УДК 342.9
DOI https://doi.org/10.32782/2524-0374/2024-10/63

КІБЕРТЕРОРИЗМ ЯК ФАКТОР ЗАГРОЗИ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ

CYBER TERRORISM AS A THREAT FACTOR TO NATIONAL SECURITY

Мазур Я.П., аспірант кафедри конституційного, адміністративного та фінансового права
Хмельницький університет управління та права імені Леоніда Юзькова

У статті розглянуті питання кібертероризму, як фактору загрози та приведені основні підходи до визначення поняття кібертероризму в літературі та законодавстві, представлено історію загроз інформаційній безпеці, оцінено небезпеку кібертероризму для людини і суспільства в цілому, наведено розмежування понять «кіберзлочинність» і «кібертероризм». Розглянуті поняття способи і можливості кібертероризму та кіберзлочинності як окремої категорії злочинів, притаманних інформаційній сфері. Кібертероризм – це використання комп'ютерних і телекомунікаційних технологій у терористичних цілях. До кіберзлочинів в Україні належать порушення авторського права та суміжних прав, шахрайство, незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, а також обладнанням для їх виготовлення,ухилення від сплати податків, зборів обов'язкових платежів, ввезення, виготовлення, збут і розповсюдження предметів порнографічного характеру, незаконне збирання з метою використання або використання відомостей, що становлять комерційну чи банківську таємницю. В статті розглянуті основні принципи діяльності у сфері кібербезпеки України та основні документи, що регулюють сферу забезпечення кібербезпеки України, це на національному рівні, закон № 2163-VIII від 5 жовтня 2017 року «Про основні засади забезпечення кібербезпеки України» та Національна стратегія кібербезпеки України. Закон «Про основні засади забезпечення кібербезпеки України» визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки України. Досліджено, що кіберзлочинність – це комплексне поняття, яке містить ознаки кіберзлочинності як особливого суспільно небезпечного явища, притаманного суспільству з високорозвиненими інформаційними технологіями. Різниця в суспільній небезпеці кібертероризму визначається як більш небезпечне явище, ніж кіберзлочинність. Проаналізовано теоретичні підходи до кримінальної відповідальності за кібертероризм, так ст. 361 та 361-1 КК України узгоджені з законодавством у сфері кібербезпеки, у ст. 361 КК України розмежована суворість покарання за кібератаку залежно від наслідків та посилив покарання – від штрафу до 15 років в'язниці, посилено покарання за ст. 361-1 КК України – від штрафу до 5 років в'язниці. Проаналізовано законодавство України щодо кібертероризму, надано рекомендації щодо вдосконалення правої основи.

Ключові слова: інформаційна безпека, інформаційні відносини, захист у сфері інформації, забезпечення, кібертероризм, кіберзлочинність, кібербезпека.

The article examines the issue of cyberterrorism as a threat factor and presents the main approaches to defining the concept of cyberterrorism in literature and legislation, presents the history of threats to information security, assesses the danger of cyberterrorism for a person and society as a whole, distinguishes between the concepts of «cybercrime» and «cyberterrorism». Concepts of ways and possibilities of cyberterrorism and cybercrime as a separate category of crimes inherent in the information sphere are considered. Cyber terrorism is the use of computer and telecommunication technologies for terrorist purposes. Cybercrimes in Ukraine include violations of copyright and related rights, fraud, illegal actions with transfer documents, payment cards and other means of access to bank accounts, as well as equipment for their production, tax evasion, mandatory payments, import, production, sale and distribution of objects of a pornographic nature, illegal collection for the purpose of use or use of information constituting a commercial or banking secret. The article examines the main principles of activity in the field of cyber security of Ukraine and the main documents regulating the sphere of cyber security of Ukraine at the national level, Law No. 2163-VIII of October 5, 2017 «On the Basic Principles of Cyber Security of Ukraine» and the National Cyber Security Strategy of Ukraine. The law «On the basic principles of ensuring cyber security of Ukraine» defines the legal and organizational foundations of ensuring the protection of the vital interests of a person and citizen, society and the state, national interests of Ukraine in cyberspace, the main goals, directions and principles of state policy in the field of cyber security of Ukraine. It has been investigated that cybercrime is a complex concept that contains signs of cybercrime as a special socially dangerous phenomenon inherent in a society with highly developed information technologies. The difference in public danger of cyberterrorism is defined as a more dangerous phenomenon than cybercrime. The theoretical approaches to criminal responsibility for cyberterrorism are analyzed, as well as art. 361 and 361-1 of the Criminal Code of Ukraine are harmonized with the legislation in the field of cyber security, in Art. 361 of the Criminal Code of Ukraine demarcated the severity of the punishment for a cyberattack depending on the consequences and increased the punishment – from a fine to 15 years in prison, increased the punishment under Art. 361-1 of the Criminal Code of Ukraine – from a fine to 5 years in prison. The legislation of Ukraine on cyber terrorism was analyzed, and recommendations were made to improve the legal framework.

Key words: information security, information relations, protection in the field of information, security, cyber terrorism, cyber crime, cyber security.

За останні десятиліття інформація стала потужним фактором розвитку суспільства. Становлення інформаційного суспільства дає нові імпульси традиційним загрозам безпеці держави та створює принципово нові ускладнення для системи національної безпеки, важливе місце посідає проблема тероризму, особливо такого його аспекту, як інформаційний тероризм, який виник внаслідок стрімкого розвитку суспільства. У таких умовах пошук нових шляхів забезпечення безпеки держави набуває особливого значення з огляду на появу нового поля протистояння – кіберпростору. Кіберзлочинність є міжнародним явищем. Ще в 2000 році на Форумі Конгресу ООН із запобігання кіберзлочинності цей термін був розкритий у двох значеннях. По-перше, кіберзлочин у строгому сенсі – це будь-яка незаконна дія, яка здійснюється за допомогою електронних транзакцій і метою якої є подолання захисту комп'ютерних систем і даних.

Поява кібертероризму, який експерти розглядають як різновид технологічного тероризму та визнають одним із найнебезпечніших видів кіберзлочинності, пов'язана з переходом до електронного управління технологічними процесами. У найширшому розумінні кіберзлочин – це будь-яка незаконна дія, вчинена у зв'язку з комп'ютерною системою або мережею або за допомогою неї, включаючи такі злочини, як незаконне зберігання, надання або розповсюдження інформації за допомогою комп'ютерної системи чи мережі. Сучасний кібертероризм за своїми масштабами технічний, здатен призводити до серйозних наслідків як на національному, так і на міжнародному рівнях. Можливості та наслідки можна з повною впевненістю прирівняти до традиційного тероризму та організованої злочинності.

Аналіз останніх досліджень та публікацій. Концепція кібертероризму виникла на рубежі 20–21 століть,

задовго до початку масового використання Інтернету. Термін «кібертероризм» є синтезом понять «простір кібербезпеки» та «тероризм».

Ліпкан В. А стверджує, що кіберзлочин – це злочинна діяльність, спрямована на отримання інформації з баз даних, перехоплення інформації, знищення інформації шляхом розповсюдження вірусних програм, фішингових програм і злому з корисливих, політичних чи особистих мотивів. Кіберзлочинці, стають все більш витонченими, а сучасні системи реалізації кіберзахисту не встигають адаптуватися до нових обставин.

Метою даного дослідження є визначення поняття «кіберзлочинність» і «кібертероризм» та загальних характеристик кібертероризму, його характерних рис та способів протидії цьому явищу. Небезпечність даного виду тероризму полягає у тому, що він не має ніяких національних меж та у проблематичності виявлення терориста в інформаційному просторі. Кібератака може статися на об'єкти критичної інфраструктури не тільки завдати величезних економічних збитків, але й порушити роботу багатьох компаній. Тому можливість терористичних атак з використанням інформаційно-комунікаційних технологій на об'єкти критичної інфраструктури викликає особливе занепокоєння.

Грищук В. К. визначає, що кібертероризм характеризується використанням комп'ютера як знаряддя злочину та існуванням Інтернету як міжнародного інформаційного простору, в якому вчиняється злочин. Зловмисна атака злочинців або їх груп відбувається на конкретні об'єкти, такі як інформація, програми, комп'ютери, локальні та глобальні мережі. Під кібертероризмом ми розуміємо шахрайські дії, вчинені з метою досягнення негативних наслідків, таких як отримання матеріальної вигоди або створення загрози інформаційній безпеці держави.

Макаренко Є. А. стверджує, що кіберзлочинність це будь-яка злочинна діяльність, яку здійснюють у цифровому просторі. Кожні 60 секунд в світі від кіберзлочинності втрачається 1 138 888 мільйонів доларів. Хакерські атаки, віруси, трояни, кібератаки, фізичні атаки, несанкціонований доступ і нещасні випадки, а також стихійні лиха – все це становить загрозу національній безпеці України в інформаційній сфері та підтримки захищеного середовище для обміну інформацією, яке реалізує правила та політику безпеки держави і є важливим і вагомим фактором [8].

Кібертероризм виникає у сфері кібербезпеки. Загрози національній безпеці України в інформаційній сфері це сукупність умов і факторів, що створюють загрозу важливим інтересам держави, суспільства та особи внаслідок можливості негативного інформаційного впливу на свідомість і поведінку громадян, а також про інформаційні ресурси та інформаційну інфраструктуру [11].

Фурашев В. М. стверджує, що кібертероризм – багатогранне явище, яке значною мірою зумовлене неконтрольованим використанням глобальних мереж, недостатньою увагою держави, громадянського суспільства та спецслужб до цього сегменту інформаційного простору. Кібертероризм виражається в атаках на комп'ютери, комп'ютерні програми та мережеву інформацію, ці атаки спрямовані на створення в суспільстві атмосфери страху та безнадійності в ім'я реалізації цілей та інтересів суб'єктів терористичної діяльності. Тероризм у сфері комп'ютерних технологій має такі ознаки: анонімність, віддаленість дійової особи, відносна дешевизна, відсутність необхідності використання вибухівки і самогубних акцій, великий розголос інформації [3].

Терористичні організації широко використовують Інтернет та новітні інформаційні технології для досягнення таких цілей, як встановлення конфіденційного зв'язку (наприклад, через онлайн-ігри в чатах або зашифрованих повідомленнях), атак за допомогою таких сервісів, як Google Maps або Earth, координація атак з використанням VoIP-телефонії та інших інформаційних технологій забезпечують анонімність і конфіденційність. Кібертерористами виконуються дії, щодо виявлення потенційних цілей (наприклад, використання соціальних мереж для виявлення «вигідних» жертв з метою отримання викупу за їх викрадення), фінансування терористичної діяльності через анонімні онлайн-пожертви зроблені через електронні платіжні системи, залучення нових учасників та поширення терористичної ідеології через створення якісних медіа-ресурсів та активну роботу з вербування в соціальних мережах [5]. Ефективність форм і методів кібертероризму залежить від характеристик інформаційної інфраструктури та рівня її безпеки.

Аналіз наукової літератури свідчить, що більшість дослідників поділяють позиція про те, що інформаційний тероризм є видом терористичної діяльності, пов'язаної з досягненнями інформаційних технологій.

Кібератака становить серйозну загрозу для людства, порівнянну з ядерною, бактеріологічною та хімічною зброєю. Через свою новизну масштаби цієї загрози недостатньо зрозумілі та досліджені. Кібератака не знає національних кордонів, кібертерорист може загрожувати інформаційним системам майже в будь-якій точці світу. Виявити та знешкодити віртуального терориста дуже проблематично через малу кількість слідів, які він залишає.

Терористичний акт із застосуванням високих технологій – це комплексна дія, що виражається в умисній політично мотивованій атаці на інформаційні системи, яка створює реальну загрозу життю людей або тягне за собою інші тяжкі наслідки [8].

Кібертерористи не тільки здійснюють теракти за допомогою електронних мереж, а й мають можливість отримувати конфіденційну інформацію та державну таємницю. На багатьох сайтах державних органів розміщена інформація різної важливості. Наприклад, плани підземних комунікацій, стратегічних об'єктів, що будуються, розташування об'єктів життєзабезпечення. Крім того, злочинці можуть отримати доступ до багатьох особистих даних користувачів мережі, починаючи від адрес і номерів телефонів до детальної особистої інформації.

Одним з способів кібертероризму є політично мотивована атака на інформацію, в прямому контролі суспільства шляхом превентивного залякування. Другий спосіб кібертероризму – інформаційна атака на комп'ютерну інформацію, комп'ютерні системи, пристрої передачі даних та інші компоненти інформаційної інфраструктури, що здійснюється групами або окремими особами. Така атака дає можливість проникнути в систему, перехопити або придушити контроль над мережевими інформаційними обмінами та досягти інших руйнівних ефектів [4].

Рульов І. М. пише про рівні можливості кібертероризму, такі як простий неструктурований кібертероризм, що має здатність здійснювати базові атаки на окремі системи за допомогою інструментів, створених кимось іншим і в його організації мало аналізу цілей, управління та контролю. Більш розвинутий кібертероризм, має можливість проводити складніші атаки на кілька систем або мереж і потенційно змінювати або створювати базові інструменти злому та організація має елементарний предмет аналізу, управління та контролю. Існує і кібертероризм де дія комплексно скоординована, є можливість скоординованих атак, які можуть призвести до масового руйнування інтегрованих різнорідних систем захисту (включаючи криптографічні системи), організація має дуже ефективний аналіз цілей, управління та контроль [7].

Відомий український дослідник з кібербезпеки професора В. Л. Бурячко сформулював таке визначення терміну, «кібератака» – це сукупність узгоджених за метою, змістом і часом дій або заходів, так званих кібератак, спрямованих на конкретний об'єкт впливу з метою заподіяння шкоди [4].

Гавва С. К., Головко С. Г. пишуть про різні техніки кібертероризму в кіберпросторі, такі як пошкодження окремих фізичних елементів інформаційного простору, наприклад, руйнування електромереж, створення перешкод, використання спеціальних програм, що стимулюють руйнування обладнання, викрадення або знищення інформації, програмних і технічних ресурсів суспільного значення шляхом подолання систем захисту, запровадження вірусів тощо, використання програмного забезпечення та інформації з метою їх спотворення або модифікації в інформаційних системах і системах управління, розголошення та загроза оприлюднення конфіденційної інформації про функціонування державної інформаційної інфраструктури.

У юридичній літературі вказується, що доступність інформаційних технологій значно підвищує інформаційні ризики. Тероризм та розвиток інформаційної інфраструктури суспільства сприяють створенню додаткових ризиків інформаційного тероризму.

Кібербезпека – це захист життєво важливих інтересів людини і громадянина, суспільства і держави при використанні кіберпростору, що забезпечує сталий розвиток інформаційного суспільства та цифрового комунікаційного середовища, а також своєчасне виявлення, запобігання та нейтралізацію реальних і потенційні загрози національній безпеці України в кіберпросторі [14].

В. А. Ліпкан зазначає, що інформаційна безпека України є органічною частиною національної безпеки та що її врахування є необхідним для формування базових знань та уявлень про національну безпеку. Нормальна життєдіяльність суспільства визначається рівнем розвитку, якістю функціонування та безпеки інформаційного середовища, а також ступенем і станом нормативно-правового забезпечення цих процесів. Законодавство спрямоване на закріплення державної інформаційної політики, яка передбачає забезпечення гарантованого рівня національної безпеки в інформаційній сфері та нормальний розвиток інформаційних технологій [3].

Положення правового регулювання відносин у сфері інформації відображено в указах та розпорядженнях Президента України, Постановах та розпорядженнях Кабінету Міністрів України, нормативних актах міністерств і відомств. Правовою основою забезпечення кібербезпеки України є Конституція України, закони України.

У Статті 17 Конституції України сказано, що захист інформаційної безпеки є однією з найважливіших функцій держави та справою всього українського народу. Закон України «Про основні засади забезпечення кібербезпеки України» дає таке визначення: «кібернетична безпека (кібербезпека) – це стан захищеності життєве важливих інтересів людини та громадянина, суспільства та держави. Закон № 2163-VIII від 5 жовтня 2017 року «Про основні засади забезпечення кібербезпеки України» та Національна стратегія кібербезпеки України є основними документами, що регулюють цю сферу. Стратегія кібербезпеки України встановлює пріоритети національних інтересів у сфері кібербезпеки, існуючі та потенційно можливі кіберзагрози, цілі та завдання щодо забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору з використанням в інтересах особистості, суспільства і держави [6].

Основними принципами діяльності у сфері кібербезпеки України є: координація дій із забезпечення кібербезпеки суб'єктів кібербезпеки відповідно до їх призначення (специфіки діяльності) та повноважень, співпраця структур державного та приватного секторів на національному та міжнародному рівнях для забезпечення належного реагування на кіберзагрози, розставляти пріоритети завдань і зосередити зусилля на забезпеченні кібербезпеки об'єктів критичної інформаційної інфраструктури, застосувати новітні технології та технології передового досвіду для покращення стану кіберзахисту критичних об'єктів інформаційної інфраструктури. У стратегії визначено, що «забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України» [2].

Мацюк В. Я. визначає, що до кібербезпеки входить безпека комп'ютерної мережі, безпека операційної системи, безпека програмного забезпечення, методи тестування захищеності комп'ютерних систем, забезпечення безперервності бізнесу та інформаційної безпеки, комплексні системи захисту інформації, управління інформаційною безпекою. Норми інформаційного права регулюють суспільні відносини, що виникають в інформаційній сфері з приводу реалізації інформаційних прав і свобод [10].

У вітчизняній юридичній літературі проблема кіберзлочинності та кібертероризму висвітлювалися, досліджується рядом вчених. Автори підкреслюють складність застосування організаційно-правових заходів захисту інформації та методів провідних правових напрямків в інформаційному праві.

Характерною рисою кібертероризму є те, що всі відомі хакерські групи та особи не прагнуть рекламувати свої дані, а діють лише під псевдонімом. При цьому хакера-терориста слід відрізняти від простого хакера, який діє з корисливих чи хуліганських мотивів. Проте, якщо дії таких осіб призвели до тяжких наслідків, наприклад, до загибелі людей, то цей вид хуліганства не можна вважати інакше як тероризмом.

Заходи з захисту інформації складають методологічну основу правозастосовної роботи, і від правильного вибору захисту значною мірою залежить ефективність інформаційних відносин [7].

Кібертероризм – це серйозний злочин, у якого є виконавець і спонсор. Злочинець, як і будь-який злочинець, має мотив – як правило, гроші. Але якщо подивитися на мотивацію клієнтів, то тут їхнє коло ширше. Слід зазначити, що попри всю сукупність матеріалів досліджень, що проводились з цього питання, протидія даному виду злочинної діяльності значно відстає. Необхідно зосередитися на політиці безпеки не лише на національному рівні, а й на адміністративному рівні, який є нижчим, але не менш важливим. Терористи та кібертерористи – це злочинці, які кинули виклик культурі, цивілізації та суспільству, з якими неможливий компроміс і які повинні бути притягнуті до відповідальності.

В Україні прийнято низку законів та нормативно-правових актів, щодо забезпечення інформаційної безпеки. Є перспективи для подальшого розвитку законодавства по боротьби з кібертероризмом. Своєчасне реагування, запобігання та припинення кібератак є однією з основних вимог забезпечення національної безпеки України.

ЛІТЕРАТУРА

1. Про рішення Ради національної безпеки і оборони України: Указ Президента України від 14 вересня 2020 року «Про Стратегію національної безпеки України» № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text
2. Бурячок В. Л. Інформаційна та кібербезпека. Київ : ДУТ, 2015. 288 с.
3. Гавва С. К., Головко С. Г. Сучасний кібертероризм як загроза національній безпеці. *Наукові* праці. *Свобода, безпека та незалежність: правовий вимір: матеріали XIII Міжнародної науково-практичної конференції*, м. Київ, 24 лютого 2023 р. С. 54–56.
4. Глазов О. В. Міжнародний інформаційний тероризм у контексті загроз національній безпеці України. *Наукові праці. Політологія*. 2012. № 185. С. 78–82.
5. Грищук В.К. Тероризм: теоретико-прикладні аспекти. Львів: ЛьвДУВС, 2011. 328 с.
6. Ліпкан В. А. Боротьба з тероризмом. Київ : Знання,2002. 254 с.
7. Ліпкан В. А. Національна безпека України : нормативно-правові аспекти забезпечення Київ : Знання,2003. 180 с.

8. Макаренко Є. А. Міжнародні інформаційна безпека: сучасні виклики та загрози. Київ : Центр вільної преси, 2006. 916 с.
9. Рульов І. М. Співвідношення кібертероризму та кіберзлочину. *Юридичний вісник*. Одеса : Гельветика, 2021. № 3. С. 178–185.
10. Топчій В.В. Кібертероризм в Україні: поняття та запобігання кримінально-правовими та кримінологічними засобами. Київ : ДУТ, 2015. 188 с.
11. Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. Інформація і право. 2012. № 2. С. 162–169.
12. Цимбалюк В.С. Основи інформаційного права України. Київ: Знання, 2004. 274 с.
13. Шеломенцев В.П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення. Боротьба з організованою злочинністю і корупцією (теорія і практика). 2012. № 1. С. 312–320.
14. Широкова-Мурараш О. Г. Кіберзлочинність та кібертероризм як загроза міжнародній інформаційній безпеці. *Науковий* фаховий журнал з питань правової інформатики, інформаційного права безпеки. *«Правова інформатика»*. Київ : ПанТот, 2011. № 1. 12 с.