ЧЕРНИШ Роман
кандидат юридичних наук,
співробітник Управління СБ України
в Житомирській області,
м.Житомир, Україна

ОСАУЛЕНКО Іван
співробітник Управління СБ України
в Житомирській області
м.Житомир, Україна

ЩОДО ОКРЕМИХ АСПЕКТІВ ПРОТИДІЇ ІНФОРМАЦІЙНОМУ ТЕРОРИЗМУ В СУЧАСНИХ УМОВАХ

Терористична діяльність як один із засобів досягнення протиправних цілей почала широко застосовуватися досить давно. Однак, починаючи з 90-х років XX століття, вона значно еволюціонувала, що пов'язано, перш за все, з надшвидким розвитком науково-технічного прогресу.

Зокрема, відбулася її інтеграція до інформаційного простору (кіберсфери). Інформаційний простір, за умови жорсткої міжнародної конкуренції, став головною ареною зіткнень і боротьби різновекторних національних інтересів держав. Насамперед, це пов'язано з тим, що сучасні інформаційні технології дають змогу державам реалізувати власні інтереси без застосування військової сили, послабити або завдати значної шкоди безпеці держави - протагоніста, яка не має дієвої системи захисту від негативних інформаційних впливів.

Зважаючи на викладене, особливу увагу дослідники приділяють інформаційному тероризму як новому виду терористичної діяльності, спрямованому на використання інформаційних технологій та засобів зв'язку з метою порушення належного функціонування чи знищення державних інфраструктур. Попри наявність численних наукових робіт, а також різноманітних наукових заходів, присвячених інформаційному тероризму, нині відсутнє уніфіковане бачення визначення поняття "інформаційний тероризм". Крім того, у сучасній юридичній науці немає системного ґрунтового бачення інформаційних правопорушень та, відповідно, наукових розробок щодо ефективної їм протидії [5].

Особливої актуальності досліджуване питання набуло в контексті ведення Російською Федерацією "гібридної війни" стосовно України. На жаль, розробка способів протидії вказаному виду злочинної діяльності значно відстає від потреб правоохоронної практики.

Окремі дослідники вважають, що інформаційний тероризм — це новий вид терористичної діяльності, орієнтований на використання різних форм і методів тимчасового або незворотного виведення з ладу інформаційної інфраструктури держави або її елементів, а також створення за допомогою протиправного використання інформаційної структури умов, що тягнуть за собою тяжкі наслідки для різних сторін життєдіяльності особистості, суспільства і держави [3, с. 6].

На нашу думку, інформаційний тероризм - це один із видів терористичної діяльності, в межах якої, шляхом використання сучасних інформаційних технологій (передусім, мережі Інтернет), здійснюється негативний вплив на належне функціонування відповідних державних інституцій.

Можна виділити такі основні ознаки вищевказаної протиправної діяльності:

- реалізується через засоби масової інформації та за допомогою мережі Інтернет (насамперед, профільних соціальних спільнот);
- є однією із форм організованого насильства;
- має на меті здійснення психологічного впливу на громадян (як окремих суб'єктів, так і широких верств населення);
- є особливим різновидом психологічного терору;
- публічний і демонстративний характер дій тощо.

Масове та досить швидке поширення інформаційного тероризму обумовлене широким запровадженням інформаційно-телекомунікаційних систем у всіх сферах життєдіяльності суспільства [2, с. 254].

Особливістю сучасного тероризму є активне застосування у якості важливого елемента маніпуляції інформаційно-психологічних технологій для впливу на людську свідомість та суспільну думку, з можливістю використання глобальних комунікацій. Такі дії терористів розраховані, в основному, на виклик своїми діями інформаційно-психологічного шоку серед великих мас, що має забезпечити таким чином досягнення зловмисниками своїх цілей. Вміло враховуючи здобутки інформаційної епохи та існування глобальних ЗМІ, терористи зробили своєю основною зброєю та інструментами впливу телебачення та кіберпростір [4].

На думку вчених, найбільшу небезпеку представляє саме кібертероризм — тероризм спланований, вчинений чи скоординований в кіберпросторі, тобто в терористичних акціях використовуються новітні досягнення науки і техніки в галузі новітніх інформаційних технологій [1, с. 13].

Як свідчать реалії сьогодення, протягом 2014-2016років для України значної актуальності набуло питання виявлення та блокування сепаратистських Інтернет-ресурсів, які використовуються представниками терористичних організацій так званих "ДНР/ЛНР", та особами, які їх підтримують, з метою поширення соціально небезпечної інформації, а також реалізації інших форм інформаційного тероризму. Вказані ресурси є інструментом пропаганди ідеології, що закликає до повалення конституційного ладу в Україні, відокремлення її територій, екстремізму та тероризму.

Основну небезпеку становить те, що вони негативно впливають на свідомість та підсвідомість громадян України та поступово її змінюють. Зазначене призводить до того, що особи, які піддалися впливу, у випадку інтервенції з боку держави-агресора (на прикладі анексії РФ території АР Крим та участі громадян України в бойових діях на Сході України в складі терористичних підрозділів) незважаючи на необхідність виконання конституційного обов'язку (захист територіальної цілісності), виступають на боці противника.

Водночас, занепокоєння викликає те, що представники спеціальних служб РФ активно використовують соціально орієнтовані ресурси мережі Інтернет для впливу на молодь з метою формування у них антигромадської позиції (недовіри до чинної влади, правоохоронних органів тощо), а також спонукання до вчинення

актів непокори чи інших протиправних дій, які можуть призвести як до дестабілізації суспільно-політичної ситуації всередині країни, так і до нанесення шкоди іміджу держави у сфері зовнішньополітичних відносин [6, с. 403].

За результатами аналізу встановлено, що найбільшого розмаху пропаганда сепаратистської інформації досягла на сторінках соціальної мережі "ВКонтакте". Другою, і не менш значущою за обсягом поширення сепаратистського контенту спільнотою є соціальна мережа "Одноклассники".

Підсумовуючи вищевикладене, керуючись необхідністю організації ефективної та дієвої протидії агресору (в т.ч. й в інформаційному просторі), вважаємо за доцільне на рівні відповідних профільних комітетів ВР України розглянути можливість внесення змін до:

- національного законодавства в частині передбачення механізму позбавлення громадянства за здійснення інформаційного тероризму, за аналогією з тим, як це зробили окремі європейські держави (зокрема Франція);
- Кримінального кодексу України в частині посилення кримінальної відповідальності за розповсюдження публічних закликів до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади, зокрема з використанням ресурсів мережі Інтернет;
- прийняття законопроекту, який дозволить на законних підставах на час проведення АТО за спрощеною процедурою (без обов'язкового отримання рішення суду) блокувати можливість перегляду на території України Інтернет-ресурсів, діяльність яких загрожує територіальній цілісності України та безпеці її громадян (не зважаючи на місце їх реєстрації чи фізичне розташування технічного обладнання).

Список використаних джерел:

1. Виявлення та розслідування злочинів, що вчиняються у сфері інформаційних технологій: Наук. -практ. посіб. /Б. М. Романюк, В. Д. Гавловський, М. В. Гуцалюк, В. М. Бутузов; За заг. ред. проф. Я. Ю. Кондратьева. — К. : Вид. ПАЛИВОДА А. В., 2004. — 144 с.

2. Кондратьєв Я. Ю. Тероризм: сучасний стан та міжнародний досвід боротьби : навчальний посібник [для студ. вищ. навч. закл.] / Я. Ю. Кондратьєв, В. В. Романюта. - К, 2005. - С. 254-257.

3. Коршунов В. О. Політичний тероризм: інформаційні методи боротьби: автореф. дис. на здобуття наук. ступеня канд. політ. наук: спец. 23.00.02 "Політична інститути та процеси"/Коршунов В. О. — Дніпропетровськ, 2008. — 18 с. 3

4. Кукса І. Інформаційний аспект тероризму та переговорний процес із терористами / І.Кукса // [Електронний ресурс]. – Режим доступу: http://mskod.com/informatsiyniy-aspekt-terorizmu-ta-peregovorniy-protses-iz-teroristami/. 4

5. Максименко Ю.Є. Інформаційний тероризм: актуальність чи данина моді? / Ю. Максименко // [Електронний ресурс]. – Режим доступу: http://goal-int.org/informacijnij-terorizm-aktualnist-chi-danina-modi/.

6. Черниш Р.Ф. Соціальні мережі, як спосіб деструктивного впливу спецслужбами Російської Федерації на свідомість молоді / Р. Черниш //Сучасні тенденції розбудови правової держави в Україні та світі : Зб. наук. ст. за матеріалами ІІІ Міжнар. наук.-практ. конф. (Житомир, 14 травня 2015 р.) – 544 с.