DOI: 10.26565/2220-8089-2021-39-15
УДК 004.056: 341(045)

Зінченко Олександра Ігорівна
магістр політології,
Харківський національний
університет імені В. Н. Каразіна,
майдан Свободи, 4, Харків, 61022,
alekca.98@ukr.net,
https://orcid.org/0000-0003-1623-957X

ЄВРОПЕЙСЬКА РЕГІОНАЛЬНА СИСТЕМА ПРОТИДІЇ КІБЕРТЕРОРИЗМУ: ПОЛІТИЧНІ, ІНСТИТУЦІЙНІ ТА ПРАВОВІ МЕХАНІЗМИ

Розглянуто сучасний етап розвитку кібертероризму в Європі. Прогресуванню цього явища сприяє мережа «Інтернет», яка має суттєвий вплив на всі сфери суспільного життя, надаючи величезну кількість інформації будь-якому користувачеві та заохочуючи висвітлення такої інформації та її поширення. Виявлено фактори, що ускладнюють процес протистояння кібертероризму, доведено, що сучасний кібертероризм є складовою частиною гібридних воєн і одним із дієвих важелів досягнення політичних цілей на міжнародній арені. Розкрито політичні, інституційні та правові механізми протидії кібертероризму в європейській регіональній системі кібербезпеки. Показуються способи та методи здійснення кібератак, а також можливості європейської регіональної системи протидії їм. Ця проблема висвітлюється на міжнародному рівні, вказуються документи, які передбачають методи протидії. Розглядається досвід передових країн у боротьбі із кібертероризмом. Зазначається, що особливістю кібертероризму є прагнення атакуючих зробити ефектний терористичний акт не тільки з небезпечними наслідками для інфраструктури та населення, а й зі значним суспільним резонансом. Цей фактор є особливо ускладнюючим для сучасної ситуації, адже соціальні мережі сьогодні дозволяють висвітлювати будь-яку інформацію у бажаний час, із бажаною метою та у бажаному ключі. Однак кіберзлочинці постійно вдосконалюють свою діяльність, з'являються все нові форми вчинення тероризму в мережі Інтернет, нові способи залякування населення, нові методи впливу на свідомість людей. Разом із тим і структура кіберзлочинності помітно різниться в різних країнах залежно від характеру і ступеня розвитку в них інформаційних технологій, поширення мережі Інтернет, використання електронних сервісів і електронної комерції. Зазначене зумовлює необхідність постійного оновлення, вдосконалення та коригування чинного антитерористичного національного, регіонального і міжнародного законодавства.

Ключові слова: *європейська регіональна систем, кібертероризм, причини розвитку кібертероризму, мережа Інтернет, система протидії кібертероризму, кібертероризм в європейських країнах.*

Зинченко Александра Игоревна
магистр политологии ,
Харьковский национальный
университет имени В. Н. Каразина,
площадь Свободы, 4, Харьков, 61022
alekca.98@ukr.net,
https://orcid.org/0000-0003-1623-957X

ЕВРОПЕЙСКАЯ РЕГИОНАЛЬНАЯ СИСТЕМА ПРОТИВОДЕЙСТВИЯ КИБЕРТЕРРОРИЗМУ: ПОЛИТИЧЕСКИЕ, ИНСТИТУЦИОНАЛЬНЫЕ И ПРАВОВЫЕ МЕХАНИЗМЫ

Рассмотрен современный этап развития кибертерроризма в Европе. Прогрессированию данного явления способствует сеть «Интернет», которая оказывает существенное влияние на все сферы общественной жизни, предоставляя огромное количество информации любому

пользователю и поощряя размещение такой информации и ее распространение. Выявлены факторы, затрудняющие процесс противостояния кибертерроризма, доказано, что современный кибертерроризм является составной частью гибридных войн и одним из действенных рычагов достижения политических целей на международной арене. Раскрыты политические, институциональные и правовые механизме противодействия кибертерроризму в европейской региональной системе кибербезопасности. Показываются способы и методы осуществления кибератак, а также возможности европейской региональной системы противодействия им. Данная проблема освещается на международном уровне, указываются документы, которые предусматривают методы противодействия. Рассматривается опыт передовых стран в борьбе с кибертерроризмом. Отмечается, что особенностью кибертерроризма является стремление атакующих сделать террористический акт не только с опасными последствиями для инфраструктуры и населения, но и с значительным общественным резонансом. Данный фактор является особенно осложняющим для современной ситуации, ведь социальные сети сегодня позволяют освещать любую информацию в желаемое время, с желаемой целью и в желаемом ключе. Однако киберпреступники постоянно совершенствуют свою деятельность, появляются все новые формы совершения терроризма в сети Интернет, новые способы запугивания населения, новые методы воздействия на сознание людей. Вместе с тем и структура киберпреступности заметно различается в разных странах в зависимости от характера и степени развития в них информационных технологий, распространения сети Интернет, использование электронных сервисов и электронной коммерции. Указанное обусловливает необходимость постоянного обновления, совершенствования и корректировки действующего антитеррористического национального, регионального и международного законодательства.

Ключевые слова: *европейская региональная систем, кибертерроризм, причины развития кибертерроризма, сеть Интернет, система противодействия кибертерроризма, кибертерроризм в европейских странах.*

Oleksandra Zinchenko
Master of Political Science
V. N. Karazin Kharkiv National University,
4, Svoboda Sq., Kharkiv, 61022, Ukraine,
alekca.98@ukr.net,
https://orcid.org/0000-0003-1623-957X

EUROPEAN REGIONAL SYSTEM FOR COMBATING CYBERTERRORISM: POLITICAL, INSTITUTIONAL AND LEGAL MECHANISMS

The current stage of development of cyberterrorism in Europe is considered. The progression of this phenomenon is facilitated by the Internet, which has a significant impact on all spheres of public life, providing a huge amount of information to any user and encouraging the placement of such information and its dissemination. The factors that complicate the process of countering cyberterrorism are identified; it is proved that modern cyberterrorism is an integral part of hybrid wars and one of the effective levers of achieving political goals in the international arena. The political, institutional and legal mechanisms of countering cyberterrorism in the European regional cybersecurity system are revealed. The ways and methods of carrying out cyberattacks, as well as the capabilities of the European regional system of countering them are shown. This problem is highlighted at the international level, documents are indicated that provide methods of counteraction. The experience of advanced countries in the fight against cyberterrorism is examined. It is noted that a feature of cyberterrorism is the desire of the attackers to commit a terrorist act not only with dangerous consequences for the infrastructure and the population, but also with significant public resonance. This factor is especially complicating for the current situation, because social networks today allow you to cover any information at the desired time, with the desired goal and in the desired manner. However, cybercriminals are constantly improving their activities; there are new forms of terrorism on the Internet, new ways of intimidating the population, new methods of influencing the minds of people. At the same time, the structure of cybercrime differs significantly in different countries depending on the nature and degree of development of information technologies

in them, the spread of the Internet, the use of electronic services and e-commerce. The aforementioned necessitates constant updating, improvement and adjustment of the existing anti-terrorist national, regional and international legislation.

Keywords: *European regional systems, cyberterrorism, reasons for the development of cyberterrorism, Internet, anti-cyberterrorism system, cyberterrorism in European countries.*

Кібертероризм визнається проблемою не окремої держави, а всього світового співтовариства в цілому. Протидія кібертероризму в розвинених країнах є однією з найважливіших завдань, що забезпечують внутрішню безпеку держави. 10 грудня 1934 року Рада Ліги Націй, попередниці ООН, прийняла рішення, в якому говорилося, що «на всіх державах лежить обов'язок не заохочувати і не терпіти на своїй території жодної терористичної діяльності, яка має політичну мету ... Кожна держава не повинна нічим нехтувати у справі попередження і репресії терористичних актів і надання в цих цілях допомоги тим урядам, які за нею звернуться» (Лебедєв 2008: 12). У 1937 р Ліга Націй намагалася дати своє визначення терористичного акту як злочинній дії проти держави з метою викликати страх у певних людей або групи населення.

Форми і методи боротьби з кібертероризмом досить детально регламентовані в законодавстві більшості зарубіжних країн (США, КНР, Великобританії та ін.). Однак кіберзлочинці постійно вдосконалюють свою діяльність, з'являються все нові форми вчинення тероризму в мережі Інтернет, нові способи залякування населення, нові методи впливу на свідомість людей. Разом із тим і структура кіберзлочинності помітно різниться в різних країнах залежно від характеру і ступеня розвитку в них інформаційних технологій, поширення мережі Інтернет, використання електронних сервісів і електронної комерції. Зазначене зумовлює необхідність постійного оновлення, вдосконалення та коригування чинного антитерористичного національного і міжнародного законодавства.

Сьогодні на міжнародному рівні з метою протидії кібертероризму прийняті Декларація про заходи щодо ліквідації міжнародного тероризму (Декларація про заходи ліквідації міжнародного тероризму 1994), Європейська Конвенція про боротьбу з тероризмом 1977 р. (Європейська конвенція про боротьбу з тероризмом (ETS N 90) 1977), які покликані забезпечити безпеку міжнародної спільноти і невідворотність кримінального переслідування осіб, які вчинили терористичні акти.

Значна роль у протидії кібертероризму на міжнародному рівні відводиться Конвенції Ради Європи про кіберзлочинність, прийнятої в 2001 р., де визначено поняття кіберзлочинів, під яке підпадають «правопорушення, вчинені в інформаційному середовищі або проти інформаційних ресурсів, або за допомогою інформаційних засобів, а також детально описані проблеми взаємодії правоохоронних органів окремих європейських держав у ситуації, коли злочинець і жертва знаходяться в різних країнах і підпорядковуються різним законодавствам» (Конвенція про кіберзлочинність 2001). Складність протистояння кібертероризму зумовлена низкою факторів, до яких варто віднести:

1) простір Інтернету вкрай широкий – передбачити характер інформації, час, місце, автора і його мету практично неможливо. Сучасні технології дозволяють лише частково відстежити першочергову інформацію. Однак ряд програмних засобів, доступних звичайному користувачеві, дозволяють обійти і ці технології;

2) терористи можуть використовувати для завантаження своїх матеріалів ресурси, які не потребують реєстрування даних, і, крім того, популяризувати посилання на них через соціальні мережі. В цьому випадку з'являється маса користувачів, які, переглядаючи новинні стрічки, випадково отримують доступ до того чи іншого матеріалу;

3) ймовірність того, що опублікований де-небудь матеріал відразу ж виявлять і видалять вкрай мала;

4) єдиної законодавчої бази, що регулює вміст контенту Інтернету, поки не існує, хоча спроби її створення робилися вже не раз.

Крім використання Інтернету для початку кібератаки проти національних держав, терористичні організації можуть використовувати Інтернет для проведення хактивізму.

Протягом багатьох років різні відомства, подібні Агентству передових оборонних дослідних проектів (DARPA) і Агентству національної безпеки (NSA), набирають талановитих фахівців під час таких заходів,

як серія конференцій з комп'ютерної безпеки Black Hat і з'їзд хакерів Def Con. У 2011 році DARPA оголосило про запуск нової програми Cyber Fast Track (CFT), створеної колишнім хакером, менеджером проектів в DARPA. Вона була спрямована на поглиблення і впорядкування співпраці з цими спільнотами. В рамках CFT агентство залучає окремих фахівців і невеликі компанії до роботи над короткостроковими цільовими проектами у сфері мережевої безпеки.

Ця ініціатива спрямована на роботу з дрібними гравцями і її відрізняє можливість швидко схвалювати виділення грантів. Протягом перших двох місяців після запуску програми DARPA схвалив висновок восьми контрактів – іншими словами, вона працює зі швидкістю світла порівняно з нормальними для державних відомств темпами. Це дозволяє досвідченим фахівцям, які інакше навряд чи погодилися б працювати на уряд, внести свій внесок у важливу справу зміцнення кібербезпеки, причому легко і в ті тимчасові рамки, які відповідають терміновості завдання. Програма CFT стала однією з ознак зсуву агентства у бік демократичних інновацій з використанням краудсорсингу.

Також на міжнародному рівні діє Конвенція про кіберзлочинність, підписана державами-членами Ради Європи в Будапешті 23 листопада 2001 року (Конвенція про кіберзлочинність 2001). Цей документ встановлює порядок взаємодії країн у боротьбі зі злочинами проти конфіденційності, цілісності і доступності комп'ютерних даних і систем, а також всіма видами правопорушень, пов'язаних з використанням комп'ютерних засобів, зі змістом даних і з порушенням авторських та суміжних прав. Багато заходів, передбачених Конвенцією, спрямовані на недопущення несанкціонованого втручання в роботу комп'ютерних систем, і можуть виступити своєрідним заслоном на шляху до здійснення терористичних злочинів.

У 2020 році всі країни і великі організації надавали великого значення боротьбі з кібертероризмом. Сучасний кібертероризм є складовою частиною гібридних воєн і одним із дієвих важелів досягнення політичних цілей на міжнародній арені. Особливістю кібертероризму є прагнення атакуючих зробити ефектний терористичний акт, який би мав не тільки небезпечні наслідки для інфраструктури та населення, а й набув широкого суспільного розголосу та міжнародного резонансу.

Між тим, хочемо зазначити, що уряди більшості зарубіжних держав стурбовані зростаючим рівнем кіберзагроз та комп'ютерної злочинності, в зв'язку з чим приймають спеціальні заходи з їхньої нейтралізації. Можна констатувати, що вже сьогодні на міжнародному рівні напрацьовано певний позитивний досвід боротьби з кібертероризмом. Так, наприклад, у Великій Британії вступив в дію закон про тероризм, покликаний посилити боротьбу з різними угрупованнями, які використовують територію Сполученого Королівства для своєї діяльності. Відповідно до нього, в разі злому хакерами комп'ютерної системи, що забезпечує національну безпеку країни, а також спроб з їхнього боку будь-яким чином впливати на державні структури або загрожувати суспільству, вони можуть бути звинувачені в тероризмі з усіма наслідками, що випливають з цього.

Важливе значення в питаннях протидії кібертероризму відводиться міжнародному співробітництву, яке включає діяльність держав з різних напрямків:

1) визнання небезпеки певних кримінальних діянь і необхідності застосування спільних заходів для їх припинення;

2) допомога в розшуку правопорушників, які переховуються на чужій території, і передачі їх зацікавленій державі;

3) допомога в отриманні необхідних матеріалів з кримінальної справи;

4) вивчення проблем злочинності і боротьби з нею, питань пенітенціарної системи;

5) надання практичної допомоги окремим державам у розв'язанні проблем злочинності;

6) обмін необхідною для боротьби з кібертероризмом інформацією.

Варто зауважити, що при ООН в рамках цільових груп здійснення контртерористичних заходів діє Робоча група, яка займається виявленням зацікавлених сторін і партнерів і об'єднанням їх зусиль для боротьби зі зловживаннями Інтернетом у терористичних цілях. До таких зловживань входить і використання мережі з метою радикалізації, вербування, підготовки, оперативного планування, збору коштів та інших антигуманних цілей. У співпраці з державами-членами Робоча група вивчає методи використання терористами мережі Інтернет, визначає масштаби створюваної цим загрози і вивчає можливі заходи із протидії цій загрозі на національному,

регіональному та глобальному рівнях, включаючи визначення тієї ролі, яку може відігравати у цій сфері ООН, без шкоди для прав людини, основних цінностей і відкритого характеру самого Інтернету. Популяризація великих європейських і внутрішньодержавних Інтернет-сайтів викликає інтерес і стурбованість з сторін більшості сучасних держав і органів, компетентних у сфері безпеки.

Аналізуючи європейське законодавство щодо протидії кібертероризму, П.М. Кобець резюмує, що цей досвід може бути корисний для вдосконалення національного законодавства, в частині окремих законодавчо-технічних прийомів, використовуваних парламентами цих країн, а також в частині про наділення особливою компетенцією органів, що займаються розслідуванням терористичних злочинів, про права жертв терористичних актів на матеріальну компенсацію за заподіяну їм шкоду, а також про можливі заходи щодо попередження терористичних актів, що в сукупності, як показує досвід, може відігравати певну позитивну роль (Кобець 2018: 32).

Однак досвід не всіх, навіть європейських, держав можливо імплементувати у вітчизняне законодавство в частині законодавчо-технічних прийомів, що пояснюється не тільки відмінністю в політичному устрої, культурних традиціях, але й у приналежності окремих держав, таких, наприклад, як Великобританія, до англосаксонської системи права. Незважаючи на це, ми повинні ставити перед собою завдання з об'єднання зусиль у сфері протидії тероризму і екстремізму на всьому європейському просторі.

Отже, можемо сказати, що нині стає все більш очевидним, що загроза кібертероризму є актуальною проблемою сьогодення глобального характеру, причому вона буде неухильно наростати в міру розвитку й поширення інформаційних технологій. Тому ефективне європейське співробітництво у сфері попередження і ліквідації наслідків кібератак на державні, життєво важливі, екологічно вразливі та інші об'єкти набуває все більшого значення.

Між тим, у 2020 році всі країни і великі організації надавали великого значення боротьбі з кібертероризмом. Із зростанням напруженості в світі загроза кібертероризму завжди буде присутня, більш того, в ряді країн вона може бути однією зі складових державної політики. У країнах, для яких проблема кіберзлочинності є особливо гострою, приймаються не тільки технічні, а й законодавчі заходи, спрямовані на протидію кіберзлочинності і кібертероризму. Оскільки методи, що застосовуються кібертерористами, багато в чому збігаються з методами, якими користуються кіберзлочинці, то і дії керівників компаній, організацій повинні бути спрямовані на збереження безперервності бізнесу і дотримання заходів інформаційної безпеки.

ЛІТЕРАТУРА

Лебедєв, А.С. 2008. "Роль ООН у боротьбі з тероризмом", *Оглядач-OBSERVER* 5: 12-47.

Декларація про заходи ліквідації міжнародного тероризму від 09.12.1994. URL: https://zakon.rada.gov.ua/laws/show/995_502#Text.

Європейська конвенція про боротьбу з тероризмом (ETS N 90) від 27.01.1977. URL: https://zakon.rada.gov.ua/laws/show/994_331#Text

Конвенція про кіберзлочинність від 23.11.2001. *Рада Європи*. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text.

Кобець, П.М. 2018. "Законодавчі основи попередження тероризму в європейських країнах", *Міжнародне публічне і приватне право* 20-52.

REFERENCES

Lebedyev, A. S. 2018. "Rol′ OON u borot′bi z teroryzmom (The role of the UN in the fight against terrorism)", *Ohlyadach-OBSERVER*. 5: 12-47 (in Russian).

Deklaratsiya pro pro zakhody likvidatsiyi mizhnarodnoho teroryzmu vid (Declaration on measures to eliminate international terrorism from) 09.12.1994. URL: https://zakon.rada.gov.ua/laws/show/995_502#Text. (in Ukrainian).

Yevropeys′kakonventsiya pro borot′bu z teroryzmom (ETS N 90) vid 27.01.1977 (European Convention on the Suppression of Terrorism (ETS No. 90) of 27 January 1977). URL: https://zakon.rada.gov.ua/laws/show/994_331#Text (in Ukrainian).

Konventsiya pro kiberzlochynnist′ vid 23.11.2001 (Convention on Cybercrime of November 23, 2001). *Rada Yevropy*. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (in Ukrainian).

Kobets′, P.M. 2018. "Zakonodavchi osnovy poperedzhennya teroryzmu v yevropeys′kykh krayinakh (Legislative bases of terrorism prevention in European countries)", *Mizhnarodne publichne i pryvatne pravo*. 20-52 (in Ukrainian).