

**Сергій Марків,**

викладач кафедри кримінального права  
та процесу Тернопільського національного  
економічного університету

## ІСТОРИКО-ПРАВОВИЙ АСПЕКТ КІБЕРТЕРОРИЗМУ

*Наголошено, що кібертероризм є похідним від більш широкого загального поняття «тероризм» і полягає у глобальній загрозі інформаційній безпеці суспільства. Зазначено, що єдиної позиції щодо визначення «кібертероризму» немає, і науковці дотепер дискутують з приводу цієї проблематики. Зазначено, що в Україні на сьогодні не розроблено нормативно-правових актів, що регулюють такий вид злочинності. Вказано, що головною зброєю у боротьбі з цією загрозою залишається законодавство, яке потребує подальшого вдосконалення. З огляду на сучасні реалії життя все більш поширеного розвитку набуває науково-технічний прогрес, поза межами якого не залишаються й комп'ютерні інновації.*

**Ключові слова:** кібертероризм, кіберзлочин, інформаційні технології, інформаційна безпека, тероризм.

**Марків С.**

### **Историко-правовой аспект кибертерроризма**

*Подчеркнуто, что кибертерроризм является производным от более широкого общего понятия «терроризм» и заключается в глобальной угрозе информационной безопасности общества. Отмечено, что единой позиции по определению «кибертерроризма» нет, и ученые до сих пор спорят по поводу этой проблематике. В Украине на сегодня не разработано нормативно-правовых актов, которые регулируют такой вид преступности. Указано что главным оружием в борьбе с этой угрозой остается законодательство, которое требует дальнейшего совершенствования. Учитывая современные реалии жизни все более распространенного развития приобретает научно-технический прогресс, за пределами которого остаются и компьютерные инновации.*

**Ключевые слова:** кибертерроризм, киберпреступность, информационные технологии, информационная безопасность, терроризм.

**Markiv S.**

### **Historical and legal aspect of cyberterrorism**

*Cyberterrorism is derived from the broader general concept of “terrorism” and is a global threat to information security community. Immediately it should be noted that a common position on the definition of “cyber terrorism” is not, and scientists are still debating on this issue. In Ukraine, currently not developed regulations governing this type of crime. But the main weapon in the fight against this threat is legislation needs further improvement. Given the current realities of the increasingly widespread development takes technological progress, beyond which no remains and computer innovation.*

**Keywords:** cyberterrorism, cybercrime, information technology, information security, terrorism.

**Постановка проблеми.** На сьогодні все більшого значення в межах становлення міжнародно-правових відносин та формування світового суспільства набуває розвиток науково-технічного прогресу, складовим елементом якого є високі комп'ютерні технології. Поява технологічних новел у різних сферах нашого життя стає не лише запорукою високоякісної продуктивності праці та швидкої поіформованості людини, але своїм наслідком породжує появу негативного та несанкціонованого втручання у їх роботу, що призводить до кібертероризму.

**Аналіз останніх досліджень і публікацій.** Дослідників кібертероризму та його історико-правових аспектів ми зустрічаємо як на сторінках вітчизняної літератури, так і у працях зарубіжних науковців. Серед вітчизняних видається важливим згадати наступних: С. О. Гнатюк, В. П. Харченко, О. Г. Корченко, Є. В. Паціра, С. В. Казмірчук, В. Л. Бурячок, М. А. Погорецький, С. В. Мельник, Д. Б. Дубов, Р. М. Кравченко, та ін. До зарубіжних вчених, які дискутують над цією темою можемо, вважати: В. А. Мазурова, Ю. В. Гаврилова, М. М. Безрукова, В. Б. Вехова, С. Гриняєва, Е. О. Роговського, Е. Конрі-Мюррея, Рональда Л-Діка та ін.

**Цілями статті** є аналіз основних аспектів становлення та розвитку кібертероризму, пошук шляхів боротьби із ним і методів його попередження.

**Виклад основного матеріалу дослідження.** Історія сучасного кібертероризму має давню історію і сягає своїм початком у далеке минуле. Кібертероризм є похідним від більш широкого загального поняття «тероризму» і полягає у глобальній загрозі інформаційній безпеці суспільства. Відразу слід зазначити, що

єдиної позиції щодо визначення «кібертероризму» немає, науковці дотепер дискутують з приводу цієї проблематики. Єдиним є об'єкт посягання, на який відбувається в межах такого протиправного злочинного діяння, – це інформація, інформаційні технології.

Термін «кібертероризм» був запропонований у 1980-х р. старшим науковим співробітником американського Інституту безпеки і розвідки (анг. – Institute for Security and Intelligence) Баррі Колліном, який використав його в контексті тенденції до переходу тероризму від фізичного до віртуального, породжуючого перетин та злиття цих світів [1].

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 [2].

Отже, спершу розкриємо поняття «тероризм». У найбільш загальному розумінні суть тероризму полягає у використанні насильства з метою залякування. Суб'єкт терористичного насильства – окремі особи або неурядові організації. Об'єкт насильства – влада в особі окремих державних службовців або суспільство в особі окремих громадян (в тому числі іноземців або держслужбовців інших держав), а також приватне і державне майно, інфраструктури, системи життєзабезпечення. Мета насильства – домогтися бажаного для терористів розвитку подій: революції, дестабілізації суспільства, розв'язання війни з іноземною державою, здобуття незалежності, зміну правового режиму, зміну кордонів або порушення територіальної цілісності чи недоторканності державних кордонів, зменшення обсягу прав людини [3].

В історичному аспекті термін «тероризм» вперше з'явився в 1798 р., коли філософ Еммануїл Кант використовував його для опису песимістичного погляду на долю людства. У той же рік цей термін можна було знайти в додатку до великого словнику Французької академії, це було викликано ексцесами революційного терору, і тому термін не мав такого значення, яке ми сьогодні в нього вкладаємо.

Нині під цим терміном в більшості випадків розуміються дії різних рухів, які впливають на уряд держави з метою радикальної зміни його політичного і соціального управління, при цьому об'єктом впливу є не тільки держава, але й внутрішня соціальна система [4].

Використовуючи національну законодавчу базу, зауважимо, що під тероризмом розуміється 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 [5].

У «Великому тлумачному словнику української мови» «тероризм» визначено як здійснювання, застосування терору; діяльність і тактика терористів [6].

Визначення ж інформаційного або кібертероризму можна знайти як в міжнародно-правових документах та проектах конвенцій, так і в дослідженнях фахівців з цієї проблематики. Однією з характерних рис визначень інформаційного тероризму є те, що в переважній більшості в них згадується тільки один аспект інформаційної безпеки, пов'язаний із засобами оброблення інформації, що звужує поняття інформаційного тероризму, тим самим обмежуючи сферу правового регулювання, що не сприяє ефективній співпраці держав у справі боротьби з інформаційним тероризмом [4].

Під кібертероризмом розуміють навмисну мотивовану атаку на інформацію, що обробляється комп'ютером, комп'ютерну систему або мережу, яка пов'язана з небезпекою для життя і здоров'я людей або настанням інших тяжких наслідків, якщо такі дії вчинені з метою порушення громадської безпеки, залякування населення, провокування військового конфлікту [5].

Таким чином, можна визначити кібертероризм як похідний тероризму, об'єктом посягання якого є інформаційна безпека. Він є найбільш небезпечним, оскільки межі його визначені віртуальним середовищем, і знайти порушника дуже важко.

Розгляд «кібертероризму» в історичних рамках охоплює чималий період і пов'язаний головним чином із еволюцією комп'ютерної обчислювальної техніки.

Доцільним є посылитися на етапи становлення, виділені С. О. Гнатюком у своїй статті «Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи» [2], однак, на наш погляд, можна їх систематизувати.

Перший період – 1960–1970 рр. – поява перших транзисторних обчислювальних систем, як наслідок поява дрібних кіберзлочинів.

Другий період – 1980–1990 рр. – випуск першої операційної системи, перший арешт «віртуальних злочинців», зареєстроване перше «сімейство комп'ютерних вірусів».

Третій етап – поява і активне запровадження «кібератак», втручання у роботу державних органів, в т. ч. військових, утворення хакерських груп та проведення шпінських кібероперацій.

Отже, із еволюцією людського суспільства розросталася і система кіберзлочинності, кіберзлочинів.

Поява такого роду протиправних злочинних діянь зумовила необхідність правового врегулювання відносин, що виникають у кіберпросторі. Відразу наголосимо, що однозначного і чіткого визначення поняття «кібертероризму» у юридичних документах немає.

У Ковенції Ради Європи про кіберзлочинність від 23.11.2001 р. немає чіткої дефініції «кібертероризму», проте з її положень випливає, що кібертероризм є навмисне застосування незаконно встановленого повноваження, насильства, руйнування або проникнення в кіберсистему, у разі якщо подібні дії можуть спричинити смерть або заподіяти шкоду особі або особам, істотної шкоди майну, цивільний безлад або значну економічну шкоду. Ця Конвенція є свого роду реакцією США на терористичні акти 11 вересня 2001 р.

У Конвенції Ради Європи 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 [8].

В Україні на сьогодні не розроблені нормативно-правові акти, що регулюють такий вид злочинності. Але головною зброєю у боротьбі з цією загрозою залишається законодавство, яке потребує подальшого вдосконалення. В українському законодавстві навіть немає такого виду злочину, як кібертероризм, є тільки тероризм [9], та 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 [10]. А тому на сьогодні важливим є юридичне закріплення «кібертероризму» у вітчизняному законодавстві, створення єдиної нормативної бази, як закріплювала б механізм захисту суспільства від кіберзлочинців.

Боротьба із кібертероризмом має включати усі дієві шляхи та методи захисту і попередження вчинення таких злочинів. На наш погляд, до таких основних шляхів належать:

- належне законодавче врегулювання поняття «кіберзлочинності», «кіберзлочину», його видів, основних характеристик, відповідальності за його вчинення, порядку притягнення особи до відповідальності;
- створення відповідних державних органів, із безумовним залученням спеціалістів у сфері комп'ютерних технологій, для захисту та боротьби з кібертероризмом;
- розроблення стійкого системного захисту інформації, інформаційних технологій, захисту ЕОМ;
- належне фінансування такого роду діяльності із привенції та захисту інформаційної безпеки;
- міжнародне співробітництво як у теоретичних розробках, так і у практичній діяльності.

**Висновки.** З огляду на сучасні реалії життя, все більш поширенішого розвитку набуває науково-технічний прогрес, поза межами якого не залишаються й комп'ютерні інновації. Інформаційні технології потрапляють під негативну дію осіб-кіберзлочинців, які посягають на персональну інформаційну безпеку кожного особи, людства загалом. Як наслідок, з'являється таке криминогенне явище, як «кіберзлочинність», в рамках якої ми розглядаємо «кібертероризм» як найбільш небезпечну загрозу інформаційному суспільству, він не має меж, існує у віртуальному світі, не має належного правового врегулювання як у вітчизняному, так і в міжнародному законодавстві. Саме тому на сьогодні головне завданням – віднайти шляхи та методи боротьби із кібертероризмом, щоб не допустити його поширення та захоплення нашого інформаційного простору. Важливим, безумовно, є міжнародне співробітництво, адже самотужки боротися із такою глобальною проблемою – складно, та, на наш погляд, не виправдано, оскільки ми живемо у єдиній інформаційній мережі та за її безпеку повинні боротися спільно.

#### Список використаної літератури

1. Collin B. *The Future of Cyberterrorism* // *Crime & Justice International Journal*. – 1997. – Vol. 13. – Bun. 2.
2. Гнатюк С. О. *Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи* / С. О. Гнатюк // *Ukrainian Scientific Journal of Information Security*, 2013. – Vol. 19/ – Issue-2.
3. Діордіца І.В. *Поняття та зміст кібертероризму [Електронний ресурс]* / І. В. Діордіца. – Режим доступу : <http://goal-int.org/ponyattya-ta-zmist-kiberterorizmu/>.
4. Кубишкін О. В. *Міжнародно-правові проблеми забезпечення інформаційної безпеки держави [Електронний ресурс]* / О. В. Кубишкін. – Режим доступу : <http://pravolib.pp.ua/informatsionnyy-terrorizm-15103.html>.

5. *Про боротьбу з тероризмом : Закон України від 20.03.2003 р. [Електронний ресурс]. – Режим доступу : <http://zakon0.rada.gov.ua/laws/show/638-15/page2>.*
6. *Великий тлумачний словник сучасної української мови / уклад. О. Єрошенко. – Донецьк : ТОВ «Глорія Трейд», 2012. — 864 с.*
7. *Топчій В. В. Кібертероризм в Україні: поняття та запобігання кримінально-правовими та кримінологічними засобами [Електронний ресурс]. – Режим доступу : [http://www.lj.kherson.ua/2015/pravo06/part\\_3/16.pdf](http://www.lj.kherson.ua/2015/pravo06/part_3/16.pdf).*
8. *Конвенція про кіберзлочинність від 23.11.2001 р. [Електронний ресурс]. – Режим доступу : [http://zakon2.rada.gov.ua/laws/show/994\\_575/page](http://zakon2.rada.gov.ua/laws/show/994_575/page).*
9. *Грицак Н. І. Кібертероризм як сучасна загроза національної безпеки [Електронний ресурс] / Н. І. Грицак. – Режим доступу : [http://ena.lp.edu.ua:8080/bitstream/ntb/13207/1/191\\_Gricak\\_466-468\\_69.pdf](http://ena.lp.edu.ua:8080/bitstream/ntb/13207/1/191_Gricak_466-468_69.pdf).*
10. *Кримінальний кодекс України від 05.04.2001 р. [Електронний ресурс]. – Режим доступу : <http://zakon3.rada.gov.ua/laws/show/2341-14/page11>.*

Стаття надійшла до редакції 18.05.2017.