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/ap.21.01.04**

НАЦІОНАЛЬНІ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ: ПОРІВНЯЛЬНИЙ АНАЛІЗ

Стаття присвячена аналізу стратегій кібербезпеки 14 країн світу, виокремлено цілі та зацікавлені сторони реалізації таких стратегій. Розглянуто вплив міжнародної спільноти на формування національних стратегій кібербезпеки, запропоновано низку пунктів, які має включати національна стратегія кібербезпеки будь-якої країни.

Ключові слова: критична інфраструктура; кібербезпека; кіберпростір; інформаційні системи; політика; стратегія.

Постановка проблеми. Глобальна технологічна взаємопов'язаність постійно зростає, вона стає невід'ємною частиною нашого життя. А разом із цим, ми стаємо більш уразливими до кіберзагроз. Отже, актуальним напрямом наукових досліджень стає аналіз сучасних стратегій захисту кіберпростору, щоб виокремити певні загальні місця, уникнути прогалин вже існуючих документів при складанні стратегії кібербезпеки України. Адже низка країн уже розробили і опублікували свої національні стратегії кібербезпеки (далі – НСК), які мають різні назви (національні стратегії інформаційної безпеки, стратегії захисту інформаційного простору, стратегії протидії інформаційним загрозам тощо), але також мають багато спільних рис.

Аналіз останніх досліджень і публікацій. Загальні питання побудови стратегій як на рівні держави, так і певної організації розглядали Г. Мінцберг та У. Кєчел, взаємозв'язку безпеки та сучасного кіберпростору присвятили свої дослідження К. Раушер та В. Ященко. Л. Деррік опікувався проблемами роботи органів розвідки у царині кібербезпеки.

Мета статті полягає в аналізі й порівнянні документів у сфері кібербезпеки 14 країн світу: з одного боку, найбільш розвинених країн світу, зокрема Австралії, Франції, Німеччини, Японії, Нідерландів, Іспанії, Великобританії та США; з іншого – країн, що швидко розвиваються, – Індії та Уганди.

Виклад основного матеріалу. Загальновідомо, що стратегія – це "план дій, метою якого є досягнення певної візії (довгострокової мети)". Інші визначення стратегії включають такі аспекти як напрям або шлях до візії та (ближчих) цілей [13], бажане майбутнє [12] і комплекс дій для досягнення довгострокових цілей (тощо). Таким чином, національні стратегії кібербезпеки являють собою національний план дій на основі національної візії, яка має на меті досягнення певних довгострокових цілей щодо підвищення рівня безпеки в інформаційній сфері. Узагальнення змісту розроблених документів, дозволяє стверджувати, що національні стратегії включають три групи цілей:

– систематизація державної політики в інформаційній сфері;

– координація дій різних суб'єктів у сфері кібербезпеки та розподіл відповідальності між усіма зацікавленими сторонами;

– донесення національних намірів у сфері кібербезпеки до інших держав та зацікавлених сторін.

Прикладами третьої цілі є демонстрація сили та позиціонування стратегії як засобу затвердження лідерства у сфері кібербезпеки. Зацікавленими сто-

ронами в контексті НСК є уряд, урядові органи з цивільних справ, військові, контролюючі органи, оператори об'єктів ключової інфраструктури, великі, середні та малі підприємства, науково-дослідні організації, університети, окремі громадяни та населення в цілому.

Візія НСК та напрям її стратегічних цілей повинні бути максимально чіткими з метою стимулювання зацікавлених сторін до об'єднаних дій, прописаних у НСК. Якщо є можливість, національна стратегія повинна виходити за територіальні кордони відповідної держави і враховувати вплив зовнішніх чинників (протидію йому).

Далі порівняємо НСК різних країн за низкою ключових ознак.

Як зазначено у таблиці 1, лише вісім з чотирнадцяти держав чітко визначили поняття "*кібербезпека*". Великобританія описово характеризує поняття кібербезпеки, Уганда і США дають визначення поняттю "інформаційна безпека", не згадуючи про "кібербезпеку". Дві з чотирнадцяти держав (Іспанія та Японія) говорять кібербезпеку на стратегічному рівні без визначення самого поняття. Більш того, десять держав, які визначили або описали поняття кібербезпеки, розуміють його зовсім по-різному. Деякі держави визначають кібербезпеку як колегіальний підхід до захисту і гарантій прав фізичних та юридичних осіб у сфері інформаційної безпеки. Інші держави застосовують державницький підхід і акцентують на захисті від загроз у кіберпросторі [14].

Таблиця 1

Визначення поняття кібербезпеки

Країна	*Визначення*	*Кібербезпека*
Австралія	є	Заходи, пов'язані з конфіденційністю, доступністю і цілісністю інформації, яка обробляється, зберігається і передається за допомогою електронних та аналогічних засобів
Німеччина	є	Бажана ситуація у сфері інформаційної безпеки, у якій ризики в (міжнародному) кіберпросторі було знижено до прийнятного мінімального рівня Примітка: цивільну та військову кібербезпеку визначено у схожому формулюванні.
Франція	є	Інформаційна система, яка забезпечує опір ймовірним випадкам у кіберпросторі, які можуть поставити під загрозу доступність, цілісність або конфіденційність даних, які зберігаються, обробляються або передаються, а також пов'язаних сервісів, які надаються за допомогою систем інформаційно-комунікаційних технологій (далі – ІКТ)
Велика Британія	опис	Охоплює як захист національних інтересів у кіберпросторі а також переслідує мету розширення політики національної безпеки шляхом використання багатьох можливостей, запропонованих кіберпростором
Індія	є	Діяльність із захисту інформації та інформаційних систем (мереж, комп'ютерів, баз даних, дата-центрів та застосунків) за допомогою відповідних процесуальних і технологічних заходів безпеки
Нідерланди	є	Відсутність загрози або шкоди, завданої порушенням або знищенням ІКТ або через їх злочинне використання
Румунія	є	Нормальний стан в результаті комплексу превентивних та зворотних заходів, які забезпечують конфіденційність, цілісність, доступність, достовірність та відмовостійкість інформації у електронній формі, а також державних і приватних ресурсів та послуг у кіберпросторі
Уганда	не визначено	Посилання на "інформаційну безпеку": захист інформації та інформаційних систем від неавторизованого доступу, використання, розкриття, порушення, змін або знищення

Відсутність спільних узгоджених визначень понять, пов'язаних з кіберпростором, прийнятих декількома державами ймовірно є причиною непорозумінь між державами під час обговорення міжнародних підходів до міжнародних загроз у кіберпросторі. На початку 2011 р. двостороння російсько-американська робоча група Інституту досліджень у сфері безпеки Захід-Схід та МГУ підготувала чорновий варіант моделі міжнародної термінології. Вони визначили кібербезпеку як "властивість кіберпростору до опору навмисним і ненавмисним загрозам, реагування на них та відновлення" [16, ст. 31]. Незважаючи на безперервну академічну дискусію більшості визначень термінології у кіберпросторі, визначення Раушера-Ященко може стати заміною більшості національних визначень та розуміння кібербезпеки, розглянутих вище.

Визначення, сформульоване Великобританією, включає фізичні загрози та загрозу електромагнітних завад у кіберпросторі [5; 19]. Німеччина включає поняття прийняття ризику у своє визначення [4]. Більшість держав обговорюють поняття кіберзлочину без його визначення, як і поняття кібербезпеки. Румунія – це єдина країна, яка у НСК дає визначення всім поняттям, пов'язаним з кіберпростором [17].

Далі порівняємо базову інформацію про НСК, зокрема таку, як кількість редакцій, сфера регулювання, зв'язок з іншими нормативними документами, а також обсяг та зміст. Останнє включає зв'язок між іншими національними та міжнародними стратегіями, усвідомлення наявних загроз і засобів протидії ним.

1. Кількість редакцій. Дванадцять з 14-ти держав один раз ухвалювали свою НСК; Японія та Великобританія мають вже другу редакцію НСК.

2. Сфера регулювання. Більшість НСК передбачають комплексний підхід до регулювання кіберпростору. Щоправда, у німецькій НСК прямо вказано, що сферою її регулювання є лише ІКТ, підключені до Інтернету. Формулювання австралійської та іспанської НСК пропонує таке ж вузьке бачення кіберзагроз. У голландській НСК прямо зазначено, що вона зосереджена на широкому діапазоні ІКТ, який, на відміну від ІКТ, підключених до Інтернету, включає, наприклад, смарт-карти, автомобільні систем та засоби передачі інформації. Франція має аналогічне бачення. У інших НСК ця тема менш виражена, але вони не зосереджуються безпосередньо "лише на Інтернеті".

3. Зв'язок з іншими нормативними документами. НСК восьми країн безпосередньо пов'язано зі стратегіями національної безпеки у їхніх державах. Іспанська НСК є фактично частиною іспанської стратегії національної безпеки. Низка держав розробила НСК в результаті минулих оцінок національних загроз та ризиків, а в деяких випадках НСК навіть включає оцінку національних загроз та ризиків. Цікаво, що Уганда застосовує SWOT-аналіз (аналіз сильних і слабких сторін, можливостей та загроз) на національному рівні для створення плану стратегічних і пов'язаних дій [15]. Нідерланди запровадили зовнішній циклічний процес: один з напрямів реалізації НСК – проведення щорічної оцінки національних кіберзагроз та ризиків для включення у реєстр оцінки національних ризиків [18]. У свою чергу процес оцінки NRB може викликати потребу у оновленні самої НСК.

У більшості НСК прямо зазначається загроза кібербезпеці ключових об'єктів інфраструктури. Щоправда, зв'язок НСК зі стратегією національного захисту ключових об'єктів інфраструктури обговорюється не так прямо. Цікаво, що дев'ять з десяти країн-членів ЄС не пов'язують з НСК з Європейською Директивою Захисту Ключових Об'єктів Інфраструктури [1].

Між тим, аналіз НСК більшості держав свідчить про те, що в урядах відповідних країн триває дискусія про те, яка урядова установа або орган відіграє ключову роль у разі масштабної кібератаки проти держави або порушення роботи ІКТ. Як стратегію національної оборони деякі держави розробляють військові кібероперації/засоби для оборони у інформаційні сфері. У НСК Великої Британії з 2009 р. [5, ст. 14, 26] підвищення військового та розвідувального потенціалу у сфері кібербезпеки прописано чіткіше, аніж у пізнішій редакції 2011 р. [19]. Французька НСК посилається на свою стратегію національної оборони та безпеки, яка підкреслює потребу у (військовій) обороні та стримування у сфері кібербезпеки [10, ст. 3]. Німецька [4, ст. 4] та нідерландська [18, ст. 8] НСК посилаються на свої напрацювання у сфері військових кібероперацій.

У своїх НСК всі держави зосереджуються на кіберзагрозах для своїх ключових об'єктів (інформаційної) інфраструктури. Переважна більшість країн прямо вказують на ці загрози, називаючи кіберзагрози важливим ризиком для своєї національної безпеки. Франція непрямо зазначає кіберзагрози значущим чинником для оборонної сфери, посилаючись на свою "Білу книгу" з питань оборони та національної безпеки [7].

У своїх НСК Німеччина, Індія та Японія зосереджуються на загрози зростання глобалізаційних факторів у сфері кібербезпеки. З цими загрозами вони пов'язують ризики зростання соціальної напруженості, а також порушень особистих прав та свобод громадян. Шість держав прямо вказують на цю загрозу. Вісім держав взагалі не згадують цей тип загрози у своїх НСК, незважаючи на визнання певних ризиків, пов'язаних із швидким розвитком інформаційного суспільства.

Усі держави, окрім США та Японії, прямо називають окремих осіб, злочинців та організовану злочинність суб'єктами зловмисної загрози. Кібершпигунство (електронне шпигунство) прямо зазначено у НСК десяти держав. Тринадцять держав визначили загрозу ворожих дій з боку іноземних держав (наприклад, кібервійна) у своїх НСК. Незважаючи на низку атак у кіберпросторі з боку таких угрупувань як Anonymous та LulzSec, лише Нідерланди та Велика Британія прямо визнають хакерів та екстремістів суб'єктами зловмисної загрози [18; 19].

Німеччина, Японія та Великобританія прямо вказують на загрозу широкомасштабних кібератак на свої ключові об'єкти (інформаційної) інфраструктури. У випадку з Японією це не дивно, оскільки ця країна пережила кілька широкомасштабних кібератак на урядові та комерційні системи у недалекому минулому [9].

Японська і німецька НСК посилаються на загрозу невідповідностей між існуючими розробками в сфері ІКТ та необхідним рівнем кібербезпеки, пов'язаним з цими розробками. Цікаво, що жодна з інших держав не піднімає тему загроз, викликаних інноваціями у сфері ІКТ, та ризиків, які вони несуть.

У табл. 2 викладено стратегічні цілі кібербезпеки держав. Щоправда, у [4; 6] Німеччина презентує набір стратегічних пріоритетів, які в інших НСК представлені як напрями дії. Більшість НСК містять 3-4 стратегічних цілі. Такі держави як Німеччина та Уганда, які мають більше чотирьох цілей, об'єднують свої стратегічні цілі з напрямами дії або презентують власні основні напрями дій.

Таблиця 2

Стратегічні цілі НСК

Австралія	1	Усі австралійці знають про ризики у кіберпросторі, захищають свої комп'ютери і вживають всіх належних заходів для захисту своєї особи, недоторканості особистого життя і коштів в мережі
	2	Австралійські компанії керують надійними і стійкими ІКТ з метою захисту цілісності транзакцій, особи та недоторканості особистого життя клієнтів
	3	Австралійський уряд забезпечує свої транзакції, особи та недоторканості особистого життя своїх клієнтів
Німеччина		Представлені скоріше стратегічні сфери безпеки, а не стратегічні цілі:
	1	Захист ключових об'єктів інфраструктури
	2	Забезпечення надійності ІТ-систем в Німеччині
	3	Підвищення рівню інформаційної безпеки у сфері державного управління
	4	Національний центр реагування на кіберзагрози
	5	Національна рада кібербезпеки
	6	Ефективна боротьба зі злочинністю з кіберпростором
	7	Ефективні координовані дії з метою забезпечення кібербезпеки у Європі та в світі
	8	Використання надійних ІТ-технологій
	9	Підвищення кваліфікації персоналу, який працює у федеральних органах
	10	Інструменти для реагування на кібератаки
Іспанія		Іспанська НСК є невід'ємною частиною іспанської стратегії національної безпеки і має на меті захищати іспанських ключових і стратегічних інтересів та цінностей
Франція	1	Стати світовим лідером у сфері кібербезпеки
	2	Гарантувати французам свободу прийняття рішень на національному рівні шляхом захисту інформації про громадян
	3	Підвищувати рівень кібербезпеки ключових об'єктів інфраструктури
	4	Гарантувати безпеку у кіберпросторі.
Велика Британія	1	Боротися з кіберзлочинами і стати одним з найбезпечніших місць у світі для бізнесу у кіберпросторі
	2	Бути більш стійкими до кібератак та краще захищати свої інтереси у кіберпросторі
	3	Допомагати формувати відкритий, стабільний та здоровий кіберпростір, який наше населення може безпечно використовувати і яке підкреслює відкрите суспільство
США	1	Запобігання кібератакам проти ключових об'єктів інфраструктури США
	2	Зниження вразливості держави до кібератак
	3	Мінімізація шкоди та скорочення часу на відновлення від реальних кібератак
	4	Розбудова дієвих структур кібербезпеки

Продовження табл. 2

Індія	1	Розвивати ІКТ в Індії у якості рушійної сили для економічного росту та благополуччя
	2	Створити модель безпеки для забезпечення надійності кіберпростору
Японія	1	Покращена політика боротьби з кібератаками
	2	Політика адаптації до змін у середовищі кібербезпеки
	3	Активні/динамічні заходи з кібербезпеки
Нідер-ланди	1	Покращити безпеку цифрового суспільства з метою підвищення довіри громадян, компаній та уряду до ІКТ, щоб стимулювати голландську економіку та підвищити рівень благополуччя та добробуту громадян
	2	Гарантія належного правового захисту у цифровій сфері та запобігання дестабілізації суспільства
	3	Вживання достатніх заходів у випадку проблем
Уганда	1	Систематизація впровадження інформаційної безпеки на національному та міжнародному рівні
	2	Систематизація, класифікація та захист ключових об'єктів інфраструктури від порушень
	3	Розробка моделі моніторингу інформаційної безпеки
	4	Поширення інформації про надійну е-комерцію, послуги електронного уряду та інші національні ІТ-проєкти
	5	Гарантія прав громадян на недоторканість особистого життя завдяки якісному управлінню інформаційною безпекою
	6	Розвиток культури обізнаності у сфері кібербезпеки на національному рівні та зміцнення потенціалу у сфері людських ресурсів
	7	Підтримка управління ризиками, пов'язаними з інформаційною безпекою, та забезпечення зрілого рівня інформаційної безпеки

Значна різниця між цілями національної стратегії викликана різними відправними точками та різними за змістом візіями, зокрема, такими, як безпечне, надійне та стійке ІКТ-середовище, економічне благополуччя, національна безпека та оборона, захист законних прав та інтересів громадян. Австралія будує свої цілі навколо аналогічної схеми зацікавлених сторін: уряду, ключових об'єктів інфраструктури, компаній та громадян/приватних осіб (використовуючи економічний підхід). У своєму наборі стратегічних цілей Японія прямо визнає потребу у швидкому пристосуванні до нових та майбутніх загроз кібербезпеці. У Франції інший підхід: вона висловлює свої амбіції в тому, щоб стати світовим лідером у кібербезпеці та зберігати свій статус інформаційної переваги у національній кібербезпеці. До речі, Франція – єдина держава, яка чітко йде цим шляхом, хоча в деяких інших НСК у певному вигляді підтримується концепція демонстрації сили. Наприклад, Великобританія має законне право збирати розвіддані про злочинців, терористів та інших небезпечних суб'єктів у кіберпросторі та використовує цю інформацію для боротьби з кіберзлочинами та зниження мотивації і можливостей ворога діяти у кіберпросторі [5, ст. 4, 16]. Згідно з публікацією Дерріка, МІ-6 здійснив хакерську атаку на Інтернет-журнал терористичної організації Аль-Каїда "Інспайр". Згідно з цією публікацією, Інтернет-стаття "Зроби бомбу на кухні твоєї матусі" було замінено на рецепти кращих амери-

канських капкейків [8]. Це наочний приклад впровадження цієї стратегії. При цьому НСК Великої Британії містить посилання на можливості використання кіберпростору, які можна віднести до "деяких дій, що були ініційовані урядом і які не підлягають розголошенню"[19, ст. 9].

У табл. 3 відображається класифікація зацікавлених сторін, пов'язаних з кібербезпекою і визнаних такими у НСК. Як видно з наведеного, більшість країн очікують, що громадяни братимуть активну роль у кібербезпеці. Однак, Японія та Іспанія лише згадують про громадян у зв'язку з підвищенням рівня їх обізнаності в інформаційній сфері. НСК Японії зосереджено на відповідних урядах і ключових об'єктах інфраструктури.

Таблиця 3

Зацікавлені суб'єкти відносно реалізації НСК

Країна	*Громадяни*	*Середній та малий бізнес*	*Інтернет-провайдери*	*Великі організації*	*Оператори ключових об'єктів інфраструктури*	*Держава*	*Міжнародні організації*
Австралія	■	■	■	■	■	■	□
Німеччина	■	■	■	□	■	■	■
Іспанія	□	□	□	□	■	■	
Франція	■	■	□	■	■	■	□
Велика Британія	■	■	■	■	■	■	■
Індія	■	■	□	■	■	■	
Японія	□	□		□	■	■	□
Нідерланди	■	■	□	■	■	■	□
Уганда	■	■		■	□	■	
США	■	■	□	■	■	■	■

Примітки: □ якщо згадувалося у НСК, але містить обмежений набір відповідних заходів/дій.

Інтернет-провайдери прямо вказані лише у НСК Австралії, Німеччини та Великої Британії. Хоча Секретаріат Кабінету Міністрів Великої Британії не вказував Інтернет-провайдерів у НСК у редакції 2009 р., у редакції 2011 р. згадуються Інтернет-провайдери, "які допомогли приватним особам виявити, чи існує загроза для їх комп'ютерів і що вони можуть зробити для вирішення цієї загрози і захиститися від атак у майбутньому" [19, ст. 31]. Інтернет-провайдери Австралії, які мають підтримку австралійського уряду, вжили низку спільних заходів з метою підвищення рівня кібербезпеки їх операцій та клієнтів. Згідно з австралійським НСК [3, ст. 18-19], такі заходи включають практичну інструкцію для Інтернет-провайдерів та визначення систем клієнтів, для яких існує загроза.

Німеччина, Велика Британія і США прямо вказали міжнародні інформаційні інфраструктури як сторони, зацікавлені у кібербезпеці. Однак варто відзначити, що ці зацікавлені сторони (наприклад, основні провайдери) працюють за межами сфери прямого впливу національних держав.

Проведене дослідження свідчить про те, що всі держави розробили тактичні

напрями дій і часто визначали комплекс детальних функціональних заходів на підтримку своїх стратегічних цілей кібербезпеки. Оскільки у більшості НСК виражено нагальну потребу у діях, можна констатувати наявність у них конкретного, вимірюваного, досяжного, реалістичного і прогнозованого (SMART) формулювання таких заходів. Загалом SMART-підхід дозволяє національним парламентам виконувати наглядову роль, а також дозволяє іншим суб'єктам, відповідальним за кібербезпеку, моніторити хід впровадження напрямів дій, викладених у НСК. Він дозволяє виявляти недостатній прогрес, про який можна вчасно повідомити з метою успішної реалізації НСК у цілому. Найбільш відповідає SMART-критеріям НСК Японії через те, що вона безпосередньо пов'язана з підходом щодо управління якістю, по-друге, містить додаток, у якому вказано відповідальну(-і) зацікавлену(-і) сторону(-и) та набір критеріїв досяжності для кожного запланованого завдання, зазначені проміжні та кінцеві результати. При цьому Японія стала єдиною державою, що як стратегічну ціль вказала швидку адаптацію до нових кіберзагроз і запланувала комплекс пов'язаних тактичних і функціональних заходів [9]. Це свідчить про те, що японський підхід до питань кібербезпеки є найбільш раціональним в контексті динамічної перспективи безпеки у порівнянні з іншими державами. Говорячи про зміст запланованих заходів інших країн звернемо увагу, що всі держави (окрім Уганди) прямо зазначають необхідність захисту своїх ключових об'єктів інфраструктури (у т.ч. сервісів "електронного уряду").

Усі держави зазначили, що вони планували розвиток програми обізнаності з кібербезпекою. Окрім суспільних програм, Німеччина, Нідерланди, Велика Британія і США розробляли програми з навчання з роботи у кіберпросторі для певних груп держслужбовців (наприклад, для службовців в оборонній сфері та спеціалістів, які працюють у правоохоронних органах).

Більшість держав (крім Іспанії, Уганди та Великої Британії) зміцнюють заходи з регулювання кризових ситуацій і реагування у сфері ІКТ з метою вирішити серйозні проблеми в інформаційній сфері. Практичне навчання на національному і вузькоспеціалізованому рівні часто пов'язують з такою діяльністю, хоча лише десять держав вказують навчання на національному рівні у своїх НСК. Австралія, Франція і Велика Британія зазначили важливість розвитку потенціалу виявлення кіберзагроз на національному рівні.

Усі держави вказували міжнародну співпрацю як один з пріоритетних напрямів. Щоправда, у більшості НСК відсутнє детальне пояснення передбачених дій з міжнародної співпраці, окрім обміну інформацією (наприклад, через національні Групи реагування на комп'ютерні надзвичайні ситуації).

Стосовно боротьби з міжнародної кіберзлочинністю Німеччина, Нідерланди та США висловили свої наміри поширити конвенцію про кіберзлочини серед інших держав. Велика Британія вже ратифікувала договір про конвенцію по кіберзлочинам у травні 2011 р. Чотири держави (Франція, Німеччина, Іспанія та Велика Британія) прямо зазначили необхідність захисту урядового апаратного і програмного забезпечення на міжнародному рівні, адже воно є частиною ключових і стратегічно важливих об'єктів урядової інфраструктури.

У 2011 р. у США було розроблено міжнародну стратегію для кіберпростору, яка передбачала створення інформаційного середовища, яке "сповна використовує інновації та надасть приватним особам більше повноважень; встановить зв'язки між приватними особами і зміцнить громади; покращить уряди та зробить їх більш підзвітними; гарантує забезпечення основних свобод і підвисить рівень національної та міжнародної безпеки" [11, ст. 8]. За допомогою такої стратегії США мала намір уніфікувати процес залучення

декількох відомств разом з міжнародними партнерами для вирішення широкого діапазону проблем, пов'язаних із загальносвітовим кіберпростором. Міжнародна стратегія посилається на набір "ключових зобов'язань: основні свободи, недоторканість особистого життя громадян і вільний потік інформації" (ст. 5) у США. Згідно з цією стратегією, США повинні відігравати передову роль у майбутньому загальносвітовому кіберпросторі. Там обговорюються три цілі національної політики: зміцнення партнерських відносин, оборона (стримування) і технічно-економічний розвиток (інновації). У розділі про пріоритети політики подано набір напрямів дій для реалізації органами публічної влади. У межах цієї Стратегії передбачалося, що інші держави та міжнародні зацікавлені сторони мають узгодити власні стратегії кібербезпеки для ефективного розвитку загальносвітового кіберпростіру. Але такого узгодження досі не відбулося, як і підписання такого документу в цілому.

Таким чином, на основі аналізу наведених НСК можна запропонувати таку структуру НСК, яка може стати основою як для національних, так і для міжнародних документів з цієї проблематики:

1. Резюме.
2. Вступ.
3. Стратегічна візії кібербезпеки.
4. Зв'язок НСК з іншими стратегіями (національними і міжнародними) та існуючою правовою базою.
5. Керівні принципи.
6. Пріоритетні напрями діяльності у сфері кібербезпеки (бажано 1-4).
7. Короткий опис тактичних напрямів дій.
8. Глосарій (на основі міжнародного узгодженого набору визначень).
9. Додатки, що включатимуть передбачені функціональні заходи, визначені за допомогою SMART-підходу.

Залежно від цільової аудиторії та національних традицій, розділи НСК можуть містити описи інцидентів, статистику та супутні цитати ключових політичних діячів та лідерів індустрії. Це дозволяє підвищити рівень підтримки населення та підкреслити важливість питання. Якщо держава вирішила включити оцінку загроз та ризиків в SWOT-аналіз, його можна розмістити або між вступом та стратегічною візією кібербезпеки або як окремий додаток.

Висновки з даного дослідження та перспективи подальших розвідок у даному напрямку. Проведений аналіз НСК 14 країн дозволив виявити основні відмінності між ними, залежно від обраних пріоритетів: національна економіка (економічний підхід), національна безпека або оборона (державницький підхід). При цьому показано, що у більшості НСК зв'язки з існуючою національною та міжнародною політикою (наприклад, стратегією національного захисту ключових об'єктів інфраструктури, європейською установкою по електронним засобам комунікації і політикою національної політики) прописані нечітко.

Лише шість держав дали визначення поняттю "кібербезпеки". Інші вісім держав або роблять це описово у НСК або дають загальне розуміння. Це може призводити до непорозумінь на національному та міжнародному рівнях. Оскільки державам бракує узгодженої термінології, пов'язаної з кіберпростором, це може призводити до затримки зі спільним визначенням міжнародних загроз у кіберпросторі. Більш того, держави можуть по-різному розуміти сферу, яку повинна охоплювати кібербезпека: лише системи, підключені до Інтернету, чи всі ІКТ. Перший підхід, на нашу думку, є обмеженим, оскільки держави, зосереджені на Інтернет-безпеці несвідомо нехтують

захистом ІКТ, які (ще) не підключено до Інтернету, але які є частиною інших публічних мереж (наприклад, системи управління процесами у ключових об'єктах інфраструктури та об'єктах інфраструктури другорядного значення, а також медичні системи).

У своїх НСК всі держави вказують на міжнародні загрози та ризики у кіберпросторі. Між тим, щодо опису детальних планів дій з "міжнародної співпраці" більшість розглянутих НСК є доволі слабкими. Міжнародні аспекти такі як узгодження між різними країнами, спільне прискорення заходів з міжнародного реагування на кіберзлочини та інші порушення, відслідковування кіберзлочинців не входять до пріоритетних завдань значної кількості країн. Більшості НСК також бракує динамічного підходу до технологічних кіберзагроз та викликів у кіберпросторі.

У той же час, у більшості НСК визнається потреба залучення до її реалізації широких верств населення: громадян, компаній, публічного сектору та уряду. Щоправда, комплекси заходів, спрямованих на громадян, часто обмежуються навчальними кампаніями і уроками інформаційної безпеки в школах.

Комплексну програму, яка охоплює громадян та національні інструменти кібербезпеки, було впроваджено лише в Австралії. Це також свідчить про те, що більшість держав недооцінюють ризик втрати довіри громадськості до ІКТ, що, у свою чергу, може призвести до серйозних затримок у економічному розвитку та реалізації планів електронного уряду. Саме це, на наш погляд, слід враховувати під час розробки та реалізації національної стратегії кібербезпеки України.

Kotukh Ye. V.,
PhD in Technical Sciences, Associate Professor of Computer Science Department,
Sumy State University, Sumy
ORCID 0000-0003-4997-620X

NATIONAL CYBERSECURITY STRATEGIES: COMPARATIVE ANALYSIS

In this paper were compared and analyzed 14 National cybersecurity strategies (NCSS). Comparing this NCSS, major differences in approaches stemming from the differences in starting points are found: economics, national security, or military defence. Many of the NCSS are unclear about the relationship of the NCSS with existing national and international policies such as about CIP, the European Digital Agenda, and a national security policy.

Only six countries have defined the notion cyber security. The other eight countries either use descriptive text in their NCSS or a kind of common public understanding. As there is lack a harmonized cyber terminology, they might be hampered in collaboratively addressing the global threats to cyber space. Moreover, countries have a different understanding of the scope of what cyber security is supposed to cover: internet connected systems only or the whole of ICT.

All countries pointed in their NCSS the international threats and the risk of cyberspace. Nevertheless, the NCSS are relatively weak when describing detailed action plans under the topic "international collaboration". International topics such as harmonization activities across international borders, collaborative acceleration of international response to cyber crime and other disturbances do not seem to be on the priority lists of the governments.

Most NCSS lack a dynamic approach to cyberspace (technological) threats and challenges; only the UK mentioned electromagnetic spectrum threats to cyberspace. Emerging cyber security threats are only explicitly addressed by Germany and Japan in their NCSS, where the innovation cycle of ICT is high causing a fast appearance of new security risk.

When it comes to tactical and operational plans, only two countries use some of the SMARTness criteria. Interestingly, Uganda uses a system of metrics for the current state, the midway milestone, and the end result. Whether a strategy is a success or not, and whether the action plan is on the right track, cannot be measured when SMART criteria lack. Nations could implement a dashboard, including metrics related to dependence/relevance and to changing threats.

Most NCSS recognize the need for a society-wide approach: citizens, businesses, the public sector, and the government. However, the set of actions aimed at citizens is most often limited to

awareness campaigns and information security education at schools. Only Australia has an outreach programme which supports the citizens with national cyber security tools. This also shows that most countries underrate the risk of loss of public confidence in ICT which may seriously hamper economic prosperity and e-government plans.

Keywords: critical infrastructures; cybersecurity; cyberspace; information systems; policy; strategy.

References

1. Bert, G. R. M. Walker, J. M. (2019). Does Strategic Planning Improve Organizational Performance? doi.org/10.1111/puar.13104.

2. Council Directive 2008/114/EC on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection. (2008). European Commission, Brussels, Belgium. URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF.

3. Cyber Security Strategy. (2009). Office of the Attorney General, Australia. URL: http://www.ag.gov.au/www/agd/agd.nsf/Page/CyberSecurity_CyberSecurity#h2strategy.

4. Cyber Security Strategy for Germany. (2011). Federal Ministry of the Interior (Bundesministerium des Innern). Berlin, Germany. URL: http://www.cio.bund.de/SharedDocs/Publikationen/DE/IT-Sicherheit/css_engl_download.pdf?__blob=publicationFile.

5. Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space. (2009). Cabinet Office, London, UK. URL: http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf.

6. Cyber Sicherheitsstrategie fur Deutschland. (2011). Bundesministerium des Innern, Berlin, Germany. URL: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informations gesellschaft/cyber.pdf?__blob=publicationFile.

7. Defense et Securite nationale: Le Livre Blanc. (2008). Secretariat general de la Defense et de la Securite Nationale, Paris, France. URL: http://www.livreblancdefenseetsecurite.gouv.fr/IMG/pdf/livre_blanc_tome1_partie1.pdf.

8. Derrick, L. (2011). An Intelligent Use for Cupcakes Hacking Terrorist Sites URL: http://lafiga.firedoglake.com/2011/06/03/finally-an-intelligent-use-for-cupcakes-hacking-terrorist-sites.

9. Information Security Strategy for Protecting the Nation. (2009). Information Security Policy Council, Tokyo, Japan. URL: http://www.nisc.go.jp/eng/pdf/New_Strategy_English.pdf.

10. Information Systems Defence and Security: France's Strategy. (2011). Secretariat general de la defense et de la securite nationale, Paris, France. URL: http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Information_system_defence_and_security_- _France_s_strategy.pdf.

11. International Strategy for Cyberspace. (2011). The White House, Washington DC, USA. URL: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

12. Kiechel, Walter. (2010). The Lords of Strategy. Harvard Business Press.

13. Mintzberg, Henry, Quinn, James. (1996). The Strategy Process: Concepts, Contets, Cases. Prentice Hall.

14. National Cyber Security Strategies. (2012). European Network and Information Security Agency, Heraklion, Greece (ENISA). URL: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies- ncsss/cyber-security-strategies-paper/at_download/fullReport.

15. National Information Security Strategy (2011). Ministry of Information and Communication Technology, Republic of Uganda. URL: http://www.ict.go.ug/index.php?option=com_docman&task=doc_download&gid=49&Itemid=61.

16. Rauscher, K.F. and Yashenko, V. (Eds.). (2011). Critical Technology Foundations. EastWest Institute, London. URL: http://www.ewi.info/system/files/reports/Russia-U%20S%20%20bilateral%20on%20terminology%20v76%20%282%29.pdf.

17. Strategia de Securitate Cibernetica a Romaniei. (2011). Bratislava, Romania. URL: http://www.mcsi.ro/Transparenta-decizionala/21/Strategie_Cyber_23052011.

18. The National Cyber Security Strategy (NCSS): Success Through Cooperation. (2011). Netherlands Ministry of Security and Justice, The Hague, Netherlands. URL: http://www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011.

19. The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World. (2011). Cabinet Office, London, UK. URL: https://update.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategy-final.pdf.

Надійшла до редколегії 10.02.2021 р.