

УДК 343.7

1.18. Современные информационные инструменты противодействия распространению террористических угроз в сети интернет

©Шогенов Тимур Мухамедович

Северо-Кавказский институт повышения квалификации (филиал)
Краснодарского университета МВД России, г.Нальчик, КБР, Россия
tima0301977@gmail.com

Аннотация

В статье рассмотрены актуальные проблемы противодействия террористическим угрозам, которые в процессе глобализации и информатизации общества переместились в сетевое пространство и стали следствием такого явления как кибертерроризм. Автором отмечено, что особую опасность злонамеренная кибердеятельность несет в периоды дестабилизации, что наблюдается сегодня, когда злоумышленники активно эксплуатируют возникшую в связи с пандемией нестабильность и панические настроения в обществе и наживаются на глобальном кризисе. Приведены новые виды террористических угроз в глобальной сети, связанных с пандемией коронавируса и меры, предпринимаемые государствами для их отражения.

Ключевые слова: террористические угрозы, кибертерроризм, киберпреступность, терроризм, пандемия коронавируса, сеть Интернет, глобальное информационное пространство.

Для цитирования: Шогенов Т.М. Современные информационные инструменты противодействия распространению террористических угроз в сети Интернет // Пробелы в российском законодательстве. 2020. Т. XIII. №4. С. 094-097.

Modern information tools to counter the spread of terrorist threats on the internet

©Shogenov Timur Mukhamedovich

North Caucasus Institute for Advanced Studies (branch)
of the Krasnodar University of the Ministry of Internal Affairs of Russia, Nalchik, Russia
tima0301977@gmail.com

Abstract

The article deals with current problems of countering terrorist threats, which in the process of globalization and informatization of society have moved to the network space and have become a consequence of such a phenomenon as cyberterrorism. The author notes that malicious cyber activity is particularly dangerous during destabilization periods, what is observed today, when hackers actively exploit the instability and panic in society that arose in connection with the pandemic and they profit from the global crisis. New types of terrorist threats in the global network related to the coronavirus pandemic and measures taken by states to address them are presented.

Keywords: terrorist threats, cyberterrorism, cybercrime, terrorism, coronavirus pandemic, Internet, global information space.

For citation: Shogenov T.M. Modern information tools to counter the spread of terrorist threats on the Internet // Gaps in Russian legislation. 2020. Vol. XIII. №4. Pp. 094-097. (in Russ.).

Введение. Постановка проблемы

На современном этапе обеспечение информационной безопасности государства является приоритетной составляющей ее национальной безопасности. Киберпространство, возникшее в результате развития информационно-коммуникационных технологий, предоставило безграничные возможности и преобразило повседневную жизнь не только законопослушных граждан, но и преступных сообществ и групп, а также отдельных криминальных элементов. Об актуальности проблемы свидетельствует обширный перечень возможных способов совершения компьютерных преступлений. Согласно одной из наиболее общих классификаций выделяются следующие криминологические группы компьютерных преступлений: экономические преступления; преступления против личных прав и частной сферы; преступления против государственных и общественных интересов [6]. К последней категории относятся преступления террористического характера,

совершаемые в информационном пространстве. Организаторы и члены террористических групп активно используют в своих преступных целях процесс глобализации [10]. Беря на вооружение современные информационные технологии, преступники становятся менее уязвимыми для правоохранительных органов. В основу построения современных террористических групп ставится принцип сетевой структуры, обеспечивающий единые центры и информационно-коммуникативные каналы. Террористы активно эксплуатируют возможности глобального информационного пространства, в том числе, мультимедийность среды, позволяющей интегрировать различные типы информации: текстовую, графическую, аудио-визуальную в целях устрашения и запугивания простых людей. Сегодня все активно действующие террористические организации обладают собственными интернет-сайтами в сети Интернет. Особую активность в глобальном информационном пространстве по заявлению секретаря Совета

безопасности России Николая Патрушева проявляют террористические и экстремистские организации на Юге России. В 2019 году из 460 тысяч поданных обращений об обнаружении противоправной информации террористической и экстремистской направленности в сети Интернет около 88 тысяч интернет-сайтов по решению суда было заблокировано на Юге России [7]. По данным МВД [5], в 2019 году на 25 % выросло число зарегистрированных преступлений по ст. 205.2 УК РФ [8] (публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма), совершенных с использованием информационно-телекоммуникационных сетей.

Основные положения работы

Важность и актуальность проблем противодействия распространению террористических угроз в сети Интернет подтверждается тем, что исследования в этой области активно проводятся не только отдельными учеными [1, 2, 9, 11], но и исследовательскими группами ряда аналитических центров ведущих мировых держав [4].

Согласно выводам, сделанным в процессе проведенных исследований, были разработаны следующие положения новой геополитической концепции:

– глобальная информатизация всех сфер жизнедеятельности общества приводит к снижению степени его безопасности;

– современный терроризм трансформируется в информационную технологию особого типа, в силу следующих причин: террористы все шире используют возможности глобального пространства для связи и сбора информации; «кибертерроризм» сегодня стал реальностью наших дней; большинство террористических актов в наши дни рассчитаны на информационно-психологический шок, воздействие которого на большие массы людей создает благоприятную обстановку для достижения террористами своих целей;

– рост достижений науки и техники повышает вероятность использования террористами субгубо мирных технологий в качестве средств поражения.

Таким образом, в современных условиях глобализации и формирования информационного общества терроризм стал выступать в качестве самостоятельного фактора, способного угрожать государственной целостности стран и дестабилизировать международную обстановку. Помимо этого, преступники увеличивают масштабы и методы террористических действий, расширяют их географию.

Особую озабоченность ростом киберпреступности, в том числе распространением террористических угроз в сети Интернет, специалисты в области информационной безопасности высказывают сегодня, когда планета охвачена пандемией коронавируса. В то время как мир борется с распространением эпидемии, злонамеренная кибердеятельность может нанести смертельную опасность. Ведь злоумышленники уже активно эксплуатируют возникшую в связи с пандемией нестабильность и панические настроения в обществе. К примеру, вредоносные домены, посвященные коронавирусу, уже исчисляются десятками тысяч и даже взломанные роутеры пугают своих владельцев именно срочной информацией о пандемии. Кибертеррористами активно внедряется в массовое сознание так называемая «теория заговора», согласно которой пандемия коронавируса организована заинтересованными мировыми

силами. Их цель – загнать людей в резервации, а в дальнейшем провести «чипирование» и «зомбирование» населения при помощи 5G-связи. Распространителями данных мифов становятся обычные граждане, которые пытаются «открыть людям глаза», распространяют «разоблачающие» ролики в социальных сетях. Собирая в глобальной сети миллионы просмотров, данные ролики сеют панику и страх среди населения, приводят к совершению противоправных действий. Так, серия нападений, совершенных активистами борьбы с «чипированием» началась с Европы. В Великобритании к середине апреля было сожжено почти 50 базовых станций мобильной 5G-связи. Как убеждены британцы, излучение станций негативно сказывается на иммунитете людей, вследствие чего повышается риск заражения коронавирусом и растет скорость его распространения среди населения [12]. Волна поджогов вышек 5G-связи пронеслась не только по Великобритании, но и охватила другие страны: зафиксированы случаи в Нидерландах, Франции, Бельгии, Ирландии, Кипре, России [3]. Как заявил Глава республики Северной Осетии В. Битаров, активисты небольшого селения республики под названием Ногир устроили поджог базовой станции мобильной связи, обосновав свои противоправные действия тем, что они не верят в существование коронавируса и боятся внедрения 5G [12]. При этом приверженцы обозначенной теории не ограничиваются только поджогами, в Великобритании имеются факты как словесных угроз сотрудникам телекоммуникационных компаний, так и физического нападения на них.

Таким образом, глобальная сеть Интернет, являясь на современном этапе главным источником информации, активно используется злоумышленниками для распространения террористических угроз, заключающихся в распространении слухов и домыслов о коронавирусе, ведущих к нарастанию тревожности и паники в обществе, угрожающих национальной и международной безопасности. Только в апреле число ложных интернет-сообщений составило почти четыре тысячи [3].

Многими государствами экстренно приняты меры, направленные на противодействие распространению в глобальной сети общественно-опасной информации. В РФ с апреля 2020 года были ужесточены меры за распространение фейков с административной до уголовной ответственности. Аналогичная мера была принята властями Китая еще в начале марта, в итоге сотни пользователей сети в КНР вылапали штрафы, а многие попали за решетку. Путем законодательного ограничения граждан от лживой информации пошли Иран, Саудовская Аравия, Египет, Турция и ряд стран на Балканском полуострове [3]. Озабочены фейками о коронавирусе и задумываются о принятии правовых мер и во многих других странах, которыми пока не введена ответственность за распространение ложной информации.

Заключение

На данном этапе, когда наблюдается резкий рост числа киберугроз, в том числе и террористического характера, связанных с пандемией коронавируса, все мировые державы обеспокоены обеспечением кибербезопасности глобального информационного пространства. Для этого, как отмечают специалисты в данной области, должны быть определены следующие три аспекта: информационно-правовой, предполагаю-

щий наличие соответствующей нормативной базы в сфере информационной безопасности личности, общества и государства; информационно-технический, обеспечивающий защиту информационной сферы от несанкционированного доступа, хакерских атак и дру-

гих несанкционированных воздействий на компьютерные сети; информационно-психологический, который определяет психологическую защиту человека от негативного информационного воздействия.

Список литературы:

1. Бураева Л.А. Информационный терроризм как угроза национальной безопасности Российской Федерации // Пробелы в российском законодательстве. – 2016. – № 6. – С. 139-141.
2. Гаужаева, В.А. Особенности профилактики терроризма органами внутренних дел / В.А. Гаужаева, А.М. Шамаев. // Материалы Международной научно-практической конференции. Под общей редакцией В.А. Сосова. –2017. – С. 147-153.
3. Интернет заполнили лживые и опасные слухи о коронавирусе. Как с ними бороться? [Электронный ресурс]. – Режим доступа: <https://lenta.ru/articles/2020/05/08/fakes/> (дата обращения 08.05.2020).
4. Киберпространство и информационный терроризм. [Электронный ресурс]. – Режим доступа: <http://scienceport.ru/news/kiberprostranstvo-i-informatsionny-terrorizm/> (дата обращения 06.05.2020).
5. МВД: число дел об оправдании терроризма в интернете в 2019 году выросло на четверть. [Электронный ресурс]. – Режим доступа: <https://www.sova-center.ru/racism-xenophobia/news/counteraction/2020/01/d41996/> (дата обращения 06.05.2020).
6. Минаев С.В. Компьютерные преступления: сущность, особенности и возможности предотвращения. [Электронный ресурс]. – Режим доступа: <https://cyberleninka.ru/article/n/kompyuternye-prestupleniya-suschnost-osobennosti-i-vozmozhnosti-predotvrascheniya> (дата обращения 06.05.2020).
7. Патрушев: На юге РФ заблокировано около 88 тысяч экстремистских сайтов. [Электронный ресурс]. – Режим доступа: <https://rg.ru/2019/09/13/reg-ufo/patrushev-na-iuge-rf-zablokirovano-okolo-88-tysiach-ekstremistskih-sajtov.html> (дата обращения 06.05.2020).
8. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 07.04.2020) (с изм. и доп., вступ. в силу с 12.04.2020). [Электронный ресурс]. – СПС «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 06.05.2020).
9. Шогенов Т.М. Об актуальных вопросах противодействия кибертерроризму // Пробелы в российском законодательстве. – 2019. – № 2. – С. 155-157.
10. Шогенов Т.М. Терроризм в условиях глобализации. Кибертерроризм // Социально-политические науки. –2018. – № 3. – С. 181-182.
11. Шхагапсоев З.Л. Об актуальных вопросах международного сотрудничества в противодействии проявлениям экстремизма и терроризма в интернет-пространстве / З.Л. Шхагапсоев, Бураева Л.А. // Пробелы в российском законодательстве. – 2018. – № 5. – С. 251-254.
12. Эпидемия поджогов вышек сотовой связи перерастает в пандемию? [Электронный ресурс]. – Режим доступа: <https://nag.ru/articles/article/106904/epidemiya-podjogov-vyishek-sotovoy-svyazi-pererastaet-v-pandemiyu-.html> (дата обращения 06.05.2020).

References:

1. Buraeva L. A. Information terrorism as a threat to the national security of the Russian Federation // Gaps in Russian legislation. -2016. - no. 6. - P. 139-141.
2. Gauzhayeva, V. A. Features of prevention of terrorism by internal Affairs bodies / V. A. Gauzhayeva, a.m. Shamaev. // Materials of the International scientific and practical conference. Under the General editorship Of V. A. Sosov. -2017. - Pp. 147-153.
3. The Internet is filled with false and dangerous rumors about the coronavirus. How to deal with them? [Electronic resource]. - Access mode: <https://lenta.ru/articles/2020/05/08/fakes/> (accessed 08.05.2020).
4. Cyberspace and information terrorism. [Electronic resource]. - Access mode: <http://scienceport.ru/news/kiberprostranstvo-i-informatsionny-terrorizm/> (accessed 06.05.2020).
5. Ministry of internal Affairs: the number of cases of justifying terrorism on the Internet in 2019 increased by a quarter. [Electronic resource].- Access mode: <https://www.sova-center.ru/racism-xenophobia/news/counteraction/2020/01/d41996/> (accessed 06.05.2020).
6. Minaev S. V. Computer crimes: essence, features and possibilities of prevention. [Electronic resource]. - Access mode: <https://cyberleninka.ru/article/n/kompyuternye-prestupleniya-suschnost-osobennosti-i-vozmozhnosti-predotvrascheniya> (accessed 06.05.2020).
7. Patrushev: about 88,000 extremist websites have been blocked in the South of the Russian Federation. [Electronic resource]. - Access mode: <https://rg.ru/2019/09/13/reg-ufo/patrushev-na-iuge-rf-zablokirovano-okolo-88-tysiach-ekstremistskih-sajtov.html> (acced 06.05.2020).
8. The criminal code of the Russian Federation of June 13, 1996 No. 63-FZ (ed. from 07.04.2020) (with amendments. and add., Intro. effective from 12.04.2020). [Electronic resource].- SPS "ConsultantPlus".- Access mode: http://www.consultant.ru/document/cons_doc_LAW_10699/ (accessed 06.05.2020).
9. Shogenov T. M. "On topical issues of countering cyberterrorism" // Gaps in Russian legislation, 2019, no. 2, Pp. 155-157.
10. Shogenov T. M. Terrorism in the context of globalization. Cyberterrorism // Socio-political Sciences. -2018. - № 3. - P. 181-182.
11. Shkhagapsoev Z. L. on topical issues of international cooperation in countering manifestations of extremism and terrorism in the Internet space / Z. L. Shkhagapsoev, Buraeva L. A. // Gaps in Russian legislation. 2018. N. 5. Pp. 251-254.
12. Is the Epidemic of burning cell towers turning into a pandemic? [Electronic resource]. - Access mode: <https://nag.ru/articles/article/106904/epidemiya-podjogov-vyishek-sotovoy-svyazi-pererastaet-v-pandemiyu-.html> (accessed 06.05.2020).

Рецензия

на статью «Современные информационные инструменты противодействия распространению террористических угроз в сети Интернет», подготовленную заместителем начальника кафедры деятельности ОВД в особых условиях СКИ (ф) КрУ МВД России Т.М. Шогеновым

В статье, представленной на рецензирование, рассмотрены актуальные проблемы противодействия террористическим угрозам, которые в результате развития информационно-коммуникационных технологий и информатизации общества переместились в глобальное информационное пространство и стали следствием такого явления как кибертерроризм. Автором отмечено, что киберпреступники увеличивают масштабы и методы террористических действий, расширяют их географию.

В статье исследованы современные тенденции роста киберпреступности, в том числе, связанные с пандемией коронавируса, когда злоумышленники активно эксплуатируют возникшую в связи с распространением инфекции нестабильность и панические настроения в обществе. Приведены меры, предпринимаемые государствами для отражения террористических угроз в глобальной сети.

Считаю, что в статье «Современные информационные инструменты противодействия распространению террористических угроз в сети Интернет», представленной Т.М. Шогеновым рассматриваются достаточно актуальные на сегодня проблемы и она может быть рекомендована к опубликованию.

Начальник кафедры специальных дисциплин Северо-Кавказского института повышения квалификации (филиал) Краснодарского университета МВД России, к.ю.н., полковник полиции М.М. Ардавов

Статья прошла проверку системой «Антиплагиат»; оригинальность текста – 85,75%

СВЕДЕНИЯ ОБ АВТОРЕ

Шогенов Тимур Мухамедович, канд. экон. наук, заместитель начальника кафедры деятельности ОВД в особых условиях Северо-Кавказского института повышения квалификации (филиал) Краснодарского университета МВД России. РИНЦ: 6219-1069. E-mail: tima0301977@gmail.com

ABOUT THE AUTHOR

Shogenov Timur Mukhamedovich, PhD (Econ), Senior lecturer, North-Caucasian Advanced Training Institute (branch) of the Krasnodar University of the Ministry of Internal Affairs of Russia. Author ID: 6219-1069. E-mail: tima0301977@gmail.com