УДК: 32.327: 341.161

ІНСТИТУЦІЙНА СКЛАДОВА МЕХАНІЗМУ ПРОТИДІЇ КІБЕРТЕРОРИЗМУ: ДОСВІД ЄС

Зінченко О. І.

e-mail: alekca.98@ukr.net

Харківський національний університет імені В. Н. Каразіна, Україна, Харків

Остання чверть XX століття ознаменувала собою вступ людства в епоху інформаційного суспільства, що мало наслідком використання інформаційних технологій та мережі Інтернет в усіх сферах суспільного та державного життя. Проте, поряд з очевидними перевагами інформатизація суспільства сприяла й виникненню та поширенню особливих типів правопорушень із застосуванням інформаційно-телекомунікаційних засобів, що порушують права як кожної окремої особи, наприклад, шляхом отримання доступу до конфіденційних даних, так і посягають на національну безпеку однієї чи декількох держав, наприклад, шляхом здійснення кібератак на інформаційні системи різних державних органів та установ. Таким чином, питання протидії проявам кібертероризму як всередині країни, так і в межах конкретного регіону та всього світу потребують невідкладного вирішення, що й зумовлює актуальність теми даного дослідження.

Ключові слова: кібербезпека, кіберпростір, кібертероризм, інформаційні технології, регіональна безпека, тероризм.

Зинченко А. И., Институциональная составляющая механизма противодействия кибертерроризму: опыт ЕС / Харковський национальный университет имени В. Н. Каразина

Последняя четверть XX века ознаменовала собой вступление человечества в эпоху информационного общества, в следствии использования информационных технологий и сети Интернет во всех сферах общественной и государственной жизни. Однако, наряду с очевидными преимуществами информатизация общества способствовала возникновению и распространению особых типов правонарушений с применением информационно-телекоммуникационных средств, нарушающих права как отдельной личности, например, путем получения доступа к конфиденциальным данным, так и посягают на национальную безопасность одного или нескольких государств, путем осуществления кибератак на информационные системы различных государственных органов и учреждений. Таким образом, вопрос противодействия проявлениям кибертерроризма как внутри страны, так и в пределах конкретного региона и всего мира требуют безотлагательного решения, что и обуславливает актуальность темы исследования.

Ключевые слова: кибербезопасность, киберпространство, кибертерроризм, информационные технологии, региональная безопасность, терроризм.

O. Zinchenko, The institutional component of the mechanism for countering cyber terrorism: the EU experience / N. Karazin National University, Ukraine, Kharkiv

The last quarter of the 20th century marked the entry of humanity into the era of the information society, as a result of the use of information technology and the Internet in all spheres of public and public life. However, along with obvious advantages, informatization of society contributed to the emergence and spread of special types of offenses with

the use of information and telecommunication tools that violate the rights of an individual, for example, by gaining access to confidential data, and encroach on the national security of one or more states by cyber attacks on information systems of various government bodies and institutions. Thus, the issue of countering the manifestations of cyberterrorism both within the country and within a particular region and the whole world requires an urgent solution, which determines the relevance of the research topic.

Key words: cybersecurity, cyberspace, cyberterrorism, information technology, regional security, terrorism.

У сучасному світі інформація виступає найважливішим компонентом розвитку суспільства. Перетворення постіндустріального суспільства в інформаційне означає, що інформація набуває глобального характеру, стає значущою як для людини особисто, так для держави і суспільства в цілому. Сьогодні кожен може шукати, одержувати, зберігати, використовувати і поширювати інформацію будь-яким законним способом, оскільки для її потоків не існує кордонів. Однак, транскордонний характер інформації не тільки дає можливість вільного користування будь-яким її видом, проте й породжує певні загрози. Сьогодні, свобода в пошуку та отриманні інформації сприяє її підвищеній ураженості, адже можливість вільного доступу до будь-яких ресурсів із будь-якої точки світу провокує можливість вчинення терористичних дій у кіберпросторі, залишаючись непоміченим. І тут вже можна говорити про кібертероризм, що сьогодні турбує всю світову спільноту. Проте наскільки він є небезпечним як про нього говорять? Розглянемо дане питання, сконцентрувавшись на регіональному контексті, а саме на Європейському Союзі.

Зауважимо, що питання кібертероризму тією чи іншою мірою вже було предметом розгляду таких вчених, як: Ю. Р. Акчурін, К. Баррі, А. В. Возженіков, В. О. Голубев, С. О. Гнатюк, І. В. Діордіца, В. М. Фурашев, О. Г. Широкова-Мурараш, та ін. При всій важливості цих наукових досліджень їх аналіз дозволяє стверджувати, що ряд питань лишаються відкритими, зокрема відсутність легального єдиного поняття «кібертероризм» у більшості країн Європи та системи чітких механізмів протидії кібертероризму на регіональному та національному рівнях.

Теперішня ситуація, коли лише «кліком» мишки можна знищити будь-яку систему життєдіяльності, кібертероризм набуває все більшої актуальності. Привабливим для кібертерористів є той фактор, що для здійснення атаки необхідний лише персональний комп'ютер та доступ в мережу Інтернет, фінансові витрати майже нульові, а результат може бути сильніше навіть ніж при використанні класичних терористичних засобів. Ситуація, що складається в останні роки непокоїть європейську спільноту, тож дає поштовх до пошуку рішень і методів захисту інформаційного простору як кожної держави окремо, так і ЄС в цілому. Отже, актуальність даної теми полягає у тому факті, що у міру того як сучасне суспільство все більше занурюється в інформаційний простір, а повсякденне життя людей цілком інтегрується з новітніми цифровими технологіями, все частіше доводиться стикатися з різними проявами нового виду терористичних актів, скоєних в кібернетичному просторі, тож дані питання потребують невідкладного вирішення як всередині кожної з європейських країн, так і в Європейському регіоні в цілому. Ефективне регіональне співробітництво в галузі попередження і ліквідації наслідків кібертероризму має величезне значення.

Для початку, визначимо, що під регіональною безпекою розуміється сукупність принципів і норм, що діють в межах визначеного регіону і регулюють співробітництво держав регіону в сфері підтримки миру і безпеки [1].

Під явищем кібертероризму ж будемо розуміти поєднання класичного терміну «тероризм» із поняттям «кіберпростору», власне де тероризм вчиняється. Ми вважаємо найбільш прийнятним в контексті даної роботи визначення кіберпростору, дане українським вченим Фурашевим В.М. Вчений розглядає кіберпростір як форму співіснування сукупності матеріальних та нематеріальних об’єктів і процесів, спрямованих на породження, сприйняття, запам’ятовування, переробку та обмін інформацією [2]. У Законі України «Про боротьбу з тероризмом» за № 638-IV від 20 березня 2001 року зі змінами 14 листопада 2018 року це явище трактується так: «Тероризм – суспільно небезпечна діяльність, яка полягає у свідомому, цілеспрямованому застосуванні насильства шляхом захоплення заручників, підпалів, убивств, тортур, залякування населення та органів влади, або вчинення інших посягань на життя чи здоров’я ні в чому не винних людей, або погрози вчинення злочинних дій з метою досягнення злочинних цілей» [3]. Отже, за допомогою аналізу та компіляції понять, отримаємо, що «кібертероризм»-це зближення тероризму і кіберпростору із використанням високих технологій як зброї задля нападу на інформацію, комп'ютерні системи, комп'ютерні програми та дані з метою створити паніку, плутанину і невизначеність серед населення, вплинути на уряд або міжнародну спільноту відповідно до певної політичної, соціальної чи ідеологічної програми, і може призвести до відключення або видалення критичних для інфраструктури об'єктів даних або інформації чи навіть до провокації воєнного конфлікту. Можна зауважити, що кібертероризм

використовує відкритість Інтернету для дискредитації урядів і держав, розміщення сайтів терористичної спрямованості, псування і руйнування ключових систем шляхом внесення в них фальсифікованих даних або постійного виведення цих систем з робочого стану, що породжує страх і тривогу, і є свого роду доповненням до традиційного виду тероризму.

Починаючи розглядати методи протидії ЄС вкрай небезпечному явищу, потрібно відмітити, що значним кроком у формуванні регіональної правової бази в напрямку боротьби із кібертероризмом та забезпечення кібербезпеки стало підписання 23 листопада 2001 року представниками країн-членів Ради Європи, США, Канади та Японії Конвенції Ради Європи «Про кіберзлочинність» (далі – Конвенція). Конвенція підписана 43 членами ЄС і 15 іншими країнами, включаючи США. На сьогодні конвенція є єдиним уніфікованим документом, що визначає питання злочинних дій у кіберпросторі, а також врегулює питання відповідальності за кримінальні злочини, пов'язані з комп'ютерними системами і даними. У ній визначено поняття кіберзлочину, а також детально описані проблеми взаємодії правоохоронних органів окремих держав в ситуації, коли злочинець і жертва знаходяться в різних країнах та на них розповсюджується різне законодавство, окремо приділяється увага боротьбі з терористичною діяльністю у кіберпросторі. Конвенція передбачає здійснення захисних дій на рівні держав-учасників, а також на регіональному та міжнародному рівнях. Оскільки кіберзлочинність загалом, та кібертероризм, як її новий прояв мають багато спільних ознак, передбачена Конвенцією відповідальність за будь-які здійснювані кібератаки, незалежно від їх мотивів, передбачає, що підписавши її, країни повинні на вимогу уповноважених органів затримувати і передавати в руки правосуддя всіх кіберзлочинців.

Однак, сьогодні кількість кібератак невпинно зростає, що породжує реальні загрози для безпеки суспільства.

Визнаючи реальність таких загроз, 13 березня 2004 році на базі ЄС було створено Агентство з мереж і інформаційної безпеки (ENISA), яке постійно проводить моніторинг користувачів мережі, відповідно до цього вносить поправки до вже прийнятих проектів, які стають законами і дотримуються країнами ЄС. Агентство було створено з метою регулювання та запобігання мережевих та інформаційних загроз, зміцнення багатостороннього діалогу всередині Європи і за його межами з проблеми кіберзлочинності та кібертероризму, розвитку культури мережевої та інформаційної безпеки в інтересах громадян, підприємств і організацій державного сектору Європи для сприяння нормальному функціонуванню Європейського регіону. ENISA надає консультації щодо передової практики, та проводить експертизи аналізу існуючих ризиків та надає допомогу державам-членам та європейським органам влади [4]. У доповнення до зазначених дій, у листопаді 2010 були проведені перші загальноєвропейські вчення з питань захисту інфраструктури критичної інформації (CIIP). Cyber Europe 2010 була організована державами-членами ЄС, за підтримки Європейського агентства мережевої та інформаційної безпеки (ENISA), а також за підтримки Спільного дослідницького центру (JRC). Мета даних вчень полягала в тому, щоб спровокувати комунікацію та співпрацю між країнами Європи у реагуванні на масштабні напади. Вчення Cyber Europe - це моделювання масштабних інцидентів кібербезпеки, які переростають у кіберкризи. Навчання пропонують можливість проаналізувати передові технічні інциденти, пов'язані з кібербезпекою, а також розв'язати складні ситуації з безперервністю бізнесу та кризовими ситуаціями. Під час тренувань експерти Cyber Europe 2010 від

європейських країн працювали разом, щоб протистояти спробам хакерів паралізувати Інтернет та критичні інфраструктури, особлива увага приділялася захисту інформаційних мереж саме від кібертерористичних атак. Ці вчення були першим, ключовим кроком у боротьбі з потенційними проявами кібертероризму для основної критичної інфраструктури, а також зміцнення безпеки як окремого громадянина європейської держави, так і ЄС в цілому. Результати кібервчень наголосили також на створенні додаткових структур, які б переслідували ті ж цілі що й ENISA, але розробляли більш конктеризовані й цілеспрямовані методи боротьби та протистояння кібертероризму. Так, 2011 році для підтримки різних груп IT-безпеки в установах ЄС в їх боротьбі з кіберзагрозами різних видів була створена група реагування на надзвичайні ситуації (CERT-EU). Вона діє як центр обміну інформацією про кібербезпеку і координує реагування на кіберінциденти, під якими розуміють подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів. CERT-EU тісно співпрацює з іншими CERT-ами в державах-членах і за їх межами, а також зі спеціалізованими компаніями в області інформаційної безпеки. [4]. Наступним надважливим кроком у вдосконаленні Європейської регіональної системи безпеки стала Стратегія ЄС з кібербезпеки, що була

прийнята у 2013 році і встановила «пріоритетну міжнародну політику у сфері кіберпростору для ЄС» у п'яти пріоритетах: забезпечення стійкості кіберпростору Європейського союзу; скорочення кількості кіберзлочинів; розвиток політики кібероборони, яка включає сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії [5] на основі Спільної політики безпеки і оборони Європейського союзу; розвиток виробничо-технологічних ресурсів для забезпечення кібербезпеки; створення узгодженої всіма членами Євросоюзу міжнародної політики з кібербезпеки з іноземними партнерами для підвищення кооперації в цій галузі з третіми країнами.

Згідно зі стратегією, фінансові, транспортні та енергетичні компанії повинні розробити і вжити заходів з протидії можливим кіберзагрозам. У підсумку, понад 40 тис. європейських організацій зобов'язані звітувати про спроби кібератак, а найважливіші для економіки і інфраструктури підприємства повинні доводити надійність свого захисту. Стратегія стала першим всеохоплюючим документом ЄС у даній сфері. Документ охоплює усі аспекти кіберпростору: внутрішній ринок, правосуддя, внутрішню та зовнішню політику [6]. Стратегії передувало створення 11 січня 2013 року Європейського центру по боротьбі з кіберзлочинністю (ЕС3). Його розвиток став пріоритетним напрямком в Стратегії безпеки ЄС, і був активно підтриманий міністрами Євросоюзу. Центр був створений на базі Європолу. [7]. З моменту свого створення ЕС3 зробив значний внесок у боротьбу з кібертероризмом, він був залучений до десятків гучних операцій і сотень розгортань операційної підтримки на місці, що

призвели до арештів, а також проаналізував сотні тисяч файлів, переважна більшість з яких виявилися шкідливими. ЕС3 спирається на існуючий потенціал правоохоронних органів Європолу, але він також має інші значно розширені можливості, зокрема, надання оперативної та аналітичної підтримки у розслідуванні кібертерористичних атак державами-членами. Ці заходи також підтримуються командою Cyber Intelligence (CIT), аналітики якої збирають та обробляють інформацію, пов'язану з кібертероризмом, з державних, приватних та відкритих джерел, а також визначають нові загрози та закономірності. Спільну роботу з ЕС3 проводить Спільна робоча група з кіберзлочинності (J-CAT), яка працює над найважливішими міжнародними справами про кіберзлочинність, які стосуються держав-членів ЄС та їхніх громадян [8].

Отже, кібертероризм є найнебезпечнішим серед всіх різновидів кіберзлочинів, так як цілями нападу обираються різні важливі державні та регіональні інфраструктури типу енергопостачання або транспортного сполучення. Оскільки атаки такого роду можуть швидко зруйнувати інфраструктуру держави, вони вважаються ідеальним засобом ослаблення нації. Успішно проведена кібератака на ключові точки інфраструктури може запросто паралізувати країну на деякий час, завдавши колосальних збитків. На щастя, багато країн визнають реальну загрозу кібертероризму і роблять кроки по захисту державних і громадських систем від будь-якого типу кібератак. Таким чином, можна визначити, що ЄС і його держави-члени, а також інституції ЄС загалом виробляють значну документальну базу та запускають широкомасштабні програми та ініціативи для посилення кібербезпеки у відповідь на виклики кібертероризму, пов’язані із загрозою безпеки громадян та критичній інфраструктурі кожної з європейських держав та ЄС в цілому. Проте, тільки технології і тільки внутрішня політика не

можуть забезпечити ефективний захист від кіберзлочинності та кібертероризму, необхідним залишається вдосконалення нормативного забезпечення на національному та регіональному рівнях, а також впровадження нових заходів та процедурних норм у регіональній взаємодії та співробітництва.

Література:

1. Шаклеина Т.А. (2002). Внешняя политика и безопасность современной России: в 4т. Москва: Московский государственный институт международных отношений (У) МИД России, Российская ассоциация международных исследований, АНО «ИНО-Центр (Информация. Наука. Образование.)». Т. 2: Исследования. 446 с.

2. Фурашев В.М. (2012). Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право.* 2012. № 2. С. 162 –169

3. Про боротьбу з тероризмом: Закон України від 20.03.2003 № 638-IV. URL: https://zakon.rada.gov.ua/laws/show/638-15 (дата звернення 22.05.2021)

4. The European Union Agency for Network and Information Security (ENISA). URL: https://www.enisa.europa.eu (Last Accessed 22.05.2021)

5. Convention on Cybercrime: Council of Europe. – 2311. URL: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf (Last Accessed 22.05.2021)

6. European Commission. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. *The European Union Agency for Network and Information Security (ENISA).* 2013. URL: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (Last Accessed 22.05.2021)

7. Europol. Our Thinking. A strategy for security. URL: https://www.europol.europa.eu/about-europol/our-thinking (Last Accessed: 22.05.2021).

8. EUROPOL. About EC3. URL: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3(Last Accessed: 22.05.2021).

References:

1. Shakleyna T.A. (2002). Vneshnyaya polytyka y bezopasnost' sovremennoy Rossyy: v 4t. Moskva: Moskovskyy hosudarstvennyy ynstytut mezhdunarodnykh otnoshenyy (U) MYD Rossyy, Rossyyskaya assotsyatsyya mezhdunarodnykh yssledovanyy, ANO «YNO-Tsentr (Ynformatsyya. Nauka. Obrazovanye.)» T. 2: Yssledovanyya. 446 s.

2. Furashev V. M. Kiberprostir ta informatsiynyy prostir, kiberbezpeka ta informatsiyna bezpeka: sutnist', vyznachennya, vidminnosti. Informatsiya i pravo. 2012. № 2. S. 162 –169

3. Pro borot'bu z teroryzmom: Zakon Ukrayiny vid 20.03.2003 № 638-IV. URL: https://zakon.rada.gov.ua/laws/show/638-15 (data zvernennya 22.05.2021)

4. The European Union Agency for Network and Information Security (ENISA). URL: https://www.enisa.europa.eu (Last Accessed 22.05.2021)

5. Convention on Cybercrime: Council of Europe. – 2311. URL: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf (Last Accessed 22.05.2021)

6. European Commission. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. *The European Union Agency for Network and Information Security (ENISA).* 2013. URL: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (Last Accessed 22.05.2021)

7. Europol. Our Thinking. A strategy for security. URL: https://www.europol.europa.eu/about-europol/our-thinking (Last Accessed: 22.05.2021).

8. EUROPOL. About EC3. URL: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3(Last Accessed: 22.05.2021).