Список бібліографічних посилань

1. Протягом грудня в Україні пройде операція з припинення діяльності нелегального грального бізнесу // Міністерство внутрішніх справ України: офіц. сайт. URL: http://mvs.gov.ua/ua/news/4300_Protyagom_grudnya_v_Ukraini_proyde_operaciya_z_pripinennya_diyalnosti_nelegalnogo_gralnogo_biznesu_FOTO_VIDEO.htm (дата звернення: 05.05.2017).

2. У центрі Києва поліцейські викрили підпільне казино/Департамент захисту економіки Нац. поліції України // Національна поліція: тимчас. веб-сайт. 03.12.2015. URL: https://kv.npu.gov.ua/uk/img/kyivska/uk/publish/article/1737573 (дата звернення: 05.05.2017).

Одержано 10.05.2017

УДК 343.341+343.851

Валерія Сергіївна ЧЕРНОВОЛ,
курсант 3 курсу факультету № 4 Харківського національного університету внутрішніх справ, м. Харків
Науковий керівник: ***Юртаєва Ксенія Володимирівна****,*
кандидат юридичних наук, старший викладач кафедри кримінального права і кримінології факультету № 1 Харківського національного університету внутрішніх справ, м. Харків

КРИМІНОЛОГІЧНА ХАРАКТЕРИСТИКА ТА ЗАХОДИ ПРОТИДІЇ КІБЕРТЕРОРИЗМУ

Окреслено найбільш нагальні проблеми організаційно-правового забезпечення національної безпеки в інформаційному просторі. Визначено заходи протидії кібертероризму.

Ключові слова: *кібертероризм, інформаційні системи, національна безпека, інформаційна безпека, заходи протидії.*

З розвитком високих технологій та подальшим їх впровадженням у повсякденне життя людини спостерігається перехід основної діяльності людини з матеріального світу в світ віртуальний. Але разом з позитивним прогресом, зменшенням затрат часу та ресурсів на обмін інформацією, зміну та прийняття рішень, розвитком бізнесу, виник прогрес негативний: злочинність у традиційному розумінні почала видозмінюватися, і здавалося б, сталі склади злочинів поступово почали мігрувати до віртуалізованого простору глобальної мережі Інтернет.

У сучасних умовах спостерігається поширення терористичної діяльності радикально налаштованих осіб, груп і організацій, ускладнюється характер їх діянь, зростає тяжкість вчинених

терористичних актів. Зазначена тема набуває ще більшої загостреності та актуальності, зважаючи на той факт, що терористична діяльність часто переходить у кіберпростір, з чим дедалі частіше стикаються в своїй практичній діяльності національні та міжнародні правоохоронні органи.

Кримінологічний аналіз такого суспільно небезпечного явища як «кібертероризм» наочно показує, що загрози, які воно за собою тягне, є надзвичайно серйозними, причому її актуальність зростає з розвитком і поширенням інформаційно-телекомунікаційних технологій.

На сьогоднішній день законодавчого визначення кібертероризму не існує. Деякі вчені характеризують кібертероризм як метод для захоплення інформації, а збиток, який він завдає визначають ціною цієї інформації. Вони мотивують свою думку тим, що сучасне суспільство не може обходитися без електронних носіїв інформації та цифрових методів її зберігання і обробки [1]. Досить повно кібертероризм визначає В. В. Топчій як навмисну вмотивовану атаку на інформаційний простір або інформацію, що обробляється електронно-обчислювальною машиною або транспортується по мережі, яка пов'язана з настанням небезпеки для життя і здоров'я людей або спричиненням інших тяжких наслідків, якщо такі дії вчинені з метою порушення публічної безпеки, залякування населення, провокування військового конфлікту [2]. Зазначене визначення, на нашу думку, є найбільш вдалим.

Особлива небезпека кібертероризму полягає в тому, що сучасні інформаційно-комунікативні технології забезпечують відносно невеликі терористичні групи могутньою та дієвою зброєю, своєрідним ретранслятором насильства. Об'єктивно кібертероризм може виражатися у незаконному втручанні в роботу електронно-обчислювальних машин, систем та комп'ютерних мереж, присвоєнні, вимаганні комп'ютерної інформації, організації атаки на інформаційні ресурси, закладки та розробки комп'ютерних вірусів, які здійснюють знімання, модифікацію, або знищення інформації тощо.

Аналіз сучасної кримінологічної інформації дозволяє стверджувати, що для України значну зовнішню загрозу становить розповсюдження інформаційного тероризму. Зазначений вид кібертерористичної діяльності постає перед суспільством як новий вид терористичної активності негативно налаштованої ланки суспільства, орієнтований на використання різних форм і методів тимчасового або незворотного виведення з ладу інформаційної інфраструктури держави або її елементів, а також за допомогою протиправного використання інформаційної структури для створення умов, що тягнуть за собою тяжкі наслідки для різних сторін життєдіяльності особистості, суспільства і держави [3, с. 13]. Враховуючи високий ступінь суспільної небезпеки від даного виду тероризму, на наш погляд, його слід розглядати як самостійний склад злочину.

Проте найбільш небезпечним різновидом прояву кібертероризму є використання сучасних інформаційних технологій, і в першу чергу глобальної мережі Інтернет, як виду зброї, яка застосовується з метою пошкодження важливих об'єктів державної енергетичної, транспортної або урядової інфраструктури. Загрози критичній інфраструктурі слід розглядати не тільки з точки зору можливостей та характеру їх походження, але і слід виокремлювати вразливі елементи критичної інфраструктури, на які ці загрози можуть бути спрямовані: фізичні елементи, зокрема, обладнання та ресурси об'єктів критичної інфраструктури; системи управління та комунікації, зокрема системи автоматичного управління та регулювання роботи об'єктів, системи зв'язку тощо; персонал об'єктів, зокрема диспетчерський, оперативний персонал, який безпосередньо забезпечує функціонування критичної інфраструктури у реальному часі.

Такий вид атаки поєднує підготовчий етап – дії, що створюють на об'єкті нові уразливі місця, та атакуючі дії – використання уразливих місць. При цьому, підготовчі дії можуть здійснюватися значно раніше за часом, ніж сама атака, можуть бути задіяні працівники (інсайдери) підприємства, що є об'єктом нападу, та здійснені різноманітні відволікаючі маневри. Виходячи з цього, потрібно встановити єдині кваліфікаційні вимоги для всіх категорій працівників, які задіяні в обслуговуванні та мають доступ до об'єктів критичної інфраструктури, а також впровадити для даних категорій працівників обов'язкове проходження періодичної атестації на предмет відповідності заявленим вимогам.

Аналізуючи стан забезпечення інформаційної безпеки, вбачаємо необхідність удосконалення системи законодавчого регулювання інформаційної безпеки. Одночасно з цим, постає потреба у кримінально-правовому закріпленні такого діяння як кібертероризм, виробленні нових засобів забезпечення інформаційної безпеки державного управління та введення постійного моніторингу інформаційного середовища на предмет наявності нових загроз та небезпек.

Підсумовуючи вищевикладене, необхідно зазначити, що в умовах глибокого латентного проникнення злочинності до глобальної мережі Інтернет, яка в свою чергу посідає провідне місце в регулюванні суспільного та державного життя, подолання такої злочинної активності стає нагальною потребою на шляху розбудови інформаційного суспільства і входження України у світовий інформаційний простір.

Список бібліографічних посилань

1. Гнатюк С. О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. *Безпека інформації.* 2013. № 2. С. 118–129.

2. Топчій В. В. Кібертероризм в Україні: поняття та запобігання кримінально-правовими та кримінологічними засобами. *Науковий вісник Херсонського державного університету. Серія: Юридичні науки.* 2015. Вип. 6, т. 3. С. 65–68. URL: http://www.lj.kherson.ua/2015/pravo06/part_3/16.pdf (дата звернення: 01.05.2017).

3. Коршунов В. О. Політичний тероризм: інформаційні методи боротьби: автореф. дис. … канд. політ. наук: 23.00.02. Дніпропетровськ, 2008. 18 с.

4. Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави: затв. постановою Кабінету Міністрів України від 23.08.2016 № 563 // База даних (БД) «Законодавство України»/Верховна Рада (ВР) України. URL: http://zakon.rada.gov.ua/laws/show/563-2016-п (дата звернення: 01.05.2017).

5. Стратегія національної безпеки України: затв. указом Президента України від 26.05.2015 № 287/2015 // БД «Законодавство України»/ВР України. URL: http://zakon.rada.gov.ua/laws/show/287/2015 (дата звернення: 01.05.2017).

6. Стратегія кібербезпеки України: затв. указом Президента України від 15.03.2016 № 96/2016 // БД «Законодавство України»/ВР України. URL: http://zakon.rada.gov.ua/laws/show/96/2016 (дата звернення: 01.05.2017).

7. Євсєєв В. О. Можливі шляхи удосконалення захисту критичної інфраструктури України з урахуванням світового досвіду. *Збірник наукових праць Харківського національного університету Повітряних Сил.* 2016. № 4 (49). С. 168–172. URL: http://www.hups.mil.gov.ua/periodic-app/article/17271/zhups_2016_4_35.pdf (дата звернення: 01.05.2017).

Одержано 10.05.2017

УДК 343.09

Ангеліна Віталіївна ШАЛАБАЙ,
студентка 5 курсу юридичного факультету Чорноморського національного університету імені Петра Могили, м. Миколаїв
*Науковий керівник: **Шведова Ганна Леонідівна**,*
кандидат юридичних наук, доцент, завідувач кафедри цивільного та кримінального права і процесу Чорноморського національного університету імені Петра Могили, м. Миколаїв

ПРОБЛЕМНІ ПИТАННЯ ПРАВОВОГО РЕГУЛЮВАННЯ ЗАХИСТУ ВИКРИВАЧІВ У СФЕРІ ЗАПОБІГАННЯ І ПРОТИДІЇ КОРУПЦІЇ

У статті розглянуто проблемні питання правового регулювання захисту викривачів у сфері запобігання і протидії корупції. Проаналізовано Закон України «Про запобігання корупції» щодо захисту викривачів