Горячковська Д.А.,
студентка 6 курсу, 7 групи, Інституту прокуратури та кримінальної юстиції Національного юридичного університету імені Ярослава Мудрого

КРИМІНОЛОГІЧНА ДЕТЕРМІНАЦІЯ КІБЕРТЕРОРИЗМУ

Анотація. У тезах розглянуті причини та умови вчинення кіберзлочинності, надано їх характеристику.

Ключові слова: кібертероризм, кібератака, детермінація, кіберзлочинність.

Аннотация. В тезисах рассмотрены причины и условия совершения киберпреступности, предоставлено их характеристику.

Ключевые слова: кибертерроризм, кибератака, детерминация, киберпреступность.

Summary. In theses examined the causes and conditions of cybercrime and their characteristics.

Keywords: cyberterrorism, cyberattack, determination, cybercrime.

Кібертероризм – це дії з дезорганізації інформаційних систем, що створюють небезпеку загибелі людей, заподіяння значної майнової шкоди або настання інших суспільно небезпечних наслідків, якщо такі дії вчинені з метою порушення суспільної безпеки, залякування населення або впливу на ухвалення певних рішень органами влади [1, с. 39]. З точки зору філософії, парні категорії «хаос» і «порядок» взаємопов'язані, співвідносяться як діалектичні протилежності, постійно переходять одна в іншу. Проте у впорядкованих явищ є причина, що їх породжує, визначає повторюваність, послідовність і прогнозованість розвитку [9, 204].

Характерною відмінністю кібертероризму від кіберзлочинності є його відкритість, коли вимоги терориста широко сповіщаються. Урядова активність з боку світових лідерів у кіберпросторі, лобіювання інтересів поза територіальними і національними рамками інформаційної політики та організація і успішна діяльність транснаціональних злочинних угруповань, що «фахово» вузько спрямовано займаються кіберзлочинністю все це обумовлює необхідність

виробленні рекомендацій щодо обрання напрямків і сфер видозміни [7, с. 159].

Кібертероризм, як і будь яка інша протиправна діяльність, - це одночасно функція ситуативних та індивідуальних причин. Основними причинами кібертероризму слід вважати політичні, соціально-економічні, матеріальні, релігійні та духовні. Динаміка злочинності на протязі останніх років характеризується хвилеподібними коливаннями, які чітко показують виражену тенденцію до зростання злочинності на території нашої держави. Висока складність соціальних систем є безумовною ознакою нелінійності законів залежності станів таких систем від певних зовнішніх та внутрішніх факторів [10]. За сферою злочинних проявів особливе місце посідають злочини у сферах захисту інформації, використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку [10, с. 17].

Політичною причиною кібертероризму може виступати прагнення досягнути певних цілей в політичній боротьбі, використовуючи при цьому наявну політичну нестабільність. Законом задекларовано визнання презумпції особистої свободи людини відповідно до принципу, згідно з яким дозволено все, крім того, що прямо забороняється законом, в той же час визнання обмеженості свободи держави, її органів і посадових осіб відповідно до принципу, згідно з яким дозволено лише те, що прямо передбачається законом [9].

Серед соціально-економічних причин слід відзначити низький рівень життя в країні; невідповідність між рівнем розвитку суспільного виробництва та постійно зростаючими потребами членів суспільства, що загострює соціальну нерівність; відмінності між умовами життя у різних типах поселень тощо. Кібертероризм направлений на досягнення конкретної соціальної цілі, встановлення справедливого, з точки зору кіберзлочинця, устрою суспільства, певного «ідеалу». Кібератаки використовуються з метою отримання матеріальних благ для конкретної соціальної групи або суспільством в цілому. Матеріальні причини кібертероризму випливають з того, що сьогодні тероризм загалом - це бізнес, здатний приносити своїм організаторам чималий дохід. Тому така діяльність здійснюється у зв'язку з прагненням отримати матеріальні блага для

себе всупереч встановленому порядку (вимога викупу інформації, отриманої шляхом проникнення в інформаційні системи, винагорода виконавцям з боку замовників тощо).

Слід виділити релігійні причини вчинення кібертероризму. В даний час існують різні релігійні течії і пропагування їх цінностей та ідей (особливо радикальних) може отримувати форму масових кібератак. Але в більшості випадків кібертерористи (як і звичайні терористи) лише прикривають свої справжні наміри релігійними гаслами. Поряд можна відзначити і духовні причини, зокрема, спотворення правових і загальнолюдських цінностей, «криміналізація» населення, поширення кримінальної субкультури тощо.

Причиною кібертероризму може бути і його здатність полегшити підготовку до вчинення терактів у «фізичному світі». Зокрема, кібератаки забезпечують збір інформації та коштів, необхідної для планування терактів, анонімне залучення до терористичної діяльності співучасників, розширення потенціалу малих терористичних груп, поширення агітаційно-пропагандистської інформації про терористичні рухи, їхні цілі і завдання [2, с. 95].

Детермінація кібертероризму охоплює не лише причини його вчинення, а і умови, тобто зовнішні об'єктивні негативні факти реальної дійсності, які полегшують кібератаки та сприяють досягненню їх мети.

Правові умови кібертероризму полягають в слабкій адаптованості законодавства в питаннях охорони суспільних відносин в сфері інформаційно-телекомунікаційних технологій. Доступність комп'ютерних мереж дозволяє злочинцям вибирати правове середовище тієї держави, яка оптимальним чином відповідає їх цілям і мінімізує негативні правові наслідки кібератак.

До матеріально-технічних умов існування кібертероризму слід віднести відсутність державних меж для вчинення кібератак (такі акти можуть бути здійснені з різних точок земної поверхні); стрімкий розвиток інформаційно-комунікативних технологій; низький рівень кіберзахисту критичної інфраструктури держави [3].

Серед організаційно-управлінських умов виділяють низьку підготовленість правоохоронних органів до боротьби з кіберзлочинністю, відсутність кваліфікованих кадрів, неналежне технічне оснащення, слабке фінансування [4, с.156].

Психологічні і фізичні чинники полягають у не завжди серйозному підході керівників підприємств і організацій до питань забезпечення інформаційної безпеки і захисту інформації, нехтуванні заходами інформаційної безпеки з боку простих користувачів, анонімності вчинення кібератак, невидимості, що дозволяє уникати психологічних контактів і пов'язаних з ними можливих негативних наслідків [5, с. 206].

Не зважаючи на те, що до цього часу кібератаки, здійснені терористами, ще не призводили до людських жертв, техногенних катастроф або інших тяжких наслідків, повномасштабна реалізація загрози кібертероризму є лише питанням часу. Вдалі кібератаки на об'єкти критичної інфраструктури, що були здійснені хакерами, в тому числі, під впливом терористичної ідеології, засвідчують перетворення кібертероризму на актуальну загрозу національній та міжнародній безпеці. Тому вивчення питання детермінації кіберзлочинності дозволить ефективніше протидіяти кібератакам та підвищить шанси на їх запобігання.

ЛІТЕРАТУРА:

1. Геращенко О. С. Кібертероризм як фактор загрози національній безпеці України: генеза поняття та шляхи протидії / Південноукраїнський правничий часопис. – 2016. – № 3-4 – 39 с.

2. Ілляшенко А.В., Кіяшко Ю.М. Інформаційний тероризм як злочинна діяльність міжнародного масштабу / Журнал східноєвропейського права. – 2016. – № 27 – 94 с.

3. Ткачук Н. А. Актуальні кіберзагрози сучасного безпекового середовища / Міжнародний науковий журнал «Інтернаука». Серія: «Юридичні науки». - 2018. - № 7. URL: https://doi.org/10.25313/2520-2308-2018-7-4183

4. Кравцова М.О. Сучасний стан і напрями протидії кіберзлочинності в Україні / Вісник кримінологічної асоціації України. – 2018. – № 2(19) – 155 с.

5. Таволжанський О. В. Сучасні реалії кіберпростору України / О. В. Таволжанський // Забезпечення правопорядку в умовах коронакризи : матеріали панельної дискусії IV Харків. міжнар. юрид. форуму, м. Харків, 23–24 верес. 2020 р. – Харків, 2020. – С 203–208.

6. Robotization of manufacturing process: economic and social problems and legal ways of their solution / O. E. Kostyuchenko, T. V. Kolesnik, Z. V. Bilous, O. V. Tavolzhanskyi // Financial and credit activity: problems of theory and practice. – 2019. – Vol. 3, is. 30. – P. 454–462.

7. Tavolzhanskyi, O.V. (2017). Osnovu derzhavnoi kiberpolituku Ukrainu: formuvannya ta realizatsiya. Naykovo-informatsyinui visnuk Ivano-Frankivskogo yniversutety prava imeni Korolya Danula Galutskogo: Seriya Pravo, 4. (16), 158–164 [In Ukrainian].

8. Таволжанський О. В. Особливості забезпечення кібербезпеки у сучасному світі: огляд суб'єктів запобігання кіберзлочинності. Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького. Серія : Право. - 2018. - № 6. - С. 154-163.

9. Головкін Б.М. Теперішнє і майбутнє кримінології //Проблеми законності. Харків : Нац. юрид. ун-т імені Ярослава Мудрого. 2020. № 149. С. 168- 184. URL: http://plaw.nlu.edu.ua/article/view/200724/205532

10. Головкін Б. М. Види злочинності // Журнал Східноєвропейського права. 2015. № 18. С. 14-21. URL: http://easternlaw.com.ua/wp-content/uploads/2015/08/golovkin_18.pdf

Науковий керівник: к.ю.н, доц О.В. Таволжанський