БОРЬБА С ТЕРРОРИЗМОМ В СЕТИ ИНТЕРНЕТ: МЕЖДУНАРОДНО-ПРАВОВЫЕ АСПЕКТЫ

А. Р. Романова,
студентка ИГиП ТюмГУ,
направление «Юриспруденция»,
linnna.ro@mail.ru
Научный руководитель:
Д. Е. Аржиловский,
старший преподаватель кафедры
теории государства и права
и международного права ИГиП ТюмГУ,
d.e.arzhilovskij@utmn.ru

Террористические группы существовали всегда, но действовать в киберпространстве они начали относительно недавно. Исследование Габриэлы Вейманн, немецкого обществоведа и государственного служащего, работающего в Федеральном министерстве по делам семьи, престарелых, женщин и молодежи, в 2004 году показало, что из 30 террористических организаций, внесенных США в список «иностранных террористических организаций», в 1998 году имели веб-сайты около половины, а в 2003–2004 годах веб-сайты использовали больше половины террористических организаций [3].

К середине 1990-х годов интернет соединил более 18 тыс. общественных и национальных сетей, количество которых постоянно росло. В сетях было приблизительно 3,2 млн хостов и примерно 60 млн пользователей со всех континентов. Стоит отметить, что террористические организации в первую очередь интересовал вопрос финансирования их деятельности. Именно так можно объяснить резкий скачок количества террористических организаций в сети Интернет. Под средствами финансирования Международная конвенция о борьбе с финансированием терроризма от 9 декабря 1999 года в ст. 1 подразумевает активы любого рода, осязаемые или неосязаемые, движимые или недвижимые, а также юридические документы или акты в любой форме, удостоверяющие право на такие активы или участие в них, включая почтовые переводы, акции, ценные бумаги, облигации, векселя.

Как насчитывает статистика, предполагаемое число пользователей в первый год XXI века составило более 1 млрд человек. Стоит только подумать, что за такой короткий период времени — восемь лет действительно являются коротким периодом по сравнению с другими в истории международного права — террористические организации смогли так быстро «разрастись», а главное, освоить и проникнуть в сеть Интернет и оставаться в ней до сих пор, без труда занимаясь своей деятельностью. Действительно, терроризм — это страшное глобальное явление, которое приводит в ужас абсолютно всех, а когда террористы начинают активное использование Всемирной сети как свое оружие воздействия на массы, это приводит население всех стран в шоковое состояние, а специальные службы по борьбе с терроризмом — в полную готовность вовремя остановить массовую атаку.

По своей природе Всемирная сеть — это «идеальное» поле деятельности террористических организаций. В ней есть:

1) свобода доступа;
2) анонимность связи;
3) быстрый поток информации, который меняется каждую минуту;
4) потенциальная огромная аудитория;
5) возможность комбинировать текст, фото или видео, загружать книги;
6) и многое другое.

И, естественно, перечисленные преимущества никак не остались незамеченными террористическими организациями и их деятелями, независимо от политической принадлежности или ориентации.

Каждого, кто хотя бы раз углублялся в вопрос международного терроризма, интересовали вопросы: как выглядит сайт террористической организации? Сложно ли его спутать с обычным сайтом, который появ- ляется через поиск в интернете? Что должно «выдавать» сайты террористических организаций? Отвечая на

эти вопросы, стоит отметить, что мы просмотрели в ознакомительных целях некоторые сайты террористических организаций, доступ к которым запрещен на территориях как Российской Федерации, так и других государств. Наши наблюдения сводятся к следующим выводам:

1. Большинство сайтов содержит информацию о своих «выдающихся» деятелях, об истории организации и ее деятельности.
2. Содержатся сведения о политических и идеологических целях, планах на будущее.
3. Жесткая критика врагов, вражеских государств. Контроль политики между враждующими странами.
4. Часто на главных страницах сайтов размещаются карты с указанием государства, в котором существует террористическая организация, карт спорных областей. Например, сайт «Тигры освобождение Тамила» содержит карту Шри-Ланки.
5. Большинство террористических организаций скрывают «успехи» своей деятельности, но есть и исключения: например, сайт «Хамас» содержит отчеты об их действиях, список мертвых мучеников и количество убитых врагов.

Дополняя наши выводы, хотим отметить, что сайты террористических организаций сложно спутать с сайтами, где размещается, например, информация, которую пользователи могут искать повседневно для уче- бы, работы, научных исследований. Однако есть и такой вид «безобидных», на первый взгляд, сайтов, которые под видом интернет-магазинов могут продавать футболки, флаги, видеозаписи, книги, диски и другие отличительные знаки и материалы их террористической организации.

Как же террористы используют сеть Интернет? Проанализировав сайты террористических организаций, род и виды их деятельности, истоки зарождения такого явления, как *терроризм в сети Интернет*, мы определили следующие способы:

1. Влияние на психику пользователей.

Террористы в своей деятельности находят привлекательным использование дезинформации пользователей, распространение угроз, которые прямо направлены на то, чтобы запугать людей, навести на них панику беспомощности либо безвыходности грядущей ситуации. Влияние террористов в сети Интернет направлено не только на запугивание людей, но также и на сбои в экономике, работе фондовых бирж, различных банковских систем путем выведения из строя компьютеров. Запугивание происходит насколько интенсивно и яростно, что общество всерьез начинает думать о том, что задуманное террористами случится неизбежно.

2. Реклама и пропаганда.

Чаще всего террористы ищут поддержки со стороны общества. Они заявляют, что государства, на территориях которых находятся их организации, не хотят взаимодействовать с ними и различными способами ограничивают их свободу в выражении мнения. Странно, но именно этот способ манипулирования находит отклик как среди пользователей, так и среди сторонников. Террористические организации представляют себя как постоянно преследуемые. Они заявляют, что их лидеры постоянно подвергаются попыткам убийства, сторонников организации систематически избивают и арестовывают правоохранительные органы. Такая тактика изображения организации «маленькой и слабой» превращает террористов в невиновных, а государство — в тирана.

3. Сбор данных.

Ни для кого не секрет, что всё то, что однажды попало в сеть Интернет, остается там даже тогда, когда пользователи уверены, что всё удалили. Из интернета террористы могут получать более детальную информацию, например, об АЭС, которые расположены в городах, о транспортной инфраструктуре (карты метро, поездов, автобусов), о вентиляционных выходах и запасных входах в общественные здания. Без труда террористы могут узнать информацию о группе политических деятелей, их планах на будущее. И, конечно, террористическим организациям в их целях будет полезно рассекретить информацию, которая непосредственно связана, например, с планом-перехватом данной организации. В этом случае они могут поменять тактику нападения на общество.

4. Сбор средств на счет террористических организаций.

Как мы уже говорили ранее, террористы изначально активно использовали этот метод в сети Интернет. Необходима была материальная поддержка их деятельности для приобретения средств нападения и манипулирования людьми. В свое время такая террористическая организация, как «Аль-Каида», зависела от пожертвований, именно поэтому ее сбор денег был построен как благотворительный фонд. Кроме того, террористические организации просят, чтобы люди, перечисляя деньги на счета террористическим организациям с личных кредитных карт, после рассказали об их деятельности через электронные сообщения не только своим друзьям, но и совершенно не знакомым. Пункты «a» и «b» ст. 2 Международной конвенции о борьбе с финансированием терроризма указывают на то, что любое лицо совершает преступление, если оно любыми методами, прямо или косвенно, незаконно или умышленно предоставляет средства или осуществляет их сбор с намерением, чтобы они использовались для совершения деяний, которые представляют собой преступления, согласно сфере применения, либо другого деяния, направленного на то, чтобы вызвать смерть любого лица или причинить ему тяжкое телесное повреждение.

Статья 2 Международной конвенции о борьбе с бомбовым терроризмом от 16 декабря 1997 года не закрепляет такой вид преступлений, как «распространение информации о террористических организациях лицами, не состоящими в этих организациях». На наш взгляд, было бы разумнее внести эту поправку в ст. 2 Конвенции, потому что, как мы уже обозначали ранее, террористические организации могут и умеют обращаться с рекламной рассылкой и вербовкой людей, а дополнительное распространение в массы информации об их деятельности может только усугубить положение. Люди будут приглашаться в организацию, которая может им навредить, а распространители информации, получается, не несут никакой ответственности.

5. Четкое планирование и координация своей деятельности.

Данный способ можно рассмотреть на примере событий, которые произошли 11 сентября 2001 года в г. Нью-Йорке. Тогда активисты организации «Аль-Каида» использовали интернет в планировании и нападении на Всемирный торговый центр. После ареста террориста Абу Забейда на его компьютере федеральными должностными лицами были найдены сотни и сотни зашифрованных сообщений. Чтобы сохранить анонимность, террористы «Аль-Каиды» использовали интернет в общественных местах и посылали сообщения через публичную электронную почту. «Хамас» и «Аль-Каида» также с помощью сети Интернет поддерживали контакты, периодически координируя деятельность друг друга.

Современные террористы и террористические организации не останавливаются на одном и постоянно совершенствуют свои навыки по использованию Глобальной сети. На сегодняшний день террористы различных идеологических течений — исламисты, националисты, сепаратисты и пр. — получили максимальное количество информации, используя интернет. Поэтому мы предлагаем следующие ***методы борьбы с терроризмом в сети Интернет***:

1. Информированность общества.

В первую очередь необходимо оградить мирное население от вербовки и шантажа со стороны террористических организаций. Как мы уже выяснили, террористы подают неверную информацию с целью наведения на общество паники неизбежности наступления террористических актов. Мы же предлагаем провести информирование мирных жителей не для «галочки», а с целью получения знаний о том, что такое на самом деле терроризм, как он может проявляться, в каких формах и к чему это может привести. Большинство людей знакомы только с одной-двумя формами терроризма: захват заложников, массовый террор, направленный на причинение вреда интересам общества. Существуют и другие формы терроризма, с которыми общество либо не сталкивалось вообще, либо слышало, но не знало, что это терроризм. Например, убийства государственных или общественных деятелей или других представителей власти являются формой терроризма; еще одной выступает засылка вооруженных групп, которые применяют вооруженную силу против других государств.

2. Сотрудничество в правовой помощи между всеми государствами.

К сожалению, миру, и в том числе Российской Федерации, неоднократно приходится сталкиваться с тем, что террористическая организация, располагающаяся на территории какого-то государства, использует интернет-провайдеров другого государства. Делается это для того, чтобы федеральные службы не смогли получить доступ к каналам связи, по которым террористические организации передают зашифрованные сообщения о ближайших военных нападениях. Мы не зря упомянули в этом методе Российскую Федерацию, ведь если вспомнить такую террористическую организацию, как «Кавказ-Центр», то можно вспомнить, что скрытую и засекреченную информацию о своей деятельности они передавали по провайдерам, которые предоставляло государство Литва. Сотрудничать с Российской Федерацией Литва отказалась, ссылаясь на то, что передача личной информации будет являться существенным нарушением цензуры личных данных, пусть даже и террористов.

3. Следующий метод невозможен без предыдущего. Мы предлагаем усилить такие методы по борьбе с терроризмом, как своевременный перехват зашифрованной информации и создание каких-либо помех на каналах связи.

Считаем, что действующим силовым структурам по борьбе с терроризмом необходимо *качественно* отслеживать сообщения людей, прослушивать их мобильные и иные средства связи. А при обнаружении подозрительной информации немедленно блокировать связь либо создавать различные помехи для того, чтобы информация не дошла до получателя.

4. Создание единого международного интернет-ресурса, посвященного проблемам профилактики экстремистского и террористического поведения.

Только создание такого глобального сайта, с актуальной информацией по террористическим организациям, списки которых находятся в постоянном обновлении, с действующей психологической помощью, которая предоставлялась бы бесплатно всем тем, кто пострадал от террористических атак либо был подвергнут шантажу или вербовке как со стороны террористов, так и со стороны тех, кто распространяет информацию, помогло бы объединить все вышеперечисленные пункты в один. Конечно, необходимо также включить в содержание данного сайта перечисление всех признаков терроризма, всех его форм, которые могут усвоить даже неокрепшие умы. Также необходимо указать, что терроризм не является прямым путем к свободному обществу и что, если совершать те действия и заниматься той деятельностью, которой занимаются террористические организации, непременно стоит ожидать негативной реакции государства на это. В каких-то странах обходятся максимальным сроком лишения свободы, в каких-то приходят к иным методам — смертная казнь.

5. Ужесточение наказания за такой вид противоправной деятельности.

Мы склонны считать, что на любое правонарушение или преступление реакция государства должна быть не только моментальной, но и жесткой. Хотелось бы обратить внимание на то, что в задачах действующих кодексов Российской Федерации упоминается, для чего тот или иной кодекс существует, а именно: для охраны прав и свобод человека и гражданина, общественного порядка и общественной безопасности, а также окружающей среды, конституционного строя Российской Федерации от преступных посягательств, обеспечения мира и безопасности человечества. Стоит отметить, что, например, Уголовный кодекс Российской Федерации на данном этапе своего действия стремится к гуманизации некоторых норм, полной отмене такого вида наказа- ния, как смертная казнь. Но когда речь идет о жизни граждан и их безопасности от внешних и внутренних посягательств, разве можно говорить о том, что мы должны применять к преступнику, который *умышленно посягал* на человеческие жизни при помощи взрывоопасных средств или химического оружия, всего лишь лишение свободы на определенный срок?

Для примера, в США стали применять более суровые меры по отношению к лицам, которые просто поддерживают, на уровне фанатизма, ИГИЛ (запрещенную в Российской Федерации террористическую организацию). Так, в августе 2015 года в СМИ опубликовали новость, что 17-летний гражданин Вирджинии приговорен к 11 годам реального заключения за активное размещение в Сети пропаганды террористической организации [4].

Через призму нашего восприятия информация проходит так, чтобы вызвать неподдельное чувство сомнения, подозрения, страха или ненависти к тому, на что направлен информационный терроризм. Таким обра- зом, отличаясь от традиционного терроризма, который не так угрожал обществу как таковому и основам его жизнедеятельности, современный ужасающий высокотехнологичный терроризм способен порождать системный высокоэффективный кризис в любой стране с высокоразвитой информационной инфраструктурой [5].

Соглашаясь со словами В. В. Путина о том, что «Терроризм — это чума 21-го века», и резюмируя вышесказанное, мы считаем, что терроризму в современном обществе не место. С ним не только нужно, но и можно бороться, и бороться стоит жесткими методами, в том числе и теми, которые мы предложили в данной работе. Необходимо побороть не только тот вид терроризма, который мы разобрали в данной статье, но и любой другой, который только существует на земле. Считаем, что мы должны заложить крепкий фундамент для того, чтобы наши потомки, наши дети в дальнейшем жили не просто без войн, но и без угрозы полного уничтожения человеческого рода. А угроза терроризма — угроза существования всего живого.

СПИСОК ЛИТЕРАТУРЫ

1. Международная конвенция о борьбе с финансированием терроризма от 09.12.1999.
2. Международная конвенция о борьбе с бомбовым терроризмом от 16.12.1997.
3. Вейманн Г. Как современные террористы используют Интернет // Специальный выпуск. 2004. № 116.
4. Седых Н. С. Современный терроризм и молодежь: проблемы информационно-психологического противодействия // Мусульманский мир. 2017. № 2.
5. Косоруков А. Влияние информационного терроризма на молодежь через социальные сети // Материалы XI Ковалевских чтений, посвященных тематике «Глобальные социальные трансформации XX — начала XXI вв.», 2017.
6. Асеевский А. И. Кто организует и направляет международный терроризм. М.: Изд-во полит. лит-ры, 1988.
7. Мухамбетов Ж. С, Цымбалий А. О. Терроризм в сети // Молодой ученый. 2018. № 11.
8. Лашин Р. Л, Чурилов С. А. Противодействие экстремизму и терроризму в сети Интернет и образовательной среде // Обзор. НЦПТИ. 2016. № 7.
9. Кольтюков А. А. Международный терроризм — угроза глобальной и региональной безопасности: особенности проявления и пути противодействия // Право и безопасность. 2007. № 4.
10. Галенская Л. Н. Правовые проблемы сотрудничества государств в борьбе с преступностью. Л.: Изд-во ЛГУ, 1978.

ЦИФРОВИЗАЦИЯ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ

Н. С. Серегина,
студентка ИГиП ТюмГУ,
направление «Юриспруденция»,
ninaseregina190@yandex.ru
Научный руководитель:
Е. А. Хабарова,
доцент кафедры уголовного
права и процесса ИГиП ТюмГУ,
кандидат юридических наук, доцент,
e.a.khabarova@utmn.ru

Современные технологии являются неотъемлемой частью жизни абсолютно любого человека. Они способны воздействовать практически на все сферы жизнедеятельности и изменять все уровни бытия общества и человека. Информационные технологии достаточно активно развиваются и проникают в правовую материю, в том числе во многие институты уголовно-процессуального права.

Появление цифровых технологий дало человечеству принципиально новые возможности: накопление в электронных базах неизмеримых объемов информации, доступ к этим базам для неограниченного количе-