6. Про Національну поліцію : Закон України від 02.07.2015 р. № 580-VIII : URL: https://zakon.rada.gov.ua/laws/show/580-19#Text.

7. Про затвердження Положення про Національну поліцію : Постанова Кабінету Міністрів України від 28.10.2015 №877:URL: https://zakon.rada.gov.ua/laws/show/877-2015-п#Text.

8. Про затвердження Положення про організацію службової підготовки працівників Національної поліції України : наказ МВС України від 26.01.2016 № 50. URL: https://zakon.rada.gov.ua/laws/show/z0260-16#Text.

9. Про затвердження Порядку організації системи психологічного забезпечення поліцейських, працівників Національної поліції України та курсантів (слухачів) закладів вищої освіти із специфічними умовами навчання, які здійснюють підготовку поліцейських :наказ МВС України від 06.02.2019 р. № 88. URL: https://zakon.rada.gov.ua/laws/show/z0348-19#Text.

10. Євдокімова О. О. Специфіка формування психологічної стійкості у поліцейських у процесі професійної підготовки. Підготовка поліцейських в умовах реформування системи МВС України. Харків, 2018. С. 63–66.

11. Барко В. І., Барко В. В., Остапович В. П. Професійна психологічна підготовка поліцейських Національної поліції України. Науковий вісник ХДУ. Т. 1. № 2. 2018. С. 176–181.

УДК 343.9:159.9

Тимченко Катерина Андріївна,
здобувач вищої освіти Навчально-наукового інституту права та підготовки фахівців для підрозділів Національної поліції Дніпропетровського державного університету внутрішніх справ
Науковий керівник:
Савенко Вікторія Петрівна,
старший викладач кафедри кримінального права та кримінології Дніпропетровського державного університету внутрішніх справ

ОСОБЛИВОСТІ ЗАХОДІВ ПРОТИДІЇ КІБЕРТЕРОРИЗМУ ТА ЇХ КРИМІНОЛОГІЧНА ХАРАКТЕРИСТИКА

З розвитком високих технологій та їх подальшим проникненням у повсякденне життя, предмет людської діяльності зміщується з фізичного у віртуальний світ. Однак, поряд з позитивними зрушеннями, такими як скорочення часу і ресурсів, що витрачаються на обмін інформацією, зміни, прийняття рішень і розвиток бізнесу, існують і негативні зрушення, наприклад, те, що злочинність в її традиційному розумінні починає змінюватися, і, здавалося б, стабільні

правопорушення поступово переміщуються у віртуальний простір глобальної мережі Інтернет. Це позитивна тенденція.

В умовах сучасності спостерігається поширення терористичної діяльності радикально налаштованих осіб, груп і організацій, характер їхніх дій стає все більш витонченим, а тяжкість терористичних актів зростає. Ця тема стала ще більш серйозною та актуальною у світлі того, що терористична діяльність часто переноситься в кіберпростір і з нею все частіше стикаються на практиці національні та міжнародні правоохоронні органи.

Кримінологічний аналіз суспільно небезпечного явища такого, як «кібертероризм», дає підстави стверджувати, що загроза, яку він становить, є надзвичайно серйозною, а його актуальність зростає з розвитком і поширенням інформаційно-комунікаційних технологій.

На сьогоднішній день не існує юридичного визначення кібертероризму. Деякі вчені характеризують кібертероризм як метод захоплення інформації, а шкода, яку він завдає, визначається ціною цієї інформації. В.В. Топчій описує кібертероризм як інформацію, що обробляється інформаційними просторами та комп'ютерами, або передається мережами [1]. Він визначає його як цілеспрямовану атаку на інформацію, що передається мережею. Коли така атака спрямована на порушення громадської безпеки, тероризування населення або провокування військового конфлікту, вона може призвести до загрози життю і здоров'ю людей або інших серйозних наслідків [2].

Особлива небезпека кібертероризму полягає в тому, що сучасні інформаційно-комунікаційні технології надають відносно невеликим терористичним групам потужну та ефективну зброю, пристрій ретрансляції насильства або торгівлі людьми, через Інтернет мережі. Об'ктивно кібертероризм може проявлятися у формі незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж, викрадення комп'ютерної інформації, вимагання, організації атак на інформаційні ресурси, а також впровадження та розробки комп'ютерних вірусів з метою перехоплення, маніпулювання та знищення інформації. Аналіз сучасної кримінальної розвідки свідчить, що конкретно він проявляється у поширенні інформаційного тероризму, що становить серйозну зовнішню загрозу для України.

Підтверджуючи вище викладене, варто також додати, що кібертероризм проявляється у формі ретрансляції насильства, знущання над людьми, які потрапили під експлуатацію інших людей, або втягнення у злочинну діяльність, використання у збройних конфліктах тощо. Як про це зазнача у свому дослідженні Савенко В.П. [3].

Діяльність цього виду кібертероризму спрямована на використання форм і методів тимчасового або незворотного нанесення шкоди інформаційній інфраструктурі держави або її складових частин, а також на створення ситуацій з тяжкими наслідками для всіх сфер життєдіяльності особи, суспільства і держави, негативного сприйняття

суспільства шляхом протиправного використання інформаційних структур. У суспільстві з'являється новий вид терористичної діяльності – тероризм як сегмент населення [4, с. 13].

Враховуючи високий рівень небезпеки, яку цей вид тероризму становить для суспільства, ми вважаємо, що його слід розглядати як окрему структуру. Найбільш небезпечним видом кібертероризму, однак, є використання сучасних інформаційних технологій (насамперед, глобальної мережі Інтернет) як зброї для виведення з ладу критично важливих об'ктів енергетичної, транспортної або урядової інфраструктури країни. Загрози критичній інфраструктурі необхідно визначати не лише з точки зору можливостей та характеру їх джерел, але й з точки зору вразливих елементів критичної інфраструктури, які можуть бути об'ктом цих загроз (наприклад, фізичні елементи, зокрема обладнання та ресурси критичної інфраструктури, системи управління та зв'язку, зокрема автоматизовані системи управління та координації об'кту, та системи зв'язку) [5].

Цей тип атаки поєднує в собі підготовчий етап (дії зі створення нової вразливості на об'кті) та атаку (використання вразливості). При цьому підготовчі дії можуть передувати самій атаці із залученням співробітників компанії-мішені (інсайдерів) або проведенням різноманітних підривних дій. Тому необхідно встановити єдині кваліфікаційні вимоги до всіх категорій працівників, задіяних в обслуговуванні та доступі до об'ктів критичної інфраструктури, а також запровадити обов'язкову періодичну атестацію цих категорій працівників з метою забезпечення відповідності заявленим вимогам.

Аналіз сучасного стану інформаційної безпеки показує, що нормативно-правова база потребує вдосконалення. Необхідна також криміналізація кібертероризму, розробка нових засобів забезпечення інформаційної безпеки в публічному управлінні та постійний моніторинг нових загроз і небезпек в інформаційному середовищі. В умовах, коли злочинність проникла в глобальну мережу Інтернет і домінує в регулюванні суспільного та державного життя, існує нагальна потреба в побудові інформаційного суспільства та залученні України до світового інформаційного простору.

Список використаних джерел

1. Гнатюк С. О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. Безпека інформації. 2017. № 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 .

3. Окремі питання кримінальної відповідальності за торгівлю дітьми. Автори: Савенко, В.П. URL: http://er.dduvs.in.ua/handle/123456789/4407.

4. Коршунов В. О. Політичний тероризм: інформаційні методи боротьби: автореф. дис. … канд. політ. наук: 23.00.02. Дніпро, 2018. 18 с.

5. 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.

УДК 34.018:340.132.6:364.694:376

Щур Софія Олегівна,
курсант навчально-наукового інституту № 1 Національної академії внутрішніх справ, здобувач-координатор юридичної клініки «Захист»
ORCID: https://orcid.org/0009-0008-6397-4829;
Болістовська Діана Дмитрівна,
курсант навчально-наукового інституту № 1 Національної академії внутрішніх справ, здобувач-консультант юридичної клініки «Захист»;
Наумейко Анастасія Олександрівна,
студент навчально-наукового інституту № 1 Національної академії внутрішніх справ, здобувач-консультант юридичної клініки «Захист»
Науковий керівник:
Задорожна Анастасія Петрівна,
викладач кафедри цивільно-правових дисциплін Національної академії внутрішніх справ, кандидат юридичних наук, викладач-куратор юридичної клініки «Захист» навчально-наукового інституту № 1 Національної академії внутрішніх справ
ORCID: https://orcid.org/0000-0002-8681-1386

ПРАВОПРОСВІТНИЦЬКА ДІЯЛЬНІСТЬ ЮРИДИЧНОЇ КЛІНІКИ «ЗАХИСТ» ЗІ СЛУХАЧАМИ АВТОШКОЛИ ДЛЯ ОСІБ З ІНВАЛІДНІСТЮ

Міністерство внутрішніх справ України реалізує проєкт «Автошколи для осіб з інвалідністю» на базі автошкіл закладів вищої освіти із специфічними умовами навчання. Даний проєкт відбувається у межах ініціативи «Без бар'рів» Першої леді України Олени Зеленської. Завдяки реалізації даного проєкту державну послугу з навчання керування автомобілем та отримання посвідчення водія отримають люди з інвалідністю, в тому числі й набутої внаслідок війни [7].