

УДК 342.95 :323.285

ТРОФІМОВ С.А., кандидат юридичних наук, доцент кафедри адміністративно-правових та кримінально-правових дисциплін Кримського юридичного інституту Національного університету “Юридична академія України імені Ярослава Мудрого”

ДЕСТРУКТИВНІ ХАРАКТЕРИСТИКИ ІНФОРМАЦІЙНИХ РЕСУРСІВ ЩОДО МОЖЛИВОСТІ ЇХ ВИКОРИСТАННЯ З ТЕРОРИСТИЧНОЮ МЕТОЮ

***Анотація.** Про сучасний стан використання деструктивних можливостей інформаційних ресурсів з терористичною метою та шляхи посилення безпеки соціуму в цьому аспекті.*

***Ключові слова:** терористична діяльність, протидія тероризму, послуги з надання хостингу, послуги з надання Інтернету, деструктивні характеристики інформаційних ресурсів, засоби масової інформації.*

***Аннотация.** О современном состоянии использования деструктивных возможностей информационных ресурсов с террористической целью и путях усиления безопасности социума в этом аспекте.*

***Ключевые слова:** террористическая деятельность, противодействие терроризму, услуги по предоставлению хостинга, услуги по предоставлению Интернета, деструктивные характеристики информационных ресурсов, средства массовой информации.*

***Summary.** About the modern consisting of the use of informative resources with a terrorist purpose and ways of strengthening of safety of sociuma of this aspect.*

***Keywords:** terrorist activity, counteraction to terrorism, services in the grant of hostingy, service in the grant of the Internet, destructive descriptions of informative resources, mass medias.*

Постановка проблеми. З інноваційним розвитком суспільства у геометричній прогресії зростає й потреба в інформації. В реаліях сьогодення інформація з об'єкта, що супроводжував розвиток суспільства на всіх етапах, перетворюється на потужний інструмент впливу на поведінку як представників окремої категорії людей, так і людства в цілому. Суспільство впродовж століть мало стійку тенденцію до вдосконалення технологій, якими все частіше користуються значна кількість його представників. З розвитком інформаційних технологій представники різних деструктивних напрямів намагаються використовувати такі технології із злочинною метою з максимальним ефектом для себе.

Окремими проблемами забезпечення антитерористичної діяльності в інформаційному аспекті у своїх наукових дослідженнях займалися І.В. Арістова, К.І. Беляков, В.В. Грибакін, В.В. Коноплев, О.В. Лукасевич, Т.А. Мартиросян, А.І. Марущак, В.Я. Настюк, О.В. Петришин, О.О. Погрібний, В.Г. Пилипчук, Г.П. Середа, Є.Д. Скулиш, Д.А. Соломін, Д.В. Сорокін, В.М. Цуканов та інші вітчизняні та іноземні науковці, але питанням можливості використання з терористичною метою інформаційних ресурсів приділялася недостатня увага.

Метою статті є окреслення деструктивних характеристик інформаційних ресурсів в аспекті можливості їх використання задля досягнення терористичних цілей та визначення шляхів зменшення негативного впливу на суспільство в даному вимірі.

Виклад основних положень. Слід зазначити, що одним з факторів, який має найбільший потенціал сучасного розвитку й можливого негативного ефекту для суспільства, є активне запровадження електронного управління різними технологічними

процесами, у тому числі системами водопостачання, каналізації, управління рухом (автомобільним, залізничним, авіаційним тощо) транспорту, безпеки виробництва й т.п. Необхідно погодитися, що так званий людський фактор інколи призводить до серйозних людських та матеріальних втрат, а можливості електронного управління процесами з кожним роком зазнають суттєвого розвитку, й можливість помилок з його боку майже не існує. Однак, з розвитком телекомунікаційних технологій, необхідно враховувати можливості зовнішнього втручання у систему електронного управління й спричинення суттєвої шкоди. Насамперед слід враховувати можливості названих систем управління з огляду на захищеність від можливих атак з боку терористів. Можна тільки уявити негативні наслідки виходу з ладу систем життєзабезпечення міста з кількістю жителів більше мільйона або систем безпеки управління повітряним рухом чи військовою зброєю.

Негативними прикладами такої діяльності лише за жовтень-листопад 2011 р. стали комп'ютерні втручання в електронні системи управління у США:

- електронну систему, яку використовують військові США для управління безпілотними літальними апаратами [1];

- електронну систему управління водонапірної станції у штаті Іллінойс [2].

Зацікавленість провідників тероризму щодо цієї сфери почала розвиватися на початку XXI сторіччя. Такий інтерес був обумовлений розвитком мережі Інтернет та активним запровадженням електронного управління різноманітними процесами. Слід підтримати позицію В.М. Цуканова, що дії, спрямовані на вивід з ладу електронно-обчислюваної техніки, автоматизованих систем управління, що знайшли своє застосування у банківській справі, управлінні повітряним рухом, космічних технологіях є надзвичайно небезпечними. Вивід з ладу комп'ютерних мереж може викликати хаос на національному й міжнародному рівнях [3, с. 33].

Якщо взяти за приклад один з сучасних найбільш резонансних проявів терористичної діяльності, якими є терористичні акти 22 липня 2011 року у Норвегії під час якого загинуло близько вісімдесяти осіб та біля ста отримали поранення[4], можна дійти висновку, що такий терористичний акт став можливий в тому числі й з причин неконтрольованого обігу товарів у мережі Інтернет. Зокрема, Андерс Беринг Брейвік (Anders Behring Breivik), який підозрюється у вчиненні цих терористичних актів придбав у мережі Інтернет поліцейську уніформу [5], що є незаконним, а також компоненти для виготовлення вибухового пристрою (хімікати, що використовуються у сільськогосподарській сфері) [6]. Все це він придбав в Інтернет-магазині або на сайтах популярних Інтернет-аукціонів, де можна придбати фактично все, навіть оснащення та предмети, що мають спеціальне призначення та виведені з цивільного обігу. Такий неконтрольований обіг товарів у мережі Інтернет має суттєвий потенціал, щодо використання у злочинних цілях, в тому числі й у терористичній діяльності.

Необхідно вказати на факт, що останнім часом правоохоронні органи різних країн світу стикаються з ситуацією, коли стає все більше осіб, які вчиняють різні форми прояву терористичної діяльності, але не мали спеціальної підготовки, що проводиться в місцях вишколу терористів. Як свідчить аналіз такої практики, це стає можливим завдяки вільному розміщенню на сайтах у мережі Інтернет відомостей щодо можливості створення різних типів вибухових речовин та пристроїв навіть у домашніх умовах. При цьому не потрібно фахової освіти хімічного чи військового спрямування. Так, якщо сформулювати пошуковий запит у найбільш популярній пошуковій системі Google у вигляді “как сделать бомбу в домашних условиях” [7], ми отримаємо близько 800 тисяч посилань на сторінки сайтів, з яких приблизно на половині пропонуються різні способи створення вибухових речовин чи пристроїв у домашніх умовах, а найбільш складні

способи супроводжуються демонструванням відеозаписів, де докладно пояснюється кожна стадія створення таких речовин чи пристроїв, у тому числі дається інформація, де можна придбати чи створити окремі компоненти. Безумовно, подальше безконтрольне наповнювання мережі Інтернет такого роду інформацією може призвести до жахаючих наслідків, адже напруження в будь-якій країні світу з огляду на різні соціально-економічні та політичні фактори має постійну тенденцію до зростання, що може мати наслідком масові заворушення, як це приміром було нещодавно у Великобританії [8], поєднані із використанням вибухових пристроїв.

Виходом із цієї ситуації, на нашу думку, вбачається співпраця правоохоронних органів України, насамперед Служби безпеки України, з операторами (провайдерами) Інтернет-послуг, тобто із суб'єктами підприємницької діяльності, які надають технічну можливість для виходу в мережу Інтернет. В даному випадку такі оператори (провайдери) Інтернет-послуг мають технологічні можливості обмеження доступу до певних сайтів за їх Інтернет-адресами. Було б доцільно, на нашу думку, поставити питання про надання компетенції щодо відстежування з боку Служби безпеки України сайтів, які можуть так чи інакше впливати на стан національної безпеки, складення відповідного переліку й ознайомлення з ним вітчизняних операторів (провайдерів) Інтернет-послуг, які у свою чергу будуть блокувати доступ до них з боку своїх користувачів.

Необхідно вказати, що спеціальні служби розвинених країн все більше уваги приділяють діяльності різного роду соціальних мереж, що дозволяє ефективно запобігати розвиненню злочинних планів або своєчасно отримувати інформацію про подальший розвиток подій. Такими позитивними прикладами можна визнати факт засудження до чотирьох років позбавлення волі судом у британському місті Честер двох молодих людей – 20-річного Джордана Блекшоу й 22-річного Перрі Ситклифф-Кінана, які створили у соціальній мережі Facebook дві групи, в яких закликали до масових заворушень та мародерства із вказівкою часу й місць зборів [9], та затримання 17-літнього підлітка, який розміщував у соціальних мережах повідомлення про намір здійснити вибух у Варшаві. У переписці з іншими користувачами підліток посилався на терористичні акти 22 липня 2011 року у Норвегії й порівнював свої плани із вчинками Андерса Беринга Брейвіка. Такими висловлюваннями зацікавилася німецьке відділення Інтерполу, оскільки одним з тих, з ким спілкувався підліток з Польщі, був громадянин Німеччини. Інтерпол передав оперативні дані в польську поліцію, яка й заарештувала підлітка [10].

На фоні означених вище сучасних проблем у використанні інформаційних технологій у злочинних цілях доволі застарілими виглядають порушення з боку головних редакторів, а також окремих авторів програм чи передач встановленого законодавством порядку інформування громадськості про терористичний акт. Отже, свій негативний вклад у розвиток тероризму вносять засоби масової інформації, які при висвітленні тих чи інших актів тероризму розкривають відомості про сили та засоби, що залучаються до проведення антитерористичної операції, їх технічні можливості, тактику проведення операції, “прикрашають” факти щодо кількості жертв, розмаху вчинення акту тероризму, невідповідності та непрофесіоналізму суб'єктів протидії тероризму й т. п. Таким чином у суспільстві створюється обстановка страху, неминучості стати наступною жертвою тероризму, відчуття неможливості отримання захисту з боку органів влади тощо. Саме це, як правило, є стратегічною метою провідників тероризму. Окрім цього, завдяки діяльності засобів масової інформації формується авторитет терористичної організації, що відбивається на її фінансуванні, отже, провідники тероризму зацікавлені у якомога гучнішому висвітленні подій та результатів своїх актів тероризму.

Необхідно зазначити, що відповідно до положень Конвенції про захист прав людини і основоположних свобод від 04.11.50 р. [11], а саме статті 10, кожен має право на свободу вираження поглядів. Це право включає свободу дотримуватися своїх поглядів, одержувати і передавати інформацію та ідеї без втручання органів державної влади і незалежно від кордонів. Однак, здійснення цих свобод, оскільки воно пов'язане з обов'язками і відповідальністю, може підлягати таким формальностям, умовам, обмеженням або санкціям, що встановлені законом і є необхідними в демократичному суспільстві в інтересах національної безпеки, територіальної цілісності або громадської безпеки, для запобігання заворушенням чи злочинам, для охорони здоров'я чи моралі, для захисту репутації чи прав інших осіб, для запобігання розголошенню конфіденційної інформації або для підтримання авторитету і безсторонності суду. Отже, є всі підстави для запровадження у національному законодавстві особливого режиму висвітлення подій актів тероризму, а також інформації щодо проведення антитерористичних операцій та державної стратегії протидії тероризму. На жаль, процеси демократизації суспільства разом із суттєвим позитивним ефектом тягнуть за собою й розвиток певних негативних явищ, в тому числі й тероризму.

На нашу думку, необхідно встановити відповідні нормативні правила щодо порядку висвітлення антитерористичної операції у ст. 6 Закону України “Про телебачення і радіомовлення” від 21.12.93 р. № 3759-ХІІ [12] та ст. 3 Закону України “Про друковані засоби масової інформації (пресу) в Україні” від 16.11.92 р. № 2782-ХІІ [13], які встановлюють неприпустимість зловживання свободою діяльності телерадіоорганізацій та друкованих засобів масової інформації.

Висновки.

Проведений нами аналіз сучасної практики діяльності правоохоронних органів різних країн дає підстави стверджувати про поступову зміну театру взаємодії злочинців та співробітників правоохоронних органів. Безпосередня взаємодія цих суб'єктів має тенденцію до зменшення, переходу злочинців у “віртуальний світ”, який надає набагато більше можливостей для злочинних дій, а масштаб діяльності фактично необмежений. Інформаційні ресурси, окрім названих переваг для злочинців, дають їм можливість залишати набагато менше матеріальних слідів. Отже, боротьба із злочинними проявами в інформаційній сфері набагато складніша. Негативним фактором для розвитку злочинної діяльності в даному випадку також є недостатня технічна оснащеність правоохоронних органів й відсутність у більшості їх співробітників навичок роботи у цій сфері та низька технологічна грамотність порівняно із представниками кримінального світу. Відпрацьована практика діяльності співробітників правоохоронних органів є запорукою ефективної боротьби із злочинними проявами, а сфера, що нами розглядається, є ще недостатньо вивченою вітчизняними правоохоронцями.

Зазначимо, що подальше вивчення деструктивних характеристик інформаційних ресурсів в аспекті можливості їх використання задля досягнення терористичних цілей надасть теоретичний й практичний матеріал для діяльності правоохоронних органів України, які на відміну від правоохоронних органів інших держав ще знаходяться на стадії технологічного становлення та розвитку, отже, потребують концептуальних орієнтирів для своєї правоохоронної діяльності.

Використана література

1. Компьютерный вирус поразил систему управления беспилотниками в США: – Режим доступа : [//www.bezpeka.com/ru/news/2011/10/10/drone-virus.html](http://www.bezpeka.com/ru/news/2011/10/10/drone-virus.html)

2. Российские хакеры атаковали систему управления инфраструктурой США. – Режим доступа : [//www.voanews.com/russian/news/cyber-attack-illinois-russia-134187998.html](http://www.voanews.com/russian/news/cyber-attack-illinois-russia-134187998.html)
3. Цуканов В.Н. Административно-правовые основы деятельности милиции по предупреждению и пресечению террористических актов (на материалах деятельности служб и подразделений милиции общественной безопасности) : дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.14 / В.М. Цуканов. – Омск, 2006. – 226 с.
4. Теракты в Норвегии (2011). – Режим доступа : [//www.ru.wikipedia.org/wiki/%D0%A2%D0%B5%D1%80%D0%B0%D0%BA%D1%82%D1%8B_%D0%B2_%D0%9D%D0%BE%D1%80%D0%B2%D0%B5%D0%B3%D0%B8%D0%B8_\(2011\)](http://www.ru.wikipedia.org/wiki/%D0%A2%D0%B5%D1%80%D0%B0%D0%BA%D1%82%D1%8B_%D0%B2_%D0%9D%D0%BE%D1%80%D0%B2%D0%B5%D0%B3%D0%B8%D0%B8_(2011))
5. Slik skaffet han polituniformen. – Режим доступа : [//www.nrk.no/nyheter/norge/1.7725557](http://www.nrk.no/nyheter/norge/1.7725557)
6. “Пособник из Польши” стал свидетелем по делу норвежского террориста. – Режим доступа : [//www.lenta.ru/news/2011/07/25/polen1](http://www.lenta.ru/news/2011/07/25/polen1)
7. Как сделать бомбу в домашних условиях. – Режим доступа : [//www.google.com.ua/#scli ent=psy&hl=ru&source=hp&q=%D0%BA%D0%B0%D0%BA+%D1%81%D0%B4%D0%B5%D0%BB%D0%B0%D1%82%D1%8C+%D0%B1%D0%BE%D0%BC%D0%B1%D1%83+%D0%B2+%D0%B4%D0%BE%D0%BC%D0%B0%D1%88%D0%BD%D0%B8%D1%85+%D1%83%D1%81%D0%BB%D0%BE%D0%B2%D0%B8%D1%8F%D1%85&aq=f&aqi=g1&aql=f&oq=&pbx=1&fp=e2c88aff5a829102&biw=1280&bih=856](http://www.google.com.ua/#scli ent=psy&hl=ru&source=hp&q=%D0%BA%D0%B0%D0%BA+%D1%81%D0%B4%D0%B5%D0%BB%D0%B0%D1%82%D1%8C+%D0%B1%D0%BE%D0%BC%D0%B1%D1%83+%D0%B2+%D0%B4%D0%BE%D0%BC%D0%B0%D1%88%D0%BD%D0%B8%D1%85+%D1%83%D1%81%D0%BB%D0%BE%D0%B2%D0%B8%D1%8F%D1%85&aq=f&aqi=g1&aql=f&oq=&pbx=1&fp=e2c88aff5a829102&biw=1280&bih=856)
8. Массовые беспорядки в Великобритании подорвали доверие к экономической модели Соединенного Королевства. – Режим доступа : [//www.itar-tass.com/c137/201913.html](http://www.itar-tass.com/c137/201913.html)
9. В Британии вынесены первые жесткие приговоры за беспорядки: четыре года за призывы в Facebook. – Режим доступа : [//www.gazeta.ru/news/lenta/2011/08/17/n_1969445.shtml](http://www.gazeta.ru/news/lenta/2011/08/17/n_1969445.shtml)
10. В Польше задержан юный последователь норвежского террориста Брейвика. – Режим доступа : [//www.news.mail.ru/incident/6617148/?frommail=1](http://www.news.mail.ru/incident/6617148/?frommail=1)
11. Конвенція про захист прав людини і основоположних свобод від 04.11.1950 р. // Офіц. вісник України. – 1998. – № 13. – С. 270.
12. Про телебачення і радіомовлення : Закон України від 21.12.93 р. № 3759-ХІІ // Відомості Верховної Ради України. – 1994. – № 10. – Ст. 43.
13. Про друковані засоби масової інформації (пресу) в Україні : Закон України від 16.11.92 р. № 2782-ХІІ // Відомості Верховної Ради України. – 1993. – № 1. – Ст. 1.

~~~~~ \* \* \* ~~~~~