростору та розробила власну стратегію кібербезпеки. Крім цього, кібербезпека стала невід'ємною частиною зусиль Польщі у сфері національної безпеки і часто згадується в інших національних стратегічних документах.

Питання кібербезпеки в стратегічних документах Польщі було вперше згадано в Стратегії національної безпеки Республіки Польща в 2007 р. Документ визначав прямий зв'язок між кібербезпекою та здатністю держави до належного функціонування [10]. Пізніше, у Стратегії розвитку системи національної оборони Республіки Польща на 2011—2022 рр. було детально описано і розроблено питання, пов'язані з захистом кіберпростору Польщі [4]. Однак перший документ, присвячений виключно питанням кібербезпеки — Стратегія захисту кіберпростору — був виданий лише в 2013 р. [11]. У 2015 р. Бюро національної безпеки Польщі (пол. Biuro Bezpieczenstwa Narodowego, BBN) опубліковало доктрину кібербезпеки [10]. Документ описує завдання, які необхідно завершити для покращення стану національної кібербезпеки. Доктрина також описує завдання державних органів, зокрема органів безпеки, збройних сил, приватного сектору та недержавних організацій у цій сфері [8]. Бюро національної безпеки, як головний орган, разом з Міністерством адміністрації і цифровизації, Агентством внутрішньої безпеки та Комп'ютерною групою реагування на надзвичайні ситуації Польщі (англ. Computer Emergency Response Team, CERT) є відповідальними за досягнення цілей у сфері кібербезпеки.

Національна стратегія інформаційної безпеки Чехії, затверджена в 2005 р., є першою спробою держави щодо регулювання кіберпростору. У 2011 р., Стратегія національної безпеки проголосила кібербезпеку одним із пріоритетів уряду, а кіберзагрози були віднесені за важливістю до рівня регіональних конфліктів, тероризму і зброї масового знищення [2]. Також у 2011 р. було затверджено стратегію кібербезпеки і план дій на 2011—2015 рр. Ця стратегія направлена, перш за все, на захист систем ІКТ та мінімізацію збитків, завданих кібератаками [2]. У 2015 р. уряд Чехії затвердив оновлену стратегію національної кібербезпеки на 2015—2020 рр. Ця стратегія на другу половину десятиліття містила більш широкий комплекс заходів, спрямованих на досягнення якнайвищого рівня кібербезпеки [8].

Відповідальними за реалізацію стратегії кібербезпеки в Чеській Республіці є цивільні відомства. Загальна відповідальність за національну кібербезпеку покладається на Бюро національної безпеки (англ. National Security Authority). Національний центр з питань кібербезпеки у складі Бюро національної безпеки є частиною державної і міжнародної системи раннього попередження. Додатково Міністерство внутрішніх справ просуває питання кібербезпеки на політичному рівні, тоді як Міністерство оборони займається питаннями кібербезпеки лише спільно з НАТО.

Словаччина розробила правову основу для кібербезпеки, прийнявши в 2008 р. Національну стратегію інформаційної безпеки Словацької Республіки (англ. National Strategy for Information Security of the Slovak Republic, NSIS) на 2009—2013 рр. [4]. Проєкт стратегії був створений Міністерством фінансів — відомством, відповідальним за безпеку незасекреченої інформації державної адміністрації. У 2012 р. Словаччина розпочала реалізацію Стратегії національної кібербезпеки. До стратегії додавались план дій та звітом із завдань Національної стратегії інформаційної безпеки.

Управління національної безпеки Словаччини (англ. National Security Authority) займається засекреченою

інформацією, рештою питань займається Міністерство фінансів. Взаємну комунікацію забезпечує Комітет з питань інформаційної безпеки при Міністерстві фінансів: комітет виконує дорадчу та координаційну функції, готує стратегічні й технічні матеріали щодо інформаційної безпеки. Деякі питання вирішують Рада безпеки, Міністерство внутрішніх справ та Міністерство оборони. Таким чином, Міністерство оборони безпосередньо не займається управлінням національною кібербезпекою.

У 2013 р. Угорщина прийняла стратегію національної кібербезпеки, яка чітко визначає, що захист суверенітету держави в кіберпросторі є національним інтересом [11]. Усвідомлюючи те, що загрози та атаки із кіберпростору можуть зрости до рівня, що вимагатиме допомоги іноземних держав, Угорщина вважає, що кібербезпека має бути питанням колективної безпеки відповідно до Статті 5 установчого договору НАТО. Також варто зазначити, що кіберзагрози є пріоритетом стратегії національної безпеки Угорщини, прийнятої в 2012 р. [11].

Основним органом, відповідальним за координацію та реалізацію стратегії у сфері кіберпростору в Угорщині є Рада з питань управління національною кібербезпекою (англ. National Cybersecurity Coordination Council). Іншими органами, відповідальними за окремі аспекти кібербезпеки, є Управління кібербезпеки (англ. Cybersecurity Authority — відомство у складі Міністерства національного розвитку), Управління національної безпеки (англ. National Security Office — відомство у складі Міністерства державної адміністрації і справедливості) та Комп'ютерна група реагування на надзвичайні ситуації.

Цей огляд стратегій національної кібербезпеки чотирьох країн демонструє, що стратегії кібербезпеки в регіоні стають комплексними і всеосяжними. Стратегії трактують кібербезпеку комплексно й охоплюють економічний, соціальний, правовий, правоохоронний, воєнний та дослідницький аспекти кібербезпеки. Деякі стратегії, як у Словаччині або Чеській Республіці, підтримують більш гнучкий підхід та надають особливої уваги економічному та персональному (індивідуальному) аспектам стратегії кібербезпеки. Крім цього, Чеська Республіка, Словаччина та Угорщина належать до групи держав, в яких відповідальність за підтримку кібербезпеки несуть здебільшого цивільні відомства. З цього погляду кібербезпеку цих держав можна назвати цивільно-орієнтованою. Натомість у Польщі військові відомства більш активно координують та реалізують стратегії кібербезпеки.

Нижче розглянемо як відрізняються стратегії кібербезпеки різних держав залежно від визначення референтних об'єктів, сприйняття основних загроз та ризиків та визначенню їх джерел.

Незалежно від обраного підходу, усі країни визнають, що одним з найбільш референтних об'єктів (об'єкт, що знаходиться під загрозою) є критична інфраструктура. При цьому, як зазначають Гансен і Ніззенбаум, наукові, політичні та інші дискусії про кібербезпеку йдуть навколо основних референтних об'єктів кібербезпеки [5]. Згідно з ними, ключем до розуміння потенційних масштабів кіберзагроз є розуміння і прийняття того, наскільки розвиненими та пов'язаними стали комп'ютерні системи. Мережі обслуговують критичну цифрову інфраструктуру: регулюють енергозабезпечення, фінансову діяльність, енергоспоживання і навіть структуру трафіку. Ці мережі розглядаються як колективний референтний об'єкт, що підлягає першочерговій сек'юритизації, оскільки їх пошкодження становитиме загрозу для національної безпеки будь-якої країни.

Економічний сектор також має багато референтних об'єктів, включно з побоюваннями приватного сектору щодо можливості викрадення великих сум грошей хакерами, а також власників інтелектуальної власності щодо того, що обмін файлами ставить під загрозу їхні права та прибутки [5]. З цього погляду бере свій початок індивідуальний підхід до кібербезпеки, що наголошує на першочерговій значущості персональної (індивідуальної) безпеки. Як стверджують Гансен і Ніззенбаум, в дискурсі приватної безпеки індивід не є референтним об'єктом, але є пов'язаним з соціальними та політичними референтними об'єктами [5, с. 1163]. Інакше кажучи, захист приватності у кіберсфері повинен бути опосередкованим через колективний референтний об'єкт: чи то політико-ідеологічний, що піднімає питання щодо належного балансу між індивідом та державою, чи то національно-соціальний, що мобілізує цінності, ключові для ідентичності суспільства. Так само захист критичної інфраструктури не може зводитись лише до самої інфраструктури; наслідки краху мережі стосуються також інших референтних об'єктів: суспільства, державного устрою та економіки (прибутки) [5]. Нижче зробимо аналіз референтних об'єктів, визначених самими державами, які обрані нами як об'єкт для аналізу.

Усі чотири держави визнають зв'язок між секторами кібербезпеки та національної безпеки та те, що питання кібербезпеки — такі, як руйнування систем ІКТ або критичної інфраструктури — може зашкодити національній безпеці, вплинути на життя громадян і поставити під загрозу активи та функціонування національної економіки та державних служб. Тому у стратегічних документах усіх цих країн домінує дискурс колективної безпеки. Однак Польща та певною мірою Чеська Республіка демонструють високу необхідність інтенсивного захисту їхнього кіберпростору, більш широке і чітке бачення своїх основних референтних об'єктів. Стратегія національної кібербезпеки Чеської Республіки наголошує на захисті інформаційної інфраструктури, що є важливою для економічних та соціальних інтересів держави; вона також звертає увагу на важливість захисту прав інтернет-користувачів [2]. Вона має більш всеохоплюючу концепцію критичної інфраструктури та її вразливостей, що походять з кіберпростору, ніж стратегія національної кібербезпеки. У документі з національної безпеки вказано, що критична інфраструктура загалом має велику кількість загроз натурального, технологічного та асиметричного характеру. Серед таких: кібератаки, економічна злочинність та диверсії [2]. Проте держави, які намагаються підтримувати високий рівень безпеки свого кіберпростору, схильні пріоретизувати питання безпеки елементів критичної інфраструктури як ключової умови національної безпеки.

Оскільки національна безпека пов'язана з критичною інфраструктурою як референтним об'єктом, суб'єкти, які мають право визначати об'єкти, що потребують захисту та оборони, можуть претендувати на право застосування надзвичайних заходів. Наприклад, доктрина кібербезпеки Польщі наголошує на важливості критичної інфраструктури та прямому зв'язку між кібербезпекою та належним функціонуванням держави, включно з її економічним розвитком та здатністю ефективно діяти у воєнній сфері [11]. Крім того, Польща є єдиною країною, що прагне розвивати не лише оборонний, але також наступальний потенціал з метою стримування потенційних противників у кіберпросторі. Отже, підхід Польщі показує, що чим чіткіше сформульовано процес виявлення і захисту від кіберзагроз, тим більш мілітаризованим він стає.

З іншого боку, такі держави, як Угорщина і Словаччина також вважають критичну інфраструктуру референтним об'єктом. Однак ці країни не розглядають потенційні атаки на критичну інфраструктуру як загрозу національному існуванню, оскільки кібербезпека у цих двох країнах вважається лише одним із декількох секторів національної безпеки. Угорщина та Словаччина фокусуються в основному на інформаційній безпеці. Цілі стратегії інформаційної безпеки Словаччини зосереджені навколо захисту прав та свободи людини, покращення управління інформаційною безпекою та захисту державних ІКТ для підтримки критичної інфраструктури держави [4]. Концепція референтних об'єктів стратегії кібербезпеки Угорщини залишається ще більш амбівалентною: їй бракує прямих посилань до головних референтних об'єктів. У стратегії згадується лише захист національних баз (активів) даних та "операційна безпека елементів критичної інфраструктури, пов'язаних з кіберпростором" [8]. Ні Словаччина, ні Угорщина не виділяють конкретних референтних об'єктів, які повинні бути захищені першочергово в рамках кібербезпеки; внаслідок цього обидві країни мають переважно економічний підхід до кібербезпеки.

Варто відзначити, що питання кібербезпеки зазвичай актуалізуються тоді, коли суб'єкти, такі, як керівництва інших держав або недержавні суб'єкти, шляхом шахрайства намагаються отримати доступ до фінансової, енергетичної сфери або сфери публічної безпеки, а перспектива кібератак розглядається як загроза, що потребує термінової відповіді. Сприйняття і подання кібератак у такий спосіб веде до прийняття інтенсивних заходів безпеки.

Однак загрози для кібер- та національної безпеки не виникають лише із зовнішніх джерел. Кібератаки також можуть виникати із систематичних загроз. Ці системні загрози зумовлені властивою непередбачуваністю комп'ютерів та інформаційних систем, що "створюють ненавмисні (потенційно або дійсно) небезпечні ситуації для самих себе або ж для людей і фізичного середовища, до якого вони вбудовані" [1]. Більш поширеною проблемою, однак, є навмисне спровокована системна загроза, яку застосовують кримінальні синдикати або окремі особи. З цього погляду технічний дискурс супроводжується кримінальним. У цьому дискурсі кібербезпека може розглядатися як захист комп'ютерів від кримінальних дій, а кібератаки сприймаються не як загрози для національної безпеки, а як загальні ризики у кіберпросторі. Відповідно держави, що сприймають потенційні кібератаки як ризик для конкретного сектору, менш схильні вважати питання кібербезпеки питаннями національної безпеки і можуть називатись державами з економічним підходом.

Проте узагальнюючи, можна зазначити, що Польща і Чеська Республіка мають багаторівневий підхід до кібератак. По-перше, вони оцінюють ризики для національної безпеки і дають завдання державним органам щодо запобігання кібератакам. По-друге, вони ідентифікують виклики у сфері кібератак як невід'ємні компоненти їхньої національної безпеки: економічного, фінансового та приватного секторів.

Польща має всеосяжний підхід до кібербезпеки, що базується на точних оцінках потенційного впливу кібератак на різні сектори та на національну безпеку загалом. Оскільки кібератаки сприймаються переважно як загрози для національної безпеки, країна реагує на це, використовуючи державницький підхід.

Оновлена концепція кібербезпеки Словаччини на 2015—2020 рр. також представляє комплексне уявлення про кібербезпеку. Словаччина стверджує, що кібербезпека не повинна розглядатись як окрема проблема держави, або як проблема, що стосується одного чи декількох секторів, і що з огляду на свою глобальну суть, кібербезпека є загальносуспільним явищем [11].

Документ також описує основну проблему стратегії кібербезпеки Словаччини: кіберзагрози не розглядаються як термінова проблема. Хоча документ пропонує модель управління стратегіями кібербезпеки, в ньому немає повного бачення викликів у сфері кібербезпеки. У результаті цього потенційні кібератаки розглядаються переважно як ризики для безіменних (конкретно не визначених) цілей.

У стратегії Чеської Республіки згадуються такі ризики як кібершпигунство (промислове, воєнне, політичне або інше), організована злочинність у кіберпросторі, хактивізм, міжнародні дезінформаційні кампанії з політичними або воєнними цілями і навіть, у майбутньому, кібертероризм [2]. Ці ризики розглядаються загалом як небезпечні тенденції глобального кіберпростору, які ще однак не торкнулися чеського суспільства. Безпековий дискурс, що домінує в стратегічних документах Чеської Республіки, переважно відноситься до систематичних загроз та "комп'ютерної безпеки". З цього погляду стратегія кібербезпеки Чехії фокусується здебільшого на побудові надійної інформаційної спільноти шляхом захисту доступу до послуг, цілісності даних і покращення конфіденційності кіберпростору Чеської Республіки [2].

Угорщина, натомість, особливо наголошує на кримінальній складовій кібератак, стверджуючи, що динамічний розвиток нових технологій, на кшталт хмарних обчислень та мобільного Інтернету, веде до постійного виникнення нових загроз, таких як незаконне заволодіння критичною інформацією та персональними даними [11]. Крім цього, Угорщина не ідентифікує виклики для кібербезпеки з загрозами — у державі надають перевагу називанню кіберзагроз ризиками для кібер-сектору.

Отже, аналіз сприйняття кіберзагроз та кібербезпеки загалом дозволяє стверджувати про застосування

економічного підходу до управління кібербезпекою, що домінує в Чеській Республіці, Словаччині та Угорщині.

Сучасна архітектура кіберпростору забезпечує високий рівень анонімності та перешкоджає спробам відслідковування джерел кібератак, що є додатковим фактором небезпеки. Утім, сучасні технології дозволяють аналізувати джерела кібератак та кіберзловмисників, серед яких виділяють два основних: внутрішні та зовнішні. У воєнно-цивільній дихотомії зовнішні кіберзагрози, як-от: іноземні держави або недержавні суб'єкти, включно з кібертерористами та суб'єктами кібершпигунства, стикаються з внутрішніми суб'єктами: хактивістами, кіберзлочинцями, авторами шкідливих програм, кібершахраями та подібними організаціями. Як згадувалось раніше, держави, що активно захищають свій кіберпростір, наголошують на політичних мотивах кібератак та зовнішніх кіберзагроз. Таке відношення розглядає державницький підхід до управління кібербезпекою як найбільш ефективний. І навпаки, фокусування переважно на внутрішніх кіберзагрозах означає те, що головним референтним об'єктом є сектор економіки або персональні дані. Економічний підхід до стратегій кібербезпеки вважається у такому разі найбільш ефективним для боротьби з такими загрозами.

Подальший аналіз того, як окремі держави розуміють джерела кіберзагроз, приводить нас до висновку про те, що усі вони визнають те, що у кіберпросторі є багато суб'єктів; однак, лише декілька держав розрізняють їх природу, цілі та методи діяльності. Наприклад, Польща у своїй стратегії кібербезпеки декларує, що на національну кібербезпеку впливають суб'єкти з різними навичками, цілями та мотиваціями, і що показник кібершпигунства з метою отримання інформації з секторів національної безпеки та економіки зростає. Зовнішні загрози, перераховані в доктрині, включають кіберкризи, кіберконфлікти, кібервійни та кібершпигунство за участі держав та інших суб'єктів; "загрози (для Польщі) з кіберпростору походять від екстремістських, терористичних та міжнародних кримінальних організацій, чиї атаки у кіберпросторі можуть бути ідеологічно, політично, релігійно, бізнесово або кримінально вмотивованими" [8].

Водночас Словаччина і Угорщина мають розмите і фрагментарне бачення джерел кіберзагроз. Угорщина фокусується на технічних (внутрішніх) вразливостях і їх впливі на належне функціонування державної економіки, не вдаючись до глибшого аналізу їхніх причин та суб'єктів цього процесу.

У стратегії кібербезпеки Угорщини стверджується, що додатково до шкоди, завданої зовнішніми факторами, ще одним ризиком є невідповідне регулювання операційної безпеки інформаційної та комунікаційної систем, що формують кіберпростір. "Динамічний розвиток нових технологій, на кшталт хмарних обчислень та мобільного інтернету, веде до постійного виникнення нових загроз для безпеки" [11].

Цивільний підхід до джерел кіберзагроз застосовується також у Чеській Республіці. Стратегія національної кібербезпеки Чеської Республіки представляє великий перелік потенційних викликів для кіберпростру, однак майже всі вони є кримінальними або технологічними за своєю природою. Такими вважаються хакерські атаки з метою заволодіння персональними або конфіденційною інформацією, технічні збої, ботнет-мережі, DDoS/DoS-атаки (розподілені атаки на відмову в обслуговуванні) та ін.

Сприйняття кіберзагроз тісно пов'язане з джерелами сприйнятих загроз. Переважання сек'юритизованого погляду на кіберзагрози сприяє більш точному визначенню джерела загрози. Крім того, держави, що сек'юритизують кіберзагрози, як-от Польща, розрізняють зовнішні та внутрішні суб'єкти кіберпростору. Водночас держави, що підкреслюють кримінальний елемент кіберзагроз, розглядають їх переважно як внутрішні виклики та обмеження для кіберпростору. Варто зазначити, що більшість представлених держав розрізняють внутрішні та зовнішні джерела кіберзагроз у своїх стратегічних документах. Однак країни з економічним підходом не зацікавлені в подальшому розвитку цього розрізнення і фокусуються здебільшого на внутрішніх джерелах загроз як на найбільш поширених та ймовірних в їхньому середовищі безпеки.

ВИСНОВКИ

Компаративний аналіз стратегій кіберзагроз чотирьох країн Вишеградської групи демонструє, що кожна з них має власні стратегії кібербезпеки і відповідне законодавство для вирішення проблем кібербезпеки. Усі проаналізовані документи посилаються на стратегії національної безпеки та оборони високого рівня та представляють законодавче середовище, незважаючи на значні відмінності у їхній глибині. У документах також розглядаються різні суб'єкти кіберпростору та потенційні загрози, що походять від цих суб'єктів. У більшості національних стратегій кібербезпеки загрози для критичної інфраструктури та кіберзлочинність відіграють важливу роль і вказують на зростання шкоди для економіки, завданої кібератаками. У формальному сенсі, сфера кіберпростору вже включена до порядку денного з питань безпеки всіх держав і може бути названа "сек'юритизованою".

Однак між сек'юритизацією цих держав є також відмінності. Кібербезпека відрізняється за тим, як держави, по-перше, визначають референтний об'єкт (що потрібно захищати), по-друге, сприймають основні загрози та ризики та, по-третє, визначають джерела загроз та ризики. Відповідно до цих відмінностей їх можна віднести до двох категорій. Перша категорія — держави, що мілітаризують питання кібербезпеки (у нашому аналізі — це Польща). Такі держави більш точно визначають конкретні референтні об'єкти та називають захист цих об'єктів національним пріоритетом. Ця тенденція піднімає кібербезпеку на найвищий рівень національної безпеки та зосереджує увагу на захисті ІКТ та державних інформаційних ресурсів. У Польщі схильні трактувати виклики кібербезпеки як загрозу для належного функціонування держави та вважати атаки зі сторони іноземних держав найбільшими джерелами загроз. Відповідно, відповідальність за реагування на кіберзагрози у цих державах передана воєнним та оборонним органам.

Друга категорія держав за дискурсом сек'юритизації пов'язана з криміналізацією питань кібербезпеки. Чеська Республіка, Словаччина та Угорщина покладаються на економічний підхід в управлінні кібербезпекою. Їхні

референтні об'єкти відрізняються і здебільшого стосуються належного функціонування системи національної економіки та приватної власності. ІКТ та державні цифрові ресурси не мають переваги над іншими законними референтними об'єктами. Унаслідок цього держави з домінуючим економічним підходом зосереджуються на кримінальній діяльності у кіберпросторі, а проблеми кібербезпеки розглядають як "ризики". Перелік потенційних джерел таких ризиків також фрагментований і включає не лише зовнішні міжнародні суб'єкти, але також внутрішні суб'єкти — хакерів, хактивістів, кримінальні організації і навіть ненавмисні злами мереж. Цивільні відомства Чехії, Словаччини та Угорщини відповідають за відслідковування ризиків для кібербезпеки та координування відповіддю держави на виклики у цій сфері.

Таким чином, поділ підходів до кібербезпеки, може сприяти кращому розумінню кібербезпеки як явища і допомогти пояснити перешкоди для співпраці держав, що займаються питаннями кібербезпеки на міжнародному рівні. Крім цього, визначення особливостей різних підходів до кібербезпеки може пояснити конкретні дії держав у кіберпросторі. Розуміння відмінностей у сприйнятті державами кіберзагроз, референтних об'єктів і потенційних противників становить основу для обговорення так званої кіберідентичності держав та недержавних суб'єктів. Це може бути корисним теоретичним знаряддям для аналізу потенційних кіберконфліктів та моделей співпраці в цій сфері.

Література:

1. Anderson R.H., Anthony H. An exploration of cyberspace security R&D investment strategies for DARPA: "The day after... in cyberspace II". 1996. DOI: https://doi.org/10.7249/MR797

2. Cyber Security Strategy of the Czech Republic for the 2011-2015 Period. Ministry of Interior, Prague, Czech Republic. URL: http://www.enisa.europa.eu/media/news-items/CZ_Cyber_Security_Strategy_-20112015.PDF

3. Dunn Cavelty M. From cyber-bombs to political fallout: Threat representations with an impact in the cybersecurity discourse. International Studies Review. Vol. 15 (1). Mar 1. 2013. URL : https://doi.org/10.1111/misr.-12023

4. European Union Agency for Network and Information Security (ENISA). Cyber Europe 2012, key findings report, European Union Agency for Network and Information Security. URL: https://www.enisa.europa.eu/publications/cyber-europe-2012-key-findings-report

5. Hansen L., & Nissenbaum H. Digital disaster, cyber security and the Copenhagen School. International Studies Quarterly. № 53. 2009. P. 1155—1175. URL: https://doi.org/10.1111/j.1468-2478.2009.00572.x

6. Harknett R., Stever J. A. The cybersecurity triad: Government, private sector partners, and the engaged cybersecurity citizen. Journal of Homeland Security and Emergency Management. № 6 (1). Berlin — New York: De Gruyter. January. 2009. DOI: 10.2202/1547-7355.1649

7. Moore, T. (2010). Introducing the economics of cybersecurity: Principles and policy options. International Journal of Critical Infrastructure Protection. № 3 (3—4). P. 103—117. December 2010. DOI: 10.1016/j.ijcip.-2010.10.002

8. Newmeyer, K. P. Elements of national cybersecurity strategy for developing nations. National Cybersecurity Institute Journal. Excelsior College, Albany. № 1 (3). 2015. P. 9—19.

9. Saljic E., & Bordevic, Z. Modern forms of terroism environmental terrorism. 2011. URL: https://dk.um.si/IzpisGradiva.php?lang=eng&id=30223

10. Swiatkowska, J., et al. (2012). V4 cooperation in ensuring cyber security - Analysis and recommendations. Krakow: Koscluszko Institute. 2012. P. 83—87.

11. The cyber index, International security trends and realities. Geneva: UNIDIR, United Nations Institute for Disarmament Research. 2013. URL: https://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

References:

1. Anderson, R. H. & Anthony, H. (1996), An exploration of cyberspace security R&D investment strategies for DARPA: "The day after... in cyberspace II".

2. Cyber Security Strategy of the Czech Republic for the 2011—2015 Period (Strategii pro Oblast Kyberneticke Bezpecnosti Ceske Republiky na Obdobl 2011—2015), Ministry of Interior, Prague, Czech Republic. URL: http://www.enisa.europa.eu/media/news— items/CZ_-Cyber_Security_Strategy_20112015.PDF

3. Dunn Cavelty, M. (2013), From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. International Studies Review. URL: https://doi.org/10.1111/ misr.12023.

4. European Union Agency for Network and Information Security (ENISA). (2012), Cyber Europe 2012, key findings report, European Union Agency for Network and Information Security.

5. Hansen, L. & Nissenbaum, H. (2009), Digital disaster, cyber security and the Copenhagen School (2009). International Studies Quarterly, 53, 1155—1175. URL: https://ssrn.com/ abstract=2567410.

6. Harknett, R. & Stever, J. A. (2009), The cybersecurity triad: Government, private sector partners, and the engaged cybersecurity citizen. Journal of Homeland Security and Emergency Management. Berlin/New York: De Gruyter.

7. Moore, T. (2010), Introducing the economics of cybersecurity: Principles and policy options. National Academies of Sciences Engineering Medicine (NAP).

8. Newmeyer, K. P. (2015), Elements of national cybersecurity strategy for developing nations. National Cybersecurity Institute Journal, 1 (3), 9—19. Excelsior College, Albany.

9. Saljic, E. & Bordevic, Z. (2011), Modern forms of terroism environmental terrorism. URL: https://dk.um.si/IzpisGradiva.php?lang=eng&id=30223.

10. Swiatkowska, J. et al. (2012), V4 cooperation in ensuring cyber security — Analysis and recommendations. Krakow: Koscluszko Institute.

11. UNIDIR. (2013), The cyber index, International security trends and realities. Geneva: UNIDIR, United Nations Institute for Disarmament Research.

Стаття надійшла до редакції 25.01.2021 р.