ПРОТИВОДЕЙСТВИЕ ТЕРРОРИСТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ В СЕТИ ИНТЕРНЕТ

Моторкин Владислав Владимирович

магистрант, Международный юридический институт, РФ, г. Москва

COUNTERING TERRORIST ACTIVITIES ON THE INTERNET

Vladislav Motorkin

Master's degree, International Law Institute, Russia, Moscow

Аннотация. В данной статье рассмотрены актуальные проблемы, связанные с распространением террористической идеологии в сети «Интернет». Выявлены закономерности усиления террористической пропаганды с развитием информационного общества, показаны правовые аспекты борьбы с распространением «кибертерроризма». В заключении статьи указываются пробелы в области борьбы с терроризмом, а также предлагаются пути усовершенствования методов противодействия терроризму.

Abstract. This article looks at the current problems associated with the spread of terrorist ideology on the Internet. The patterns of strengthening terrorist propaganda with the development of the information society have been revealed, and the legal aspects of combating the spread of "cyberterrorism" have been shown. Domestic and international sources of legal regulation of the fight against terrorism are reflected and analyzed. The article concludes with a list of gaps in the fight against terrorism, as well as proposed ways to improve counter-terrorism methods.

Ключевые слова: Противодействие терроризму, Кибертерроризм, Даркнет, Интернет.

Keywords: Countering Terrorism, Cyberterrorism, Darknet, the Internet.

В конце XX-го века мир перешёл в эру цифровых технологий, которая задала новый вектор развития и позволила миру выстраивать коммуникацию между всеми континентами и государствами. В 1991 г. появилась «Всемирная паутина» или «Глобальная сеть» (англ. World Wide Web Project). Но рубеж XX-го и XXI-го веков дал не только рассвет новым информационным технологиям, он ознаменовался появлением на международной карте такого явления как Терроризм. И уже в конце 1990-х, начале 2000-х гг., террористические организации стали стремительно осваивать сеть «Интернет» для использования её в качестве инструмента для достижения своих преступных целей. Так в своём докладе Габриель Вайман поясняет, что к 1998 г. половина из тридцати террористических организаций, запрещенных в США имели веб-сайты, а уже к 2000 г. ряды web-участия пополнили и практически все остальные террористические группы, внесенные в тот же список[1]. В России в тот же временной период террористические группировки, расположенные и ведущие террористическую деятельность на территории Северного Кавказа успешно выкладывали в сеть своеобразные отчеты о проведенных боевых операциях, пропагандистскую информацию,

а также личные обращения к гражданам, и властям. К 2000-му году «объем Интернета» достиг чуть более 17 млн. ресурсов (web-сайтов) и 413,4 млн. пользователей, а к 2014-му году Интернет «вырос» до показателей в 968,8 млн. ресурсов и 2,92 млрд. пользователей, и на сегодняшний день по разным оценкам насчитывается уже более 1 млрд. ресурсов сети Интернет и более 3,8 млрд. пользователей по всему миру[2].

Соответственно с таким быстрым темпом развития сети интернет, свою нишу в нём заняли и террористические организации освоив все современные цифровые технологии, и методы ведения «информационной войны». И если на стыке XX-XXI вв. проникновения терроризма в «Глобальную сеть» не принималось всерьёз мировым сообществом и отдельными странами, то уже к 2010 г. терроризм прочно укоренился в Интернете, и освоив эту нишу, ознаменовал волну новых методов ведения Террора. Так прибегая к сравнительному анализу можно выявить следующую закономерность – «Количество террористических организаций, ведущих деятельность в сети Интернет, и их ежегодно повышаемая активность, совпадает с взлетом популярности и укоренением среди различных слоёв населения сети Интернет».

В своей работе Жаворонкова Т.В. отмечает, что для своих сайтов модераторы террористических организаций все больше используют методы подачи информации присущие СМИ, такие как: подача материала полученного якобы от «независимого» источника, цитирование «документов», заголовки с «сенсационным» характером, специально подобранные фотографии и рисунки и т.д.[3] Указанная выше свидетельствует о выходе террористических организаций на «новый» уровень ведения пропагандистской деятельности, направленной на проявление у пользователей сети Интернет интереса, симпатии, лояльности к ресурсам террористического характера и террористической деятельности. С вышеуказанной позицией невозможно не согласиться. Апогеем «кибертерроризма» на наш взгляд, стал выпуск в 2015 г. ролика «Скоро, очень скоро», организацией ИГИЛ («ИГИЛ», террористическая группировка, деятельность которой запрещена в России, – прим. ред.), запрещенной в РФ. Ролик содержал в себе сцены человеческих казней, способные вызвать у человека психическое расстройство, панику, страх, видео было смонтировано профессионально, а в тексте звукового сопровождения была выражена угроза России, и её жителям. За несколько дней видеоролик увидели миллионы людей по всему миру, и он вызвал огромный общественный резонанс как в России, так и за рубежом. Так как основной задачей террористов является распространение и нагнетание страха среди населения всего мира[4], то реакция общественности показала, что такие методы «кибертерроризма» эффективны, и могут за короткое время создать общественный резонанс и посеять страх среди общества.

В настоящий момент мировое сообщество борется с распространением террористических и экстремистских идей в сети Интернет. Об этом говорит разработка ООН Глобальной контртеррористической стратегии в 2006 г., в которой одним из пунктов отнесенных к методам борьбы с терроризмом предлагается использовать сеть Интернет в качестве инструмента борьбы с распространением терроризма[5]. Так же проблеме распространения терроризма в сети посвящен Доклад Управления ООН по наркотикам и преступности от 2013 г., в котором достаточно подробно рассматривается история вопроса, методы осуществления кибертерроризма, но самым главными на наш взгляд являются пункты доклада посвященные методам противодействия распространению терроризма в сети Интернет, выявления террористических угроз, расследования террористических преступлений, что создает методическую базу доступную для правоохранительных органов стран мирового сообщества[6].

В отечественном праве борьба с распространением терроризма в сети Интернет получила закрепление в Уголовном кодексе РФ в частности квалифицированный состав ст. 205.2 УК РФ (ч.2) содержит санкцию за Публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганду терроризма совершенные с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей, в том числе сети "Интернет" закрепляет[7]. Так же в положениях Закона «О средствах массовой информации» от 27.12.1991 г. № 2124-1 отечественный законодатель закрепляет принцип недопустимости злоупотребления свободой массовой информации, который выражается в недопущении использования средств массовой информации в целях совершения уголовно-наказуемых деяний, а также для распространения материалов, содержащих публичные призывы к осуществлению террористической

деятельности или публично оправдывающих терроризм[8]. Из практического применения правового противодействия терроризму следует отметить деятельность Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее – Роскомнадзор), которая в соответствии со своими полномочиями осуществляет государственный контроль и надзор в сфере СМИ (в том числе и сети Интернет). Грамотным шагом следует признать размещение на сайте Роскомнадзора формы с пояснением о блокировке интернет-ресурсов, а также форме обратной связи для сообщения о материалах террористического и экстремистского характера, распространяемых в сети интернет[9]. Также Роскомнадзором ведётся Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено, в который и попадают сайты, распространяющие и содержащие экстремистскую и террористическую идеологию. Так же следует отметить ведение Федерального списка экстремистских материалов Министерством Юстиции РФ, в котором на сегодняшний день находится 4920 позиций. Таким образом можно сделать вывод, что отечественный законодатель ведёт активную борьбу с терроризмом в сети Интернет, и учитывает общественную опасность данного явления.

Но с недавнего времени открылся новый фронт распространения террористической идеологии называемый «Darknet». Эта сеть, где сайты и пользователей практически невозможно обнаружить, так как вся информация о них, в том числе местоположение, надежно скрывается с помощью сети «Tor». Анонимность в ней достигается путем использования промежуточных узлов между клиентским приложением и сервисом, к которому пользователь получает доступ, таким образом идентифицировать пользователя по его IP-адресу практически невозможно. По этим причинам в сети «Darknet» можно распространять, искать, приобретать практически любой вид запрещенного контента или запрещенных услуг и при этом сохранить анонимность[10]. Таким образом «Darknet» можно считать идеальным местом для распространения террористической пропаганды в виду анонимности использования сети, и отсутствия методов блокировки ресурсов «Darknet» правоохранительными органами. На просторах «Darknet» можно с легкостью отыскать запрещенные материалs, так же сеть является одним из самых больших рынков нелегального оружия, что соответственно является подталкивающим к терроризму фактором, при этом получить доступ к «Темному интернету» не так уж и сложно[11]. Таким образом «Darknet» представляет огромную угрозу, и является благоприятной средой для деятельности террористических организаций. Таким образом в настоящий момент мы получаем большие пробелы в сфере борьбы с терроризмом, такие как:

- Распространение террористическими организациями материалов, оправдывающих терроризм в сети интернет под видом информации СМИ;

- Расшатывание стабильности общественного сознания путём подачи насильственных материалов, вызывающих резкий резонанс, панику и страх среди населения;

- Использование террористическими организациями сети «Darknet», обеспечивающей анонимность распространения террористической идеологии, и отсутствие возможности блокировки ресурсов этой сети;

- Отсутствие единой глобальной методической базы, позволяющей активно осуществлять борьбу с проявлениями терроризма в сети;

- Неэффективность используемых в настоящее время методов борьбы с «кибертерроризмом», выраженная с ростом активности террористических организаций в сети Интернет;

В связи с изложенным, в целях усовершенствования методов борьбы с терроризмом в сети Интернет считаем целесообразным:

- Совершенствование отечественного законодательства путем внесения соответствующих поправок в нормативно-правовые акты в сфере пособничества и сотрудничества террористическим организациям в сети Интернет, таким как: разработка сайтов для террористических организаций, создание методов анонимизации используемых для

распространения террористических материалов, подготовка и верстка материалов террористического толка;

- Разработка методических рекомендаций по противодействию распространения материалов террористического характера в сети Интернет;

- Заимствование зарубежного опыта в сфере противодействия терроризму;

- Разработка специального программного обеспечения для автоматизации процесса блокировки и выявления территориальной принадлежности серверов размещения террористических материалов.

В заключение следует добавить, что терроризм в современном обществе значительно интегрировался в цифровые коммуникации, которые используются большинством населения земного шара. В настоящее время государства осознают опасность данного явления и ведут борьбу с распространением терроризма в сети Интернет, но как показывает практика, информации террористического толка на просторах глобальной сети становиться все больше, более того, она становится отточенной и профессиональной. В перспективе перед правоохранительными органами и законодателями встает вопрос разработки инновационных, эффективных правовых и практических методов борьбы с терроризмом в информационном пространстве, но при этом такие методы не должны противоречить основным принципам права и не нарушать права людей, к таким правам и принципам можно отнести: свободу слова, право на тайну связи, право на охрану личной, семейной тайны и др.

Список литературы:

1. Специальный доклад № 116. Как современные террористы используют Интернет. [электронный ресурс] // URL: http://scienceport.ru/library/-literature/5170-spetsialnyiy-doklad-№-116-kak-sovremennyie-terroristyi-ispolzuyut-internet/ (дата обращения: 29.06.2019);

2. Количество web-сайтов в мировом Интернете на 2014 год [электронный ресурс] // URL: http://total-rating.ru/1189-kolichestvo-web-saytov-na-2014-god.html (дата обращения: 29.06.2019);

3. Жаворонкова Татьяна Вячеславовна Использование сети Интернет террористическими и экстремистскими организациями // Вестник ОГУ. 2015. №3 (178). URL: https://cyberleninka.ru/article/n/ispolzovanie-seti-internet-terroristicheskimi-i-ekstremistskimi-organizatsiyami (дата обращения: 30.06.2019);

4. Самохина Наталья Николаевна, Гутова Светлана Георгиевна Феномен идеологии экстремизма и терроризма в сети Интернет: проблемы и пути их решения // Общество: политика, экономика, право. 2016. №10. URL: https://cyberleninka.ru/article/n/fenomen-ideologii-ekstremizma-i-terrorizma-v-seti-internet-problemy-i-puti-ih-resheniya (дата обращения: 30.06.2019);

5. Глобальная контртеррористическая стратегия ООН [электронный ресурс] // URL: https://www.un.org/counterterrorism/ctitf/ru/un-global-counter-terrorism-strategy#poa1 (дата обращения: 30.06.2019);

6. Доклад Управления ООН по наркотикам и преступности (2013 г.) [электронный ресурс] // URL: http://referatwork.ru/kiberugrozi/section-4.html (дата обращения: 30.06.2019);

7. Уголовный кодекс РФ от 13 июня 1996 г. № 63-ФЗ // Собрание законодательства Российской Федерации - 17 июня 1996 г. - № 25 - Ст. 2954.;

8. Закон Российской Федерации «О средствах массовой информации» от 27.12.1991 № 2124-1 (Закон о СМИ) [электронный ресурс] // URL: http://www.consultant.ru/document/cons_doc_LAW_1511/ (дата обращения: 30.06.2019);

9. Часто задаваемые вопросы. Блокировка интернет-страниц. Роскомнадзор. [электронный ресурс] // URL: https://rkn.gov.ru/treatments/p459/p750/ (дата обращения 30.06.2019);

10. Фролов Алексей Алексеевич, Сильнов Дмитрий Сергеевич Исследование механизмов распространения запрещенного содержимого в Darknet // Современные информационные технологии и ИТ-образование. 2017. №4. URL: https://cyberleninka.ru/article/n/issledovanie-mehanizmov-rasprostraneniya-zapreschennogo-soderzhimogo-v-darknet (дата обращения: 30.06.2019);

11. Журнал «Хакер» Секреты Даркнета. Ищем полезное в скрытых сервисах Tor [электронный ресурс] // URL: https://xakep.ru/2016/10/05/darknet-services/ (дата обращения: 30.06.2019).