DOI 10.52363/2414-5866-2021-1-22
УДК 351.865

Котух Є.В., *к.т.н., СДУ, м. Суми, ORCID: 0000-0003-4997-620X*

Kotukh Ye., *Candidate of Technical Sciences, Associate Professor of Computer Science Department, Sumy State University, Sumy*

ПРОБЛЕМА КІБЕРШАХРАЙСТВА ТА ФАКТОРИ СТРИМУВАННЯ ЇЇ ВИРІШЕННЯ ОРГАНАМИ ПУБЛІЧНОГО УПРАВЛІННЯ

THE PROBLEM OF CYBERSPACE AND FACTORS HOLDING BACK ITS SOLUTION BY PUBLIC AUTHORITIES

У статті виокремлено низку проблем у сфері кібербезпеки в цілому, а також кібершахрайства зокрема, розглянуто конкретні дії країн-членів НАТО для підвищення рівня своєї кібербезпеки. Встановлено, що багато держав зі слабким кіберзахистом розважливо не дбають про вирішення цієї проблеми і тим самим створюють суспільну шкоду. Утім, існує група держав та міжнародних організацій, готових і здатних надати допомогу в забезпеченні кібербезпеки. Визначено низку перешкод, через які уповільнюється вирішення проблеми кібершахрайства. Доведено, що поки не визначено питання, чи можна класифікувати деякі види кібератак як еквіваленти збройних нападів у звичайній війні, ініціативи щодо зміцнення довіри в кіберпросторі, які вимагають наявності надійних режимів моніторингу, будуть марними.

Ключові слова*: публічне управління, Інтернет, кібербезпека, кіберпростір, кібершахрайство, НАТО.*

The article contains a number of problems in the field of cybersecurity in general, as well as cyber fraud in particular, and considers specific actions of NATO member countries to improve their cybersecurity. It has been established that many states with weak cyber defense prudently do not care about solving this problem and as a result create social harm. However, there is a group of states and international organizations that are ready and able to assist in cybersecurity. A number of obstacles have been identified that slow down the solution to the problem of cyber fraud. It has been shown that until the question of whether certain types of cyberattacks can be classified as equivalent to armed attacks in a conventional war has been identified (confidence-building initiatives in cyberspace that require robust monitoring regimes) will be futile.

Key words*: public administration, Internet, cybersecurity, cyberspace, cyber fraud, NATO.*

Постановка проблеми. Злочинність на сучасному етапі розвитку суспільства становить надзвичайно серйозну небезпеку для його подальшого розвитку.

Вийшовши за межі кордонів певної держави, злочинність набула небезпечного транснаціонального характеру, отримавши доступ до високих технологій, перш за все шахраї суттєво змістили свою діяльність у кіберпростір. Сьогодні суб'єктам публічного управління будь-якої держави досить важко самотужки вживати заходів для ефективної боротьби з кіберзлочинністю в цілому та таким явищем як кібершахрайство зокрема, не вдаючись до певного виду міжнародної співпраці у цій сфері. Але проблема полягає ще в тому, що реально надійний спільний захист кіберпростору несе із собою низку проблем, розгляд яких і стане метою нашого дослідження.

Аналіз останніх досліджень і публікацій. Питанням впливу кіберзагроз на життєдіяльність держав присвятили свої дослідження А. Крамер, Дж. Маркофф та Р.Харріс. С. Гейкен та Я. Трейнор розглядали питання кібервоєн та їх ознак. М. Ватіс, Т. Вінгфілд, В. Діфі, Д. Кларк, А. Соафер та А. Стейн опікувались проблемами міжнародної співпраці у царині кібербезпеки. Безпековій дилемі присвячено роботи Р. Джервіса та Г. Снайзера.

Виклад основного матеріалу. Відсутність дієвого зовнішнього контролю з боку органів публічного управління егоїстично мотивованих національних держав робить обман однією з найпроблемніших проблем міжнародної співпраці в цілому [4, с. 167] та у сфері кібербезпеки зокрема. Держави виявляються в ситуації, яка, як і знаменита дилема ув'язнених, позбавляє їх стимулів до співпраці, незважаючи на спільні інтереси [99, с. 35-38]. Міжнародні інститути (як у сфері захисту правопорядку, так і публічного управління) могли б допомогти у вирішенні цієї проблеми. Визначивши обов'язки і надавши механізми перевірки, вони можуть підтримати застосування принципу взаємовигідного співробітництва, що дозволило б стабілізувати співпрацю навіть між егоїстично мотивованими суб'єктами. Будучи стійкими структурами, міжнародні інститути також розширюють «тінь майбутнього» і змушують держави дбати про свою репутацію.

У контексті проблеми кібершахрайства, переважна більшість пересічних громадян насамперед стурбовані фінансовими втратами або зловживанням їх особистими даними, реальність цього питання для сфери публічного управління набагато ширша. У даний час ризик представляють не лише дуже часті кібератаки, що здійснюються для того, щоб, наприклад, отримати економічні вигоди, але також ненавмисно спричинені шкоди через порушення безпеки та цілісності мережі (внаслідок людських помилок, стихійних лих тощо). Отже, органи публічного управління мають бути здатними забезпечити ефективну відповідь на всі поточні та майбутні виклики в умовах постійно мінливих кіберзагроз, які можуть походити від кіберпростору, який динамічно розвивається і, таким чином, гарантувати безпечний та надійний кіберпростір.

Що стосується кіберпростору, то складнощі атрибуції у цьому просторі полегшують обман і шахрайство. Але потужні інституції можуть змінити це стано-

вище. Наприклад, держави могли б доручити міжнародному органу контролювати всі публічні та приватні мережі, що знаходяться під їх юрисдикцією. При наявності такої структури в кіберпросторі можуть бути створені добре відомі схеми на кшталт контролю над озброєннями. Зрозуміло, вони мають бути адаптовані до конкретної проблематики. Оскільки «справжньою зброєю» в кіберпросторі є знання, навряд чи має сенс класифікувати та забороняти певні можливості. Однак держави могли б домовитися про оголошення поза законом деяких дій, наприклад, кібератак на критично важливі інфраструктури, і покладатися на міжнародні органи для перевірки дотримання такої угоди. Така ж процедура могла б застосовуватися і в низці інших сфер.

Однак структури публічного управління в кіберпросторі – це двосічний меч. Ті ж самі структури, які вирішують проблеми шахрайства, швидше за все, створять проблеми іншого роду. Можна як аналогію взяти такий приклад: будь-яка установа, що має можливості та повноваження інспектувати засекречені мережі, стане основною мішенню для розміщення шпигунів спецслужбами різних держав. Тому ризики просто можуть переважати вигоди, оскільки структури в кіберпросторі є одночасно «вирішувачами проблем» і «творцями проблем». І публічна влада різних держав розуміє це добре. Розглянемо декілька прикладів, що ілюструють це.

Існує низка міжнародних інституційних платформ: наприклад, міждержавна Міжнародна мережа спостереження і попередження (IWWN), Форум груп з реагування на інциденти і забезпечення безпеки (FIRST), мережа публічних і приватних CERT, а також мережа Групи по боротьбі з високотехнологічної злочинністю. Однак на практиці інформація про високочутливі IT-вразливості майже виключно ділиться між близькими партнерами. Між європейськими CERT існують хороші робочі відносини. Ще краще співробітництво на двосторонньому рівні. Наприклад, німецькі спецслужби тісно співпрацюють з французькими та американськими колегами. Проте, важко уявити собі подібний рівень співпраці з Росією чи Китаєм. Причина цих обмежень в обміні даними проста: знання, корисні для захисту мереж, також корисні для атак в кіберпросторі. Характер загроз, про які спецслужби повідомляють іноземним агентствам, також свідчить про їх можливості виявлення та зворотного відстеження. Співпрацюючи агентства можуть використовувати ці знання для майбутніх атак на державу-інформатор. Тому на практиці США і Росія ніколи у суттєвому обсязі не обмінювались інформацією про інциденти в кіберпросторі, як це має бути відповідно до спільного меморандуму, підписаному в 2010 році [1010].

Інший приклад – інституціолізоване співробітництво між правоохоронними органами. Кіберзлочинці навмисно використовують інфраструктуру, що знаходиться під різними юрисдикціями. Найчастіше вони можуть ефективно і швидко замести сліди. Інші докази видаляються системними адміністраторами або провайдерами [1312]. Традиційна співпраця правоохоронних органів навряд

чи може відповідати цим реаліям. Недоліки традиційних процедур звернення за юридичною допомогою через офіційні дипломатичні канали є однією з причин того, що тільки приблизно 5 % кіберзлочинців коли-небудь арештовувались та піддавалися судовому переслідуванню [1413, с. 428]. Утім, згідно з дослідженням шахрайства щодо особистості в 2019 році від Javelin Strategy & Research, кількість споживачів, які стали жертвами шахрайства з особистими даними, в 2018 році впала до 14,4 млн дол. США проти рекордно високого показника у 16,7 млн дол. США в 2017 році. Однак жертви шахрайства з особистою особою в 2018 році більший фінансовий тягар: 3,3 млн людей були відповідальними за частину відповідальності за вчинене проти них шахрайство, майже втричі більше, ніж у 2016 році. Більше того, шахрайство з власними кишенями цих жертв з 2016 по 2018 рік зросло більш ніж удвічі 1,7 млрд дол. США. Втрати від шахрайства на нових рахунках також трохи зросли, і злочинці почали зосереджувати свою увагу на різних фінансових рахунках, таких як програми лояльності та винагород та пенсійні рахунки. Окрім того, злочинці стають досвідченими у перешкоджанні процесам автентифікації, особливо при поглинанні облікових записів мобільних телефонів. Ці поглинання майже подвоїлися до 680 000 жертв у 2018 р. порівняно з 380 000 у 2017 р. Дослідження зазначає, що перехід на вбудовані чіп-картки допомагає стримувати наявне шахрайство з картами, яке показало найсильніше зниження будь-якого типу шахрайства в 2018 році, з втратами на 14,7 млрд дол. США у 2018 році проти 16,8 млрд доларів у 2017 р [33].

Правоохоронні органи розробили неформальні структури, такі як «цілодобова» мережа підгрупи G7 по високотехнологічним злочинам, для забезпечення збереження цифрових доказів кіберзлочинів до початку офіційних процедур. Це, безумовно, гарний крок для поглиблення співпраці, однак заморожування та обмін даними все ще повинні бути санкціоновані кожним національним відомством в кожному окремому випадку.

Більш ефективним вирішенням проблеми кіберзлочинців, які випереджають правоохоронні органи, було б загальне та взаємне санкціонування так званих кроссбордерських пошуків. Цей термін відноситься до законного доступу до обладнання під іноземною юрисдикцією [86, с. 197; 8]. Конвенція Європейської ради по боротьбі з кіберзлочинністю, яку на сьогоднішній день ратифікували 33 країни, вже дозволяє проводити перехресний огляд при деяких особливих обставинах. Вони повинні бути санкціоновані провайдерами або адміністраторами, які можуть на законних підставах надавати доступ до даних або систем в кожному конкретному випадку12 [11]. Однак навіть ці обмежені положення є політично спірними. Деякі держави, такі як Росія, виправдовували своє неприєднання до Конвенції посиланнями на це конкретне положення [6]. Важко сказати, чи є цей аргумент просто відмовкою або виразом справжньої стурбованості. Адже всі положення про перехресний пошук дійсно можуть використовуватися як прикриття

для розвідувальних операцій. Тому найбільш ефективне інституційне вирішення проблеми кіберзлочинності пов'язане з найсерйознішим ризиком для національної безпеки. Принаймні, деякі держави думають про це саме так. Неясно, чи зможуть жорсткі вимоги щодо повідомлення та багатонаціональні правоохоронні групи – два засоби правового захисту, запропоновані деякими експертами [88], зняти ці побоювання.

Навіть серед союзників інституціоналізація співпраці у сфері кібербезпеки навряд чи набуває такої ж якості, як в інших тематичних сферах. Найкращим прикладом є Організація Північно-Атлантичного Договору (НАТО), і те, як вона вирішує так звану альянсну дилему. Союзники завжди потребують інституційних гарантій від двох основних ризиків: «захоплення» та «полишення» [77, с. 467]. Перше стосується ризику втягування у всілякі непотрібні конфлікти, які мають союзники з іншими державами. Друге стосується ризику залишитися на самоті під час реального конфлікту. Маючи на увазі ці ризики, НАТО стикається з різними імперативами: один закликає до більш низьких рівнів інтеграції, інший – до поглиблення союзницьких зв'язків. І слід визнати, що інституційна структура НАТО за часів холодної війни враховувала обидва імперативи. Розташування військових сил НАТО в Західній Європі гарантувало, що сили кожної держави-члена автоматично братимуть участь у бойових діях в разі конвенційної атаки держав Варшавського договору. Таким чином, страх полишення був зведений до мінімуму. У той же час мета НАТО була обмежена захистом територій її держав-членів. Обмеження мандата НАТО забезпечувало захист від ризиків захоплення.

Яким чином може бути досягнутий подібний баланс у сфері кібербезпеки? Мабуть, можна стверджувати, що існуючий рівень взаємозалежності між комп'ютерними мережами держав-членів вже працює проти ризику полишення. Однак випадок великомасштабних розподілених атак типу «відмова в обслуговуванні» (DDoS) на естонську Інтернет-інфраструктуру в 2007 році показав, що мережі більших країн-членів скоріше не постраждали від цих атак. Тому більш дрібні держави-члени схильні шукати формального підтвердження солідарності своїх союзників. Дійсно, відразу після DDoS-атак міністр оборони Естонії публічно обговорив питання про те, чи слід застосувати п'яту статтю договору НАТО у сфері кібербезпеки [1010]. Власне кажучи, НАТО і справді оголосила кібербезпеку новим пріоритетом у Лісабоні в 2010 році, але досі залишило відкритим питання про можливість застосування п'ятої статті 5 у сфері кібербезпеки. Таким чином, до сих пір не існує колективного стримування потенційних кібер-зловмисників. Можна вказати на декілька причин, по яких НАТО проявляє обережність у цьому відношенні. Одна з них – це питання визначень. Експерти в галузі міжнародного права досі визначаються з питанням, чи можна класифікувати деякі види кібератак як еквіваленти збройних нападів в звичайній війні [2; 1514], оскільки тільки на ці напади можна було б на законних підс-

тавах відповісти симетричними діями.

Інша причина вибору обережного підходу, на думку деяких експертів, – це очікування максимізації ризиків потрапляння в пастку. До тих пір, поки члени альянсу не будуть спільно контролювати всі свої національні мережі, окремі держави теоретично можуть проводити операції «під чужим прапором» проти своїх мереж [11]. Це може дати їм можливість підкріпити обвинувачення в агресії з боку інших держав, а якби кібератаки були класифіковані як «атаки за п'ятою статтею», то використовуючи вигадані атаки можна було б сподіватися залучити весь альянс до конфліктів з третіми державами. Окремі держави могли б також сфабрикувати докази, що збігаються з їх звинуваченнями, шляхом маніпулювання даними в своїх мережах. Потім вони могли б передати ці дані своїм партнерам по альянсу як casus belli. Щоб уникнути подібних ризиків, НАТО, звичайно, могли б створити загальну структуру моніторингу та перевірки. Але, як вже зазначалось вище, така структура була б кошмаром для будь-якого експерта з контррозвідки. І оскільки розумно вважати, що шпигунство відбувається навіть серед союзників, то шанси на те, що така структура публічного управління коли-небудь буде створена, невеликі.

Те, що буде реалізовано в межах НАТО відповідно до останніх намірів, у першу чергу стосується захисту власних мереж і можливостей НАТО. З цією метою альянс створив низку органів з управління комп'ютерними інцидентами та реагування на них. Крім того, НАТО має дослідні та навчальні центри, такі як Центр підвищення кваліфікації в галузі спільного кіберзахисту в Таллінні. Усі ці зусилля забезпечують реальне підвищення рівня кібербезпеки НАТО, і вони також побічно позитивно впливають на кібербезпеку кожної держави-учасниці.

Висновки. Озираючись на недавню історію технологічних інновацій, межа тисячоліть зазвичай вважається періодом часу, протягом якого Інтернет зробив революцію в способі ведення бізнесу та організації суспільного життя. З цим новим щаблем розвитку також з'явилися нові можливості для шахрайства – можливо, не дивно, що у світі, де шахраї йдуть за грошима та шукають оптимальну схему, яка допоможе їм збільшити свої статки. Однак викликає подив рівень, на якому кібершахрайство продовжує процвітати сьогодні, приблизно через 20 років після початку Інтернет-революції. Отже, аналіз виявив низку проблем, які перешкоджають протидії кібершахрайству:

– слабка міждержавна співпраця, особливо на рівні взаємодії національних служб, які опікуються кібербезпекою;

– відсутність зведеного банку даних, який би містив інформацію щодо методу, способу, виду шахрайства, характеристик шахрая та його жертви, мобільні телефони, IP-адреси шахраїв тощо;

– ризик зловживань з метою шпигунства, а тому політика колективного стримування кіберзагроз потребує інституційних гарантій від такого ризику.

References:

1. Gaycken, Sandro (2011). *Cyberwar: Das Internet als Kriegsschauplatz*. Open Source Press: München.
2. Hughes, Rex (2010). *A Treaty for Cyberspace*. International Affairs, 86 (2), 523-541.
3. Identity Fraud Study (2019). URL : https://www.javelinstrategy.com/coverage-area/2019-identity-fraud-report-fraudsters-seek-new-targets-and-victims-bear-brunt
4. Jervis, Robert (1978). *Cooperation under the Security Dilemma*. World Politics, 30 (4), 167-214.
5. Mansbach, Richard W.; Vasquez, John A. (1981). *In Search of Theory. A New Paradigm For Global Politics*. New York: Columbia University Press.
6. Markoff, John; Kramer, Andrew E. (2009). *U.S. and Russia Differ on a Treaty for Cyberspace.* The New York Times, 28.06.2009. URL : http://www.nytimes.com/2009/06/28/world/28cyber.html
7. Snyder, Glenn (1984). *The Security Dilemma in Alliance Politics*. World Politics, 36 (4), 461-495.
8. Sofaer, Abraham D.; Clark, David; Diffie, Whitfield (2010). *Cyber Security and International Agreements*. National Research Council: Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, Washington, DC: The National Academies Press, 179-206.
9. Stein, Arthur (1993). *Coordination and Collaboration: Regimes in an Anarchic World*. David A. Baldwin (Ed.): Neorealism and Neoliberalism: The Contemporary Debate, New York: Columbia University Press, 29-59.
10. The White House (2009). *Cyberspace Policy Review*. Washington, DC. URL : http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf
11. Traynor, Ian (2007). *Russia Accused of Unleashing Cyberwar to Disable Estonia*. The Guardian, 17.05.2007. URL : http://www.guardian.co.uk/world/2007/may/17/topstories3.russia (28.05.2011).
12. Vatis, Michael V. (2010). *The Council of Europe Convention on Cybercrime*. National Research Council: Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, Washington, DC: The National Academies Press, 207-224.
13. Vatis, Michael V. (2003). *International Cyber-Security Cooperation: Informal Bilateral Models.* James A. Lewis (Ed.): Cyber Security: Turning National Solutions into International Cooperation, Washington, DC: CSIS Press, 1-12.
14. Wilson, Clay (2009). *Cyber Crime.* Franklin D. Kramer; Stuart H.Starr; Larry K. Wentz (Eds.): Cyberpower and National Security, Washington, DC: National Defense University Press, 415-436.
15. Wingfield, Thomas C. (2009). *International Law and Information Operations.* Franklin D. Kramer; Stuart H.Starr; Larry K. Wentz (Eds.): Cyberpower and National Security, Washington, DC: National Defense University Press, 525-542.