

Бураева Людмила Александровна

кандидат физико-математических наук,
доцент кафедры действия ОВД в особых условиях
Северо-Кавказского института
повышения квалификации (филиала)
Краснодарского университета
МВД России

МИРОВОЙ ОПЫТ ПРОТИВОДЕЙСТВИЯ ЭКСТРЕМИЗМУ И ТЕРРОРИЗМУ В ГЛОБАЛЬНОМ ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

Аннотация:

В статье рассмотрены актуальные вопросы борьбы с проявлениями экстремизма и терроризма в глобальном информационном пространстве, которое все чаще используется экстремистскими и террористическими группировками для устрашения общества, пропаганды своих преступных идей, вербовки в свои ряды, распространения планов возможных террористических атак, в разведывательных целях. Перечислены меры, принимаемые различными странами в целях противодействия распространению экстремизма и терроризма в сети Интернет.

Ключевые слова:

экстремизм, терроризм, глобальное информационное пространство, сеть Интернет, кибертерроризм, компьютерные преступления, экстремистские и террористические организации, интернет-сайты, социальные сети, коммуникационные технологии.

Burayeva Lyudmila Aleksandrovna

PhD in Physical and Mathematical Sciences,
Assistant Professor, Department for Police
Special Environment Operations,
North Caucasus Institute for Advanced Training,
branch of Krasnodar University of
the Ministry of Internal Affairs of Russia

WORLD EXPERIENCE IN EXTREMISM AND TERRORISM COUNTERACTION IN GLOBAL INFORMATIONAL SPACE

Summary:

The article studies the current issues of countering extremism and terrorism manifestations in the global informational space, which is used with increasing frequency by extremist and terrorist groups for society intimidation, propaganda of their maleficent ideas, recruitment into the fold, propagation of possible terrorist attacks plans, intelligence purposes. The author considers the measures undertaken by some countries focused on counteraction of extremism and terrorism spreading in Internet.

Keywords:

extremism, terrorism, global informational space, Internet, cyber-terrorism, computer crimes, extremist and terrorist organizations, web sites, social networks, communication technologies.

Число пользователей глобального информационного пространства с каждым годом стремительно увеличивается. Сегодня оно уже составляет примерно 3,2 млрд пользователей, однако по прогнозам аналитиков к 2016 г. эта цифра может достичь 3,4 млрд человек [1]. К сожалению, быстрыми темпами растет количество не только пользователей сети Интернет, но и совершаемых в глобальном информационном пространстве преступлений. Их разновидности, способы и формы осуществления множатся в своем разнообразии. На данный момент лидирующие позиции среди так называемых киберпреступлений занимают преступления экономической направленности. Однако среди остальных видов компьютерных преступлений, совершаемых в глобальном информационном пространстве, все чаще совершаются преступления террористической и экстремистской направленности. Этому способствуют особенности Всемирной паутины, которая обладает такими преимуществами, как простота доступа, независимость от географического расположения, потенциально огромные масштабы аудитории, высокая скорость передачи информации, анонимность коммуникации, трудности в осуществлении контроля со стороны правоохранительных органов. Сейчас, для того чтобы общаться с единомышленниками, преступникам нет необходимости собираться на конспиративных квартирах и входить в «тайные кружки», достаточно иметь персональный компьютер или современный мобильный телефон с выходом в сеть Интернет. Таким образом, виртуализированные экстремистские решения беспрепятственно и бесконтрольно проникают в каждый дом.

Сегодня проблемами компьютерного терроризма и экстремизма в глобальной сети озабочено все мировое сообщество, поскольку данное явление все больше угрожает безопасности многих стран и их граждан, вызывая огромные политические, экономические и моральные потери, оказывая сильное психологическое давление на большие массы людей. По заявлению Генеральной прокуратуры РФ, за 2014 г. в России пресечено 1 034 преступления экстремистской направленности (наибольший показатель за последние 10 лет), причем две трети из них – пре-

ступления, связанные с распространением экстремистских материалов в сети Интернет [2]. Поэтому надзорное ведомство РФ ведет постоянный мониторинг глобальной сети для выявления экстремистских сайтов и ограничения доступа к ним.

Волна терактов прокатилась по Европе и Азии. Чередой террористических атак были шокированы жители Франции в январе 2015 г. В их числе нападения на редакцию сатирического еженедельника *Charlie Hebdo*, на сотрудницу полиции в пригороде Парижа, захват заложников в столице страны и Даммартен-ан-Гозель. Эксперты отмечают, что нынешние действия террористов во многом являются «ответным возмездием» после проведенных вооруженными силами Запада операций по устранению точечными ударами с воздуха руководящих звеньев «Аль-Каиды» в Азии. Группы джихада разбросаны по всему миру и в своей деятельности активно используют высококвалифицированных специалистов по компьютерным технологиям, которые угрожают кибератаками правительственным сайтам США, Израиля и других государств.

Террористическая угроза охватывает все больше государств Азии. Так, в относительно спокойной до недавнего времени Турции 20 июля 2015 г. прогремел теракт, который унес жизни 31 человека, в связи с чем ведомством страны по инфокоммуникационным технологиям был заблокирован социальный сервис Twitter [3], который являлся средством коммуникации террористов предположительно из группировки «Исламское государство» (ДАИШ).

В настоящее время все активно действующие террористические и экстремистские организации имеют свои интернет-сайты в мировой сети. Как правило, они содержат детальный обзор социальных и политических мотивов, послуживших основанием для создания террористических и экстремистских организаций, информацию о политических и идеологических целях, которые они преследуют, сведения о наиболее известных акциях, биографии основателей и «героев», жесткую критику «врагов», а также обзор текущих новостей. Современные террористические и религиозно-экстремистские организации все чаще используют глобальное информационное пространство в качестве «пресс-центров» для обращений лидеров боевиков, террористов, повстанцев, религиозных радикалов. Создаваемые сайты антиобщественной направленности проектируются на достаточно высоком профессиональном уровне с использованием большого количества наглядной информации: фото-, аудио- и видеофайлы, которые призваны облегчить восприятие информации, привлечь как можно больше сторонников и источников финансирования. На указанных сайтах часто размещаются сведения о тактике и средствах проведения террористических актов, о типах взрывчатых и отравляющих веществ, основах взрывотехники, изготовлении самодельных взрывных устройств [4], методах конспирации. Террористические и экстремистские организации стремятся использовать коммуникационные возможности Всемирной паутины для устрашения общества, распространения антиобщественной информации, пропаганды своих преступных идей [5].

Наряду с созданием и поддержанием собственных веб-сайтов террористические и экстремистские организации практикуют работу на форумах, в социальных сетях, порталах общего доступа. На сегодняшний день социальные сети – самое популярное занятие во Всемирной паутине: по статистике соцсети посещают более 90 % пользователей Интернет. По имеющимся данным [6] в десятку лидеров по числу зарегистрированных пользователей входят: Facebook (1,4 млрд), YouTube (1 млрд), Google+ (более 500 млн), Twitter (более 500 млн), «ВКонтакте» (более 230 млн), «Одноклассники» (более 205 млн) и другие социальные сервисы. Более 80 % компаний по всему миру используют социальные сети в работе, примерно 78 % людей доверяют информации из социальных сетей. Указанные социальные ресурсы все чаще используются террористами и экстремистами для вербовки в свои ряды, осуществления пропаганды и распространения планов возможных террористических атак, а также в разведывательных целях.

Террористическая группировка «ИГИЛ» («Исламское государство Ирака и Леванта») смогла вывести пропаганду в социальной сети Twitter на принципиально новый уровень, осуществив самую успешную информационную атаку в истории кибертерроризма. Чтобы держать лояльных пользователей Twitter в курсе последних новостей джихада и управлять повесткой всего иракского сегмента, программистами группировки был разработан официальный сервис – приложение для Android под названием *The Dawn of Glad Tidings* («Заря радостных вестей»). Устрашающие видеоролики, тысячи «твитов» на тему «мы идем вас убивать», рассказы об убитых иракских военных и мирных жителях, фотографии обезглавленных или распятых тел – в итоге виртуальная атака на город оказалась не менее устрашающей, чем реальная [7].

Примером террористической угрозы от социальных сетей стал захват исламистами группировки «Аль-Шабаб» заложников в торговом центре Westgate (21 сентября 2013 г., Кения). В течение четырех дней террористы комментировали свои действия в Twitter и Facebook, выкладывая фотографии убитых людей и надсмехаясь над стражами порядка в режиме онлайн [8].

Печально известные террористы Царнаевы, устроившие взрывы на марафоне 15 апреля 2013 г. в г. Бостон (США), неоднократно прямым текстом писали в Twitter и Facebook о своих планах, однако спецслужбы игнорировали их, пока не стало слишком поздно.

На видеосервисе YouTube ежедневно просматривается 4 млрд видеороликов, в числе которых и ролики террористического толка. В частности, видеообращение Доку Умарова, ныне ликвидированного лидера незаконных вооруженных формирований на Северном Кавказе, было просмотрено за короткое время пользователями YouTube сотни тысяч раз.

Активная борьба против экстремизма и терроризма в Интернете ведется всем мировым сообществом [9]. Этим занимаются международные органы и организации: ООН, Совет Европы, Международная организация экспертов, Интерпол. Однако открытым остается вопрос эффективности данной работы. По проведенным исследованиям, только за 2013 г. число комментариев, содержащих призывы к насилию и дискриминации в социальных сетях, выросло на 30 %. Данный факт изложен в докладе «Использование Интернета в террористических целях» [10], подготовленном членами целевой группы ООН по осуществлению контртеррористических мероприятий. Конечно, при всем желании проверить все заметки экстремистской и террористической направленности невозможно, однако анализ учетных записей в социальных сервисах может существенно сократить количество террористических актов. В том случае, если в социальной сети будет удалена страница, имеющая связи с террористическими или экстремистскими организациями или напрямую управляемая ими, то через некоторое время появится аналогичная новая. Данная схема, именуемая «кошки-мышки», становится сейчас все более распространенной. Анализ адресов размещения религиозно-экстремистских сайтов в глобальной сети показывает, что большинство из них размещены на домене «com», принадлежащем США. При этом значительно число террористических и экстремистских организаций, запрещенных на территории стран СНГ, легально действуют в большинстве западных стран. Это исключает возможность для организации судебного преследования граждан, регистрирующих экстремистские сайты за рубежом и наполняющих их информацией.

Значительных успехов в сфере борьбы с экстремизмом и терроризмом в сети Интернет достигли Соединенные Штаты Америки. Количество организаций и ведомств, задействованных в работе по оказанию противодействия, достаточно велико. Среди них: командование боевых действий в кибернетическом пространстве (USCYBERCOM), национальный контртеррористический центр, центр стратегического контртеррористического взаимодействия, в задачи которого входит координация сотрудничества с зарубежными странами по борьбе с терроризмом и экстремизмом. Все это позволяет Штатам более эффективно, по сравнению с другими странами, контролировать интернет-пространство. В общественных местах доступа в глобальную сеть, таких как библиотеки и школы, используются фильтры, ограничивающие доступ к сайтам, содержащим ненадлежащую информацию, в том числе экстремистские материалы. В 2015 г. США заявили о начале новой фазы в борьбе против экстремизма и терроризма в сети, сказав, что теперь основное внимание правоохранительных и специальных служб будет уделено интернету, который стал очень удобным средством для радикальных идеологов по вербовке новых членов в преступные сети.

Член комитета по безопасности палаты представителей Конгресса США Джех Джонсон заявил, что группировки «ИГИЛ» и «Аль-Каида», используя возможности Всемирной паутины, распространяют свое влияние на умы людей, живущих вдалеке от Сирии и Ирака. Так, в феврале 2015 г. сотрудниками ФБР были задержаны трое мужчин, намеревавшихся присоединиться к группировке «ИГИЛ», а также оказать материальную помощь экстремистской организации. При этом директор ФБР Джеймс Корни сообщил, что на территории США есть тысячи «зараженных» идеями радикалов из «ИГИЛ», прекрасно освоивших современные информационные технологии. В подобной ситуации, по словам Корни, очень сложно выявить и обезвредить людей, готовящих теракт внутри страны [11]. В феврале 2013 г. президентом США была подписана директива о кибербезопасности, обязывающая создать систему кибербезопасности страны и разработать стандарты и методики, которые помогут снизить риски от кибератак на самые важные объекты инфраструктуры.

Правительство Германии также уделяет серьезное внимание вопросам противодействия пропаганде экстремистских и террористических идей в интернет-пространстве, несмотря на то что многие законодательные ограничения принимаются при значительном сопротивлении со стороны общественности, СМИ и компаний, работающих в сфере компьютерных технологий. В начале 2007 г. в ФРГ был принят закон, согласно которому регистрация электронной почты на вымышленное (нереальное) лицо теоретически расценивается как преступление. С января 2007 г. в правоохранительных органах Германии функционирует специальная группа, призванная выявлять случаи радикальной исламистской пропаганды, а также анализировать работу некоторых сайтов, представляющих потенциальную опасность.

В Великобритании закон о неправомерном использовании компьютерных технологий был принят в 1990 г. В 2006 г. срок тюремного заключения за правонарушения, связанные со взломом сайтов правительственных организаций и банков, был увеличен до десяти лет. В целях противодействия распространению экстремизма и терроризма в стране функционируют специальные органы, комитеты, среди которых: управление городской полиции по борьбе с терроризмом, группа безопасности электронных коммуникаций при центре правительственной связи.

Правовая база противодействия киберугрозам терроризма и экстремизма [12] в России последовательно развивается с 2000 г., когда была принята Доктрина информационной безопасности Российской Федерации. С 2008 г. действует Указ Президента РФ от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена». В начале 2014 г. Советом Федерации для всеобщего обсуждения был предложен проект Концепции Стратегии кибербезопасности Российской Федерации, в котором были определены направления усилий государства в отношении новых угроз, возникающих в современном информационном мире [13]. В 2013 г. утверждены «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года». Указом Президента РФ от 15 января 2013 г. на ФСБ России возлагаются полномочия по созданию государственной системы обнаружения, предупреждения и ликвидации компьютерных атак на информационные ресурсы РФ, информационные системы и информационно-телекоммуникационные сети, находящиеся на территории РФ и в дипломатических представительствах и консульских учреждениях РФ за рубежом.

Таким образом, с учетом особенностей экстремизма и терроризма в глобальном информационном пространстве возникает целый комплекс юридических и технических проблем, связанных с отсутствием: соответствующих нормативно-правовых актов, регулирующих уголовно-процессуальные действия; специально подготовленных кадров, специализирующихся на выявлении и раскрытии преступлений в информационно-телекоммуникационной сфере; требуемых технических средств противодействия кибератакам; надлежащей идеологической работы в сети, направленной на обсуждение актуальных проблем противодействия идеям экстремизма и терроризма; надежной системы сотрудничества и взаимодействия с правоохранительными органами зарубежных стран.

Ссылки:

1. Бураева Л.А. О некоторых вопросах обеспечения кибербезопасности в современных условиях // Теория и практика общественного развития. 2015. № 13. С. 96–99.
2. ГП: Пик пресеченных экстремистских преступлений пришелся на 2014 год [Электронный ресурс]. URL: <http://www.rg.ru/2015/03/31/ekstremizm-anons.html> (дата обращения: 25.08.2015).
3. Из-за теракта в Турции заблокировали Twitter [Электронный ресурс]. URL: <http://tengrinews.kz/internet/iz-za-terakta-v-turtsii-zablokirovali-Twitter-278141/> (дата обращения: 25.08.2015).
4. Карданов Р.Р. Роль судебно-криминалистических экспертиз в антитеррористической деятельности // Доклады Адыгской (Черкесской) Международной академии наук. 2014. Т. 16, № 1. С. 92–96.
5. Шагапсов З.Л., Тарчоков Б.А. Современные контуры системы противодействия различным проявлениям терроризма : учеб. пособие. Нальчик, 2012. 136 с.
6. Слабко Ю. Рейтинг социальных сетей 2014 по количеству пользователей. [Электронный ресурс]. URL: <http://www.seoros.ru/146-reyting-socialnyh-setey-2014-po-kolichestvu-polzovateley.html> (дата обращения: 25.08.2015).
7. Васильченко В. Джихад в Twitter: Как террористы осваивают приемы социального маркетинга [Электронный ресурс]. URL: <http://apparat.cc/network/isis-social-war/> (дата обращения: 25.08.2015).
8. Коваль М. Социальные сети как инструмент террористов [Электронный ресурс]. URL: <http://www.imena.ua/blog/network-for-terror/> (дата обращения: 25.08.2015).
9. Бураева Л.А. Информационные войны и информационный терроризм в современном мире: методы и поле действия // Известия Кабардино-Балкарского научного центра РАН. 2014. № 1. С. 7–11.
10. Использование интернета в террористических целях / Организация Объединенных Наций. Нью-Йорк, 2013. 48 с.
11. Борьба с терроризмом выходит в Сеть [Электронный ресурс]. URL: <http://islamreview.ru/politics/borba-s-terrorizmom-vyhodit-v-set/> (дата обращения: 25.08.2015).
12. Гаужаева В.А. Признаки терроризма, формирующие его понятие в нормативных и научных источниках // Актуальные вопросы юридических наук в современных условиях : сб. науч. тр. по итогам междунар. науч.-практ. конф. (г. Санкт-Петербург, 2015). СПб., 2015. С. 69–72.
13. Концепция стратегии кибербезопасности Российской Федерации [Электронный ресурс]. URL: <http://www.council.gov.ru/media/files/41d4b3dfb25cea8a73.pdf> (дата обращения: 25.08.2015).

References:

1. Buraeva, LA 2015, 'On some issues of cyber security in modern conditions', *Theory and Practice of Social Development*, no. 13, pp. 96-99.
2. GP: *Peak Suppression of extremist crimes occurred in 2014* 2015, retrieved 25 August 2015, <<http://www.rg.ru/2015/03/31/ekstremizm-anons.html>>.

3. *Because of the terrorist attack in Turkey blocked Twitter* 2015, retrieved 25 August 2015, <<http://tengrinews.kz/internet/iz-za-terakta-v-turtsii-zablokirovali-Twitter-278141/>>.
4. Kardanov, RR 2014, 'The role of the judicial and forensic examinations in anti-terrorist activities', *Reports of the Adyghe (Circassian) International Academy of Sciences*, vol. 16, no. 1, pp. 92-96.
5. Shhagapsoev, ZL & Tarchokov, BA 2012, *The modern contours of countering the various manifestations of terrorism: manual*, Nalchik, p. 136 .
6. Slabko, Y 2014, *Rating social networks in 2014 the number of users*, retrieved 25 August 2015, <<http://www.seoros.ru/146-reyting-socialnyh-setey-2014-po-kolichestvu-polzovateley.html>>.
7. Vasylichenko, V 2015, *Jihad in Twitter: How to master the techniques of terrorists social marketing*, retrieved 25 August 2015, <<http://apparat.cc/network/isis-social-war/>>.
8. Koval, M 2014, *Social networking as a tool of terrorists*, retrieved 25 August 2015, <<http://www.imena.ua/blog/network-for-terror/>>.
9. Buraeva, LA 2014, 'Information war and information terrorism in the world today: methods and field of action', *Proceedings of the Kabardino-Balkarian Scientific Center, RAS*, no. 1, pp. 7-11.
10. *Use of the Internet for terrorist purposes*, United Nations 2013, New York, p. 48.
11. *The fight against terrorism goes online* 2015, retrieved 25 August 2015, <<http://islamreview.ru/politics/borba-s-terrorizmom-vyhodit-v-set/>>.
12. Gauzhaeva, VA 2015, 'Signs of Terrorism, forming the concept in its regulatory and scientific sources', *Actual questions of legal science in modern conditions: textbook* (St. Petersburg, 2015), SPb., pp. 69-72.
13. *The concept of cyber-security strategy of the Russian Federation* 2015, retrieved 25 August 2015, <URL: <http://www.council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf>>.