УДК 343.34:004.087

КІБЕРТЕРОРИЗМ: ТЕНДЕНЦІЇ РОЗВИТКУ ТА МЕХАНІЗМИ ПРОТИДІЇ

Вейтас М. В. Лукашенко М. І.

Національний юридичний університет ім. Ярослава Мудрого, Україна, Харків

Дана стаття присвячена дослідженню проблематики виникнення та розвитку кібертероризму. З урахуванням актуальної на час написання статті нормативно-правової бази розглянуто підходи до визначення поняття «кібертероризму» як на доктринальному, так і на законодавчому рівні. Внаслідок проведення системного аналізу найбільш масштабних випадків кібертероризму у світі запропоновані шляхи боротьби зі вказаним злочином. Авторами обгрунтовані негативні аспекти суцільної автоматизації усіх сфер суспільного життя та, у контексті процесів глобалізації та інтеграції між державами, виявлена необхідність взаємодії правоохоронних структур міжнародної спільноти для досягнення ефективних результатів протидії кібертероризму.

Ключові слова: кібертерор, кіберзлочинність, протидія, злочин, кримінальне законодавство України.

Вейтас М. В., Лукашенко М. И. Кибертерроризм: тенденции развития и механизмы противодействия / Национальный юридический университет им. Ярослав Мудрого Украина, Харьков

Данная статья посвящена исследованию проблематики возникновения и развития кибертерроризма. С учетом актуальной, на момент написания статьи, нормативно-правовой базы рассмотрены подходы к определению понятия «кибертерроризма» как на доктринальном, так и на законодательном уровне. В

результате проведения систематического анализа наиболее масштабных случаев кибертерроризма в мире, предложены пути борьбы с указанным преступлением. Авторами обоснованы негативные аспекты полной автоматизации всех сфер общественной жизни, а так же в контексте процессов глобализации и интеграции между государствами, выявлена необходимость взаимодействия правоохранительных структур международного сообщества для достижения эффективных результатов противодействия кибертерроризму.

Ключевые слова: кибертеррор, киберпреступность, противодействие, преступление, уголовное законодательство Украины.

M. Veitas, M. Lukashenko Cyberterrorism: Development Trends And Mechanisms Of Cooperation / Yaroslav Mudryi National Law University, Ukraine, Kharkiv

The article represents the study of cyberterrorism genesis and development. Considering the legal framework relevant at the time of writing different approaches to the definition of counterterrorism have been reviewed on both the doctrinal and legislative levels. As a result of systematic analysis of the most massive cases of cyberterrorism in the world the methods of combating have been suggested. The authors have substantiated negative aspects total automatization in all spheres of social life. Additionally, in context of globalization and international intergration, the collaboration between law-enforcement bodies and world community is found to be necessary in order to effectively combat cyberterrorism.

Key words: cyberterror, cybercrime, counteraction, crime, criminal legislation of Ukraine.

Вступ. XXI століття – епоха активного розвитку процесів інтеграції та модернізації в міжнародний простір, в межах яких проходить суттєве розширення масштабу інтернаціоналізації найважливіших аспектів державного життя. До таких аспектів, з огляду на їх глобальне впровадження, відносять суцільну автоматизацію установ, підприємств та організацій. В останні роки світова спільнота мала змогу спостерігати за зростанням кількості різного роду втручань у роботу інформаційних систем, які призводили до наслідків у вигляді порушення нормального функціонування найважливіших систем життєзабезпечення держави зокрема. На жаль, провідні держави світу, незважаючи на розвиненість правової та технічної регламентації захисту від несанкціонованого впливу в діяльність інфраструктури інформаційних технологій, не в змозі забезпечити її стовідсотковий захист. Можна констатувати факт того, що правоохоронні органи не в змозі контролювати кіберзлочинність, яка, внаслідок, стала транснаціональною проблемою. Проте усвідомлення вразливості інформаційних систем та, як наслідок, напрацювання в сфері розроблення адекватного законодавчого регулювання та алгоритмів швидкого реагування дозволять мінімізувати втрати від подібного роду атак.

Тема наукової статті була об’єктом наукових розробок таких зарубіжних та вітчизняних науковців, як Гнатюк С. О., Марченко А. В., Полліт М., М. Каветлі, Бурячок В. Л., Старостіна Е., Щетилов А, Богуш В. М. та інші. Незважаючи на достатньо широку наявну теоретичну базу науковцями не було досягнуто єдиної думки стосовно підходу до визначення понять «кіберзлочинності» та «кібертероризму», зокрема дискусійним залишається питання стосовно кола суб’єктів вчинення злочину.

Мета статті. Визначення тенденцій розвитку та механізмів протидії кібертероризму.

Виклад основного матеріалу. Згідно Доктрини інформаційної безпеки України, інформаційна безпека визначена невід'ємною складовою національної безпеки і, у той же час, важливою її самостійною сферою, а згідно ст.17 Конституції України вона детермінується як одна із головних функцій держави [1]. Фундаментальною основою якісної боротьби з кібрзлочинністю є розуміння сутності процесів, які мають місце при функціонуванні інформаційного простору тієї чи іншої держави. А тому, для якісного наукового та практичного осмислення даної проблематики потрібно визначити власне сутність вживаних термінів шляхом виділення понятійного апарату у сфері кіберпростору. Вперше термін «кібертероризм» був введений в обіг в 1980-х р. науковим співробітником Каліфорнійського Інституту безпеки і розвідки Баррі Колліном, який сформулював його у контексті тенденції до переходу тероризму від фізичного до віртуального.

Пізніше, в 1997 році, агент ФБР Марк Полліт витлумачив відносно нову дефініцію як: « кібертероризм – це навмисна політично-мотивована атака проти інформацій, комп'ютерних систем, комп'ютерних програм та баз даних у вигляді насильного втручання з боку міжнародних груп або секретних агентів»

«Словник терроризму» описує кібертероризм як «злочин, до якого в майбутньому буде вдаватися криміналітет, використовуючи комп'ютери». При цьому зазначається, що «кібертерористи мають політичну мотивацію для їх злочинів» [2, с. 24].

На думку М. Каветлі доцільним є таке визначення терміну кібертероризму: «Під кібертероризмом розуміємо незаконні напади з боку недержавних суб'єктів стосовно комп'ютерів, мереж та

інформації, що міститься в них, які здійснюються з метою залякування уряду (чи населення) чи з метою досягнення певної поведінки суб'єкта, що залякується. Кібератака може розумітись як кібертероризм лише в тому випадку, якщо це призводить до фізичного насилля проти осіб чи власності або виникнення значного страху у зв'язку з можливістю здійснення таких наслідків» [3,с.1]. Ми вважаємо, що таке тумачення є не зовсім коректним в частині окреслення кола суб'єктів вчинення злочину через його обмеженість – таким суб'єктом можуть бути і державні структури в тому числі.

Більш широкого трактування притримується А. Марченко, зазначаючи, що під кібертероризмом слід вважати «...навмисне застосування окремими особами, терористичними групами або організаціями засобів інформаційного насильства з метою руйнації єдиного інформаційного поля, нанесення економічної шкоди країні, створення атмосфери істерії в соціумі, нав'язування конкретної лінії поведінки у вирішенні внутрішніх і зовнішніх суперечок» [5, с. 356].

Водночас вітчизняний науковець Гнатюк зауважує, що кібертероризм є рідновидом тероризму, однак поряд із такими його формами, як ядерний, біологічний, хімічний, екологічний, комп'ютерний (кібернетичний), з огляду на масову інформатизацію суспільства, несе одну із найбільших і найсерйозніших загроз людству [4].

Незважаючи на грунтовні доктринальні напрацювання у сфері визначення досліджуваного поняття, єдиного чіткого визначення поняття «кібертероризму» як на рівні національного, так і міжнародного законодавства немає.

У 1999 році в Женеві відбувся міжнародний семінар з питань міжнародної інформаційної безпеки, у роботі якого взяли участь

представники понад 50 країн. Вони підтвердили актуальність і важливість проблеми інформаційної безпеки на міжнародному рівні.

На 54-ій сесії Генеральної Асамблеї ООН (1999-2000 рр.) було запропоновано проект Резолюції «Досягнення у сфері інформатизації і телекомунікації у контексті міжнародної безпеки», у якому вперше висловлювалось занепокоєння щодо можливості потенційного використання засобів інформаційно-комунікативних технологій (далі – ІКТ) «з цілями, що несумісні із завданнями забезпечення міжнародної стабільності та безпеки», що може негативно вплинути на безпеку держав як у цивільній, так і військовій сферах. Вважаючи за необхідне упередити «неправомірне використання або використання інформаційних ресурсів чи технологій у злочинних або терористичних цілях», Генеральна Асамблея порушила питання про «доцільність розробки міжнародних принципів, направлених на зміцнення безпеки глобальних інформаційних і телекомунікаційних систем і сприяння боротьбі з інформаційним тероризмом і криміналом»[7, с. 6].

У Ковенції Ради Європи про кіберзлочинність від 23.11.2001 р. немає чіткої дефініції «кібертероризму», проте з її положень випливає, що кібертероризмом є навмисне застосування незаконно встановленого повноваження, насильства, руйнування або проникнення в кіберсистеми, у разі якщо подібні дії можуть спричинити смерть або заподіяти шкоду особі або особам, істотної шкоди майну, цивільний безлад або значну економічну шкоду [6]. Варто зазначити, що цю Конвенцію можна сміливо назвати актом реагування на терористичні акти 11 вересня 2001 року в США, який дав початок розробкам проблематики захисту світової спільноти від кібертероризму. У документі згадується 4 типи комп'ютерних злочинів: незаконний доступ; незаконне перехоплення; втручання в дані; втручання в систему. Згідно з цим документом, засобами

кібертероризму є: комп'ютерна система, комп'ютерні дані, послуги інформаційно-комп'ютерних технологій та дані трафіку.

У червні 2015 року Парламентська Асамблея Ради Європи ухвалила резолюцію 2070(2015) «Зміцнення співпраці у протидії кібертероризму та іншим масштабним атакам в Інтернеті», в якій міститься заклик до країн-членів Ради Європи запровадити визначення кібертероризму та відповідальності за нього.

На сьогодні виникає нагальна потреба у спеціальному законі, який би врегульовував відносини, які виникають у кібернетичному просторі. Звичайно, така потреба виникла не сьогодні та не вчора, а прийняття таких необхідних нормативних актів значно затягнулось. На сьогодні простежується тенденція виникнення нових понять і термінів, і відповідно "шкутильгання" правотворчості, яка покликана в даному випадку опосередковувати та регулювати правовідносини в інформаційній сфері [8, с. 105].

У п. 13 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» в редакції від 05.10.2017 р. зазначається, що кібертероризм – терористична діяльність, що здійснюється у кіберпросторі або з його використанням.

Закон України «Про основи національної безпеки України» визначає комп'ютерну злочинність та комп'ютерний тероризм як одну із головних загроз національним інтересам та національній безпеці України.

Наразі Кримінальний Кодекс України не виокремлює поняття кібертероризму в якості злочину, лише окремим розділом XVI Кримінального кодексу України визначено злочини у сфері використання електронно-обчислювальних машин (ком'ютерів), систем та комп'ютерних мереж чи мереж електрозв'язку [9].

Проте варто зазначити, що провадиться законодавча робота у сфері створення нормативної бази, яка б захищала суспільство та державу в цілому від проявів агресії в кіберпросторі. Зокрема на порядок денний восьмої сесії Верховної ради восьмого скликання в редакції від 17.05.2018 року пропонується підготувати та доопрацювати для розгляду на сесії Проект Закону про внесення змін до Кримінального кодексу України 2439а від 24.07.2015 щодо встановлення відповідальності за кібертероризм, який було надано ініціативною групою народних депутатів . В проекті пропонується доповнити Кримінальний кодекс України статтею 258^6, яка б визначала відповідальність за кібертероризм та використовується такий варіант терміну: «Кібертероризм, тобто умисна атака на інформацію, яка обробляється комп'ютером, комп'ютерну систему чи комп'ютерні мережі, що створює небезпеку для життя і здоров'я людей або призводить до інших тяжких наслідків, якщо такі дії були скоєні з політичних мотивів, з метою порушення суспільної безпеки, залякування населення, провокації військового конфлікту…» [10]. Цілями прийняття Закону про внесення змін до Кримінального кодексу України автори Проекту зазначають можливість законодавчо визначити поняття кібертероризму й встановити кримінальну відповідальність за вчинення актів кібертероризму, що у свою чергу посилить заходи боротьби з кіберзлочинами направленими на підрив національної безпеки, залякування населення, провокацій військового конфлікту, створення небезпеки для життя і здоров’я громадян та інших тяжких наслідків [10].

На нашу думку, для демонстрації високої суспільної небезпеки такого роду атак варто навести приклади найбільш серйозних прецедентів, які призвели до надзвичайно тяжких наслідків. Так, перша кібератака на критичну інфраструктуру відбулася ще до появи

Всесвітньої Мережі – в 1982 році групі хакерів вдалося завантажити тип вірусу «Троян» в автоматизовану систему управління сибірського нафтопроводу, що призвело до масштабного вибуху. «Акція» була спланована та реалізована спецслужбами Сполучених Штатів. Проте більше двадцяти років причина вибуху залишалася незрозумілою, допоки колишній секретар Міністерства оборони США і радник Р. Рейгана Томас Рід не опублікував свою книгу "At the Abyss: An Insider's History of the Cold War", в якій і були розкриті деталі надсучасного на той час акту агресії. Таким чином, вже наприкінці XX-го століття існувала небезпека для важливих складових державної інфраструктури зі сторони хакерів, що, зважаючи на стрімкий розвиток технологій суцільної автоматизації свідчить про підвищену небезпеку в наш час. Варто зазначити, що в 90-х роках відбулося ще принаймні п’ять подібного роду атак.

У 1998р. 12-річний хакер проникнув у комп’ютерну систему, що контролює паводкові шлюзи греблі Т. Рузвельта в Арізоні – під загрозою затоплення два міста з населенням 1 млн. чоловік. В тому ж році потужна кібератака на індійський Центр ядерних досліджень ім. Баба – пряма загроза виведення з ладу системи управління реактором.

На початку 2013 року невідомі хакери отримали доступ і опублікували персональні дані 40 тис. солдатів армії США та більше 2 млн. партійних функціонерів керуючої партії Республіки Корея; в тому ж році активісти хакерського угруповання WikiCrew за допомогою DDoS-атаки вивели з ладу офіційний сайт Агентства національної безпеки США [4, с. 124].

Проте «хрестоматійним» прикладом небезпеки для держави є атака , що відбулася у 2008 році Stuxnet. Зараз вже відомо, що це була скоординована атака ізраїльських і американських спецслужб,

спрямована на зрив ядерної програми Ірану. Вони створили хробака, який заразив комп'ютери, що керують урановими центрифугами на іранському заводі в Натанзі, в результаті чого ті почали працювати на повній швидкості, в той час як інженери на своїх моніторах спостерігали нормальний режим роботи. Це завдало фізичної шкоди всім урановим центрифугам на заводі. Шкоду завдану такої атакою можна порівняти з повноцінною військовою операцією, проте без жертв серед людей. Після цього випадку широкі кола громадськості дізналися про подібного роду небезпеку.

Загалом, розглянувши найвідоміші випадки кібератак за останні 25 років можна зробити висновок, що найчастіше об’єктами кібертероризму були системи функціонування та управління приватних та державних компаній у нафто-, газопереробних та металургійній сферах.

На жаль, Україна не залишилися осторонь прогресивих злочинних дій та зазнала декілька доволі потужних актів нападу на важливі об'єкти інфраструктури. 25 грудня 2015 року оператор електричних мереж області "Прикарпаттяобленерго" повідомив про незвичну аварію, яка на кілька годин знеструмила майже десять районів області. Відома міжнародна компанія ESET, яка займається кібербезпекою, повідомила, що аварія на "Прикарпаттяобленерго" стала результатом зовнішньої хакерської атаки. В офіційній заяві з посиланням на власне розслідування вказується, що атака стала частиною глобальної хакерської діяльності проти підприємств України та Польщі. "Інші енергетичні компанії України стали мішенню атаки кіберзлочинців в той самий час", - вважають в ESET. Спеціалісти ESET стверджують, що зловмисники використали вірус-троян Black Energy, який запустив спеціальну програму KillDisk, що не дозволяє завантажуватись комп’ютерам.

Проте найбільш масовою стала атака 27 червня 2017 року. Близько 12-ї години дня вірус невідомого походження атакував комп'ютерні системи сотень держвних установ, підприємств та організацій. Цей вірус отримав назву «вірус Petya». Тоді близько 30 банків, система інфраструктури (80% підприємств, підпорядкованих Міністерству інфраструктури), Кабмін, мобільні оператори, ЗМІ, підприємства енергетичної сфери були уражені, що призвело до тимчасового припинення їх роботи. На ліквідацію наслідків фахівці витратили понад тиждень.

Еволюція кібератак показує, що кібератаки сьогодення мають яскраво виражене політичне забарвлення і все більше проявляються у кібернетичному впливі на міждержавному рівні. Досліджуючи паралельно розвиток інформаційних та комунікаційних систем та технологій, можна відмітити, що основними причинами виникнення кібератак є, перш за все, різке збільшення продуктивності та одночасне здешевлення сучасних обчислювальних засобів, що робить їх загальнодоступними і значно розширює множину потенційних кіберзагроз, а також відсутність чітких кордонів у кіберпросторі, що нівелює відмінність між зовнішніми та внутрішніми джерелами загроз кібербезпеці держави. Крім того, кіберпростір дає можливість зловмисникам маніпулювати інформацією і її сприйняттям суспільством на власний розсуд, а також дозволяє реалізувати терористичні дії з безпрецедентною оперативністю і зробити завдання ідентифікації зловмисників дуже складним [4, с. 126].

Висновки та пропозиції. Важливо зауважити, що внаслідок вчинення кібертерористичних актів може бути викрадена інформація, яка є складовою державної таємниці, порушена система життєзабезпечення держави, що є загрозою для безпеки країни і за своєю суттю є порушенням загальноприйнятих принципів

міжнародного права. Таким чином, логічним висновком є те, що акти кібертероризму постають як реальна загроза не тільки для окремих комп'ютерних мереж будь-яких корпорацій чи приватних осіб, але і для інформаційних та комунікаційних систем цілої держави, а тому їх необхідно кваліфікувати як сучасні, навіть надсучасні, форми вчинення акту агресії, оскільки наслідки таких атак сміливо можна порівнювати з наслідками озброєного нападу.

Враховуючи вищевикладене можна запропонувати наступні шляхи протидії кібертероризму. По-перше, незважаючи на позитивні зрушення у сфері законодавчої роботи над проблемою кібертероризму, вітчизняне законодавство потребує активного удосконалення та подальшого забезпечення механізмів результативної реалізації розроблених положень.

По-друге, з огляду на транснаціональний характер вказаного злочину, доцільним є налагодження більш тісної співпраці національних правоохоронних органів з відповідними компетентними органами суб'єктів міжнародної спільноти для досягнення якомога ефективніших результатів боротьби.

По-третє, виходячи з того, що багато випадків ураження об'єктів критичної інфраструктури відбулися через відсутність належним чином підготовлених до масштабних кібератак професійних кадрів, необхідно періодично підвищувати кваліфікаційний рівень останніх. Крім того варто проводити заходи по ліквідації безграмотності населення у сфері ІКТ.

По-четверте, аналіз практики продемонстрував негативні аспекти суцільної комп'ютеризації та автоматизації промислового, банківського та соціального секторів державної інфраструктури, оскільки порушення їх роботи через масштабні кібератаки може призвести до непоправних наслідків у вигляді втрати не тільки

стратегічно важливої інформації, ресурсів та коштів, але і людських життів. А тому наразі актуальною є активна діяльність відповідних структур у напрямку розробки якісних та дієвих превентивних заходів протидії кібертероризму.

Література:

1. Конституція України: Закон України від 28.06.1996 №254к/96-ВР [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=254%EA%2F96-%E2%F0

2. Дубов Д. Підходи до формування тезаурусу у сфері кібербезпеки / Д. Дубов // Політичний менеджмент. – 2010. – № 4. – С. 19–30.

3. Myriam Dunn Cavelty. Cyberwar: concept, status quo, and limitations [Electronic resource] / Center for Security Studies (CSS), ETH Zurich. - Access mode: www.sta.ethz.ch

4. Гнатюк С. О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи / С. О. Гнатюк // Ukrainian Scientific Journal of Information Security, 2013. – Vol. 19/ – Issue-2.

5. Марченко А. В. Соціальні наслідки кібертерористичної небезпеки в епоху інформаційних технологій / Анна Марченко // Методологія, теорія та практика соціологічного аналізу сучасного суспільства. Збірник наукових праць Харківського національного університету імені В. Н. Каразіна. - 2008. - №1. - С. 355 – 360.

6. Конвенція про кіберзлочинність від 23.11.2001 р. [Електронний ресурс]. – Режим доступу http://zakon2.rada.gov.ua/laws/show/994_575/page.

7. Амелін О. Злочини у сфері інформаційних відносин в міжнародно-правових актах / Олександр Амелін. // Науковий часопис Національної академії прокуратури України. – 2016. – №2. – С. 1–9.

8. Маріц Д. О. Кібератака - війна майбутнього / Дар'я Олександрівна Маріц. // Інформація і право. – 2015. – С. 104–109.

9. Кримінальний кодекс України: від 05 квітня 2001 № 2341-III [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/4495-17

10. Проект Закону про внесення змін до Кримінального кодексу України щодо встановлення відповідальності за кібертероризм [Електронний ресурс]. – 2015. – Режим доступу до ресурсу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=56183.

References:

1. Konstytucija Ukrajiny: Zakon Ukrajiny vid 28.06.1996 #254k/96-VR [Elektronnyj resurs]. – Rezhym dostupu: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=254%EA%2F96-%E2%F0

2. Dubov D. Pidkhody do formuvannja tezaurusu u sferi kiberbezpeky / D. Dubov // Politychnyj menedzhment. – 2010. – № 4. – S. 19–30

3. Myriam Dunn Cavelty. Cyberwar: concept, status quo, and limitations [Electronic resource] / Center for Security Studies (CSS), ETH Zurich. - Access mode: www.sta.ethz.ch

4. Ghnatjuk S. O. Kiberteroryzm: istorija rozvytku, suchasni tendenciji ta kontrzakhody / S. O. Ghnatjuk // Ukrainian Scientific Journal of Information Security, 2013. – Vol. 19/ – Issue-2.

5. Marchenko A. V. Socialjni naslidky kiberterorystychnoji nebezpeky v epokhu informacijnykh tekhnologhij / Anna Marchenko // Metodologhija, teorija ta praktyka sociologhichnogho analizu suchasnogho suspiljstva. Zbirnyk naukovykh pracj Kharkivsjkogho nacionaljnogho universytetu imeni V. N. Karazina. - 2008. - № 1. - S. 355 – 360.

6. Konvencija pro kiberzlochynnistj vid 23.11.2001 r. [Elektronnyj resurs]. – Rezhym dostupu http://zakon2.rada.gov.ua/laws/show/994_575/page.

7. Amelin O. Zlochyny u sferi informacijnykh vidnosyn v mizhnarodno-pravovykh aktakh / Oleksandr Amelin. // Naukovyj chasopys Nacionaljnoji akademiji prokuratury Ukrajiny. – 2016. – № 2. – S. 1–9.

8. Maric D. O. Kiberataka - vijna majbutnjogho / Dar'ja Oleksandrivna Maric. // Informacija i pravo. – 2015. – S. 104–109.

9. Kryminaljnyj kodeks Ukrajiny: vid 05 kvitnja 2001 # 2341-III [Elektronnyj resurs]. – Rezhym dostupu: http://zakon2.rada.gov.ua/laws/show/4495-17

10. Proekt Zakonu pro vnesennja zmin do Kryminaljnogho kodeksu Ukrajiny shhodo vstanovlennja vidpovidaljnosti za kiberteroryzm [Elektronnyj resurs]. – 2015. – Rezhym dostupu do resursu: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=56183.