in the form of signals, signs, sounds, moving or still images or otherwise» [6].

So we see that there are different definitions of information in science and law. And first of all it is caused by different spheres of research and aims of these documents. And at the same time we have non similar and not unified use of the term information and related concepts. These concepts have to be differentiated more strictly.

References:

1. Lewis & Short Latin Dictionary, 1879. URL: http://folio2.furman.edu/lewis-short/

2. Dictionary of Medieval Latin from British Sources. URL: https://logeion.uchicago.edu/lexidium

3. Merriam-Webster Dictionary. URL: https://www.merriam-webster.com

4. Cambridge International AS & A Level Information Technology. 9626. For examination from 2017. Topic support guide. Cambridge International Examinations 2015. Version 1. URL: https://www.cambridgeinternational.org/images/285017-data-information-and-knowledge.pdf

5. On Information: Law of Ukraine on October 2, 1992. URL: https://zakon.rada.gov.ua/laws/show/2657–12#Text

6. On Telecommunications: Law of Ukraine on November 18, 2003. URL: https://zakon.rada.gov.ua/laws/show/1280–15#Text

Малюта Владислав Васильович,
Язаджи Вікторія Сергіївна
здобувачі вищої освіти факультету цивільної
та господарської юстиції
Національного університету «Одеська юридична академія»

ЩОДО ЄВРОПЕЙСЬКОГО СПІВРОБІТНИЦТВА У ВИДАЧІ ПРАВОПОРУШНИКІВ, ПРИЧЕТНИХ ДО МІЖНАРОДНОГО КІБЕРТЕРОРИЗМУ

Тривалий час проблема кібертероризму розглядалася різними вченими багатьох країн та привертала велику увагу в контексті всеосяжної боротьби з тероризмом на початку XXI сторіччя. З розвитком новітніх технологій, кіберзлочинність привертає все більше уваги у світової спільноти. Не

оминув технічний прогрес і терористичну діяльність. Зараз терористична діяльність все більше переходить у комп'ютерну площину, терористи стають більш анонімними та невловимими. Як правило, кібертеракти мають на меті повне знищення або часткове пошкодження інфраструктури у інтернет-просторі. Практична потреба у розгляді даної проблематики полягає у чисельних терористичних актах з використанням комп'ютерних технологій. Так, наприклад, після вірусу Petya, який пошкодив бізнес в Україні та економіку України в цілому, ми бачимо розвиток охорони та захисту цієї галузі у країні. На світовому рівні слід згадати приклад, який нещодавно сколихнув весь інтернет: імовірно внаслідок хакерських атак, які спричинили збої роботи компанії Facebook, компанія втратила близько 5 % вартості акцій та суспільну довіру. Враховуючи вищезазначене, потреба у міжнародному визнанні кібертероризму є дуже гострою, а тема дослідження актуальною.

Попри широке доктринальне забезпечення кримінально-правового інституту кібертероризму правотворчість та міжнародне співробітництво обходить увагою це питання. У спеціальній доповіді «Кібертероризм – наскільки реальна загроза» Габріель Вейман надає наступне визначення. Кібертероризм – це конвергенція кіберпростору та тероризму. Він включає у себе протиправні атаки та загрози атак на комп'ютери, мережі та інформацію яка зберігається у комп'ютерах, коли це робиться з метою залякування чи примусу уряду, чи до досягнення політичних або соціальних цілей. Крім того, щоб кваліфікувати атаку як кібертероризм, напад має призвести до насильства проти людей або майна або, принаймні, викликати достатньо шкоди, щоб викликати страх. Прикладами можуть бути напади, які призводять до смерті або тілесних ушкоджень, вибухів або серйозних економічних збитків. Серйозні атаки на об'єкти критичної інфраструктури можуть бути актами кібертероризму, залежно від їх впливу на громадськість [1].

Кібертероризм охоплює такі дії як пошкодження та зміна даних, зміна або виведення з ладу комп'ютерних систем, незаконний доступ до управління системою з подальшою публікацією загрозливих повідомлень, закликів чи попереджень

тощо. Співпраці у протидії таким видам злочинів присвячена конвенція. Як зазначено у ст.4 та 5 Конвенції про кіберзлочинність Ради Європи від 23.11.2001, кожна сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності за законодавства за навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації, за навмисне серйозне перешкоджання функціонуванню комп'ютерної системи шляхом введення, передачі, пошкодження, знищення, погіршення, заміни або приховування комп'ютерних даних без права на це та відповідно до внутрішнього законодавства [2].

Міжнародна співпраця у протидії таким видам злочинів полягає, зокрема, у затриманні злочинців. Відповідно до п. 2 ст. 2 Рамкового рішення про європейський ордер на арешт та процедури передачі правопорушників між державами-членами (2002/584/ЮВС), як тероризм так і комп'ютерні злочини є підставою для видання європейського ордеру на арешт [3].

Однак віднесення кібертероризму не до тероризму, а до комп'ютерних злочинів тягне перешкоди під час видачі кібертерористів. Оскільки на кібертероризм не поширюється міжнародно-правовий режим тероризму, до нього не застосовуються заходи протидії тероризму, які є більш ефективними ніж звичайна співпраця. Відповідно до ч. 5 ст. 24 Конвенції про кіберзлочинність Ради Європи від 23.11.2001 року екстрадиція здійснюється в порядку визначеному законодавством країни, яка видає осудну особу. Також має місце відмови в екстрадиції Стороною, яку запитують про екстрадицію, відповідно до певних законодавчих підстав.

Відповідно до ст.2 Європейської конвенції про взаємну допомогу у кримінальних справах Ради Європи від 20.04.1959, у допомозі може бути відмовлено Стороною, яка надає запит про видачу, у разі якщо правопорушення є політичним, податковим або може певним чином зашкодити суверенітету, безпеці, громадському порядку або іншим суттєвим інтересам країни [5].

Такі положення дозволяють перетворити кібертероризм у кіберзброю – знаряддя ведення гібридної війни. Якщо держава бере під протекторат кібертерористичну організацію

або самостійно створює таку організації на базі власних спецслужб, вона, будучи заінтересованою у захисті кібертерористів, може створювати перешкоди під час їхнього міжнародного кримінального переслідування.

Подолати цей механізм зловживання можна шляхом поширення на кібертероризм правового режиму тероризму. Відповідно до ст.4 Європейської конвенції про боротьбу з тероризмом (ETS N 90) Ради Європи від 27.01.1977 № ETSN90 видача особи передається навіть якщо така видача не передбачена міжнародними угодами.

Визнання кібертероризму тероризмом у загальному розумінні та зазначення цього явища у переліку, наведеному у статті 1 Конвенції, унеможливить поширення на нього режиму політичного злочину, дозволить застосовувати статтю 8 Конвенції для отримання міжнародної допомоги у переслідуванні кібертерористів, а також знизить обсяг можливих штучних перешкод у видачі цих злочинців.

Така прогалина створює широкий інструментарій зловживання, яким користуються кібертерористи та їх покровителі, адже відповідно до ст. 3 Європейської конвенції про видачу правопорушників Ради Європи від 13.12.1957, видача особи не здійснюється, якщо злочин, у зв'язку з яким її запитують, розглядається вже державою, до якої надіслано запит, як злочин, що є політичним. Як вбачається з цього положення, кібертероризм може підпадати під дану категорію справ, та відповідно, особи, які здійснили дане правопорушення, можуть буди не видані [6].

Оскільки міжнародний кібертероризм не є тероризмом у розумінні Європейської конвенції про боротьбу з тероризмом, але має спільну правову природу та ступінь впливу на суспільство, у рамках європейської співдружності слід доповнити конвенцію про боротьбу з тероризмом додатковим протоколом про боротьбу з кібертероризмом.

Джерела:

1. Gabriel Weimann, 'Cyberterrorism – How real is the threat', United States Institute of Peace, Special Report 119, December 2004. URL: https://www.usip.org/sites/default/files/sr119.pdf

2. Конвенція про кіберзлочинність : Конвенція; Рада Європи від 23.11.2001 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/994_575 (дата звернення: 18.11.2021).

3. Рамкове Рішення Ради від 13 червня 2002 року про європейський ордер на арешт та процедури передачі правопорушників між державами-членами (2002/584/ЮВС) : Рішення; Рада Європи від 13.06.2002 № 2002/584/ЮВС // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/994_b17 (дата звернення: 18.11.2021).

4. Європейська конвенція про боротьбу з тероризмом (ETS N 90) : Конвенція; Рада Європи від 27.01.1977 № ETSN90 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/994_331 (дата звернення: 18.11.2021).

5. Європейська конвенція про взаємну допомогу у кримінальних справах : Конвенція; Рада Європи від 20.04.1959 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/995_036 (дата звернення: 18.11.2021).

6. Європейська конвенція про видачу правопорушників : Конвенція; Рада Європи від 13.12.1957 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/995_033 (дата звернення: 18.11.2021).

Науковий керівник – к.ю.н., доцент кафедри міжнародного та європейського права Національного університету «Одеська юридична академія» Гриб А. М.

Марценко Наталія Степанівна
к.ю.н., доцент кафедри міжнародного права та міграційної політики Західноукраїнського національного університету
Котис Вікторія Ярославівна
здобувач вищої освіти юридичниого факультету Західноукраїнського національного університету

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ПРАВОСУДДІ СПОЛУЧЕНИХ ШТАТІВ АМЕРИКИ

Інтеграція України у європейський та світовий простір вимагає від нашої держави не лише дотримуватися загальновизнаних правових стандартів, а і досліджувати та впроваджувати нові, ще недостатньо вивчені напрямки, одним із яких