

3. Fraser-Thill R. Definition of Identity. – [Електронний ресурс]. – Режим доступу: <http://tweenparenting.about.com/od/behaviordiscipline/a/Definition-of-Identity.htm>

4. Медведєва М. О. Міжнародне право та біотехнології / Київський національний університет імені Тараса Шевченка, Інститут міжнародних відносин. – К.: Видавничий дім «Промені», 2006. – 256 с.

5. Бахин С. В. Научно-технический прогресс в области медицины и международно-правовая защита прав человека: Автореф. дис. ... канд. юрид. наук: 12.00.10 / Ленинградский гос. ун-т. – Ленинград, 1990. – 21 с.

УДК 341(043.2): 004.056

Яцишин М. Ю., викладач,
Національний авіаційний університет, м. Київ, Україна,
Тимченко Л. О., к.ю.н., доцент,
Національний університет ДПС України,
м. Ірпінь, Україна

ПРОБЛЕМА ВИЗНАЧЕННЯ ПОНЯТТЯ «КІБЕРЗЛОЧИННІСТЬ» У МІЖНАРОДНО-ПРАВОВІЙ ПРАКТИЦІ

Дослідження та узагальнення поняття «кіберзлочин» є важливим кроком на шляху до формування концепції «кіберзлочинності» у міжнародному праві, створення загальних підходів до криміналізації такого роду протиправних діянь, а також боротьби із ними. В умовах відсутності єдності та одноманітності правового регулювання зазначеної сфери, що, перш за все, проявляється в застосуванні різної термінології та категоріально-понятійного апарату, сучасне міжнародно-правове поле не можна вважати ефективним.

Міжнародне співтовариство неодноразово висловлювало занепокоєння тим, що новітні технології потенційно можуть використовуватися в цілях, несумісних із завданнями щодо забезпечення міжнародної стабільності та безпеки, і в змозі негативно впливати на цілісність інфраструктури держав, порушуючи їх безпеку як в цивільній, так і у військовій сферах.

У Женевській Декларації принципів «Побудова інформаційного суспільства: глобальна задача в новому тисячолітті» прямо не застосовано термін «кіберзлочинність», однак із її положень випливає, що боротьба із кіберзлочинністю є важливою складовою глобальної культури кібербезпеки.

Жоден чинний універсальний міжнародно-правовий акт не надає визначення кіберзлочинності. Більш того, експерти, що входять до групи Усестороннього дослідження проблеми кіберзлочинності та відповідних заходів зі сторони держав-членів міжнародного співтовариства і приватного сектору, наголошують на відсутності необхідності формування тако-

го єдиного узагальнюючого поняття, що на наше переконання, не є достатньо обґрунтованим.

Важливим кроком у згаданій сфері міжнародно-правового регулювання стало прийняття регіональних договорів, які, водночас, містять різний понятійно-категоріальний апарат. Дослідивши положення Конвенції Ради Європи про кіберзлочинність 2001 р. [1], Конвенції про боротьбу із злочинами у сфері інформаційних технологій Ліги арабських держав 2010 р. [2], Угоди про співробітництво держав-членів Співдружності Незалежних Держав у боротьбі із злочинністю в сфері комп'ютерної інформації 2001 р. [3], Угоди про співробітництво в сфері забезпечення міжнародної інформаційної безпеки Шанхайської організації співробітництва 2009 р. [4], приходимо до висновку, що їх сфера дії не є ідентичною.

Водночас, порівнюючи визначення застосованих понять за контекстом, можна стверджувати, що усі вони: є видами протиправних / кримінально караних діянь, тобто злочинів; вказують на електронну / віртуальну сферу, в якій здійснюються; відображають зв'язок правопорушення із «комп'ютерною складовою» (системами, мережами, даними, комп'ютерною інформацією тощо).

Отже, досліджувані поняття є схожими за контекстом, оскільки для їх визначення використовуються синонімічні та однопорядкові категорії. Поняття, включені до Конвенції РЄ, Конвенції ЛАД, Угоди СНД та Угоди ШОС відображають результати регіональної уніфікації національних законодавств, а тому, на нашу думку, саме на їх основі потрібно сформулювати універсальне визначення поняття, яке б відображало суть явища «кіберзлочинності».

Як наслідок розвитку міжнародної співпраці у сфері боротьби із кіберзлочинністю повинен бути розроблений і прийнятий під егідою ООН багатосторонній універсальний міжнародно-правовий акт – Конвенція проти кіберзлочинності, в основу якого повинно лягти поняття «кіберзлочинність». На нашу думку, цей термін є більш обґрунтованим, аніж інші, оскільки:

- по-перше, саме цей термін витікає із більш широких понять «кіберпростір» та «кібербезпека», які вже містяться у багатьох міжнародно-правових актах;

- по-друге, він вдало відображає зв'язок понять «кібератака» – «кіберзлочинність» – «кібертероризм»;

- по-третє, частка «кібер» охоплює практично всі особливості окресленої сфери, тобто: пов'язує відповідні протиправні діяння із технологічними засобами – комп'ютерами, їх системами та мережами в цілому, а не окремими їх видами; вказує на віртуальну сферу, в якій і здійснюється кримінально карана поведінка.

Підсумовуючи вищезазначене, пропонуємо наступне визначення: «кіберзлочинність – протиправні, кримінально карані діяння, що здійснюються за допомогою чи проти комп'ютерних даних, комп'ютерів, їх систем та мереж». В рамках та у відповідності до універсальної концепції кіберзлочинності повинно бути розроблено і концепцію стратегії реалізації державної політики щодо боротьби із кіберзлочинністю в Україні.

Література

1. Конвенція Ради Європи про кіберзлочинність від 21.11.2001 р. / [Електронний ресурс]–Режим доступу: http://zakon4.rada.gov.ua/laws/show/994_575
2. Arab Convention on Combating Information Technology Offences 21.12.2010 / [Електронний ресурс] – Режим доступу: <http://cms.unov.org/DocumentRepositoryIndexer/GetDocInOriginalFormat.drsx?DocID=3dbe778b-7b3a-4af0-95ce-a8bbd1ecd6dd>.
3. Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 01.06.2001 г. / [Електронний ресурс] – Режим доступу: http://zakon4.rada.gov.ua/laws/show/997_353
4. Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности от 16.06.2009 г. / [Електронний ресурс] – Режим доступу: http://base.spinform.ru/show_doc.fwx?rgn=28340

UDC 343.2 (043.2)

Zajac D., PhD Student,
Jagiellonian University, Poland

THE REQUIREMENT OF DOUBLE CRIMINALITY FROM THE VIEW OF THE PRINCIPLE OF CITIZENSHIP

1. Introduction. The requirement of double criminality is the law institution, which regulates the issues of validity of the criminal code outside the borders of a country. In accordance with abovementioned rule it is impossible to prosecute for acts committed abroad in a case, when those acts are not prohibited according to the law being in force in the place of acting. This directive is in practice far-reaching restricted, in particular because of the provisions contained in international agreements.

2. The requirement of double criminality in Polish and Ukrainian criminal law. In Polish law the requirement of double criminality is precised in the article 111 of the Criminal Code [1. p. 1132]. It is an essential condition of prosecution of crimes committed abroad – by citizens and foreigners. The exception is prosecution based