ЮРИСПРУДЕНЦИЯ

Каскарбаева Зауре Айтошевна
старший преподаватель
Казахский агротехнический университет им.С.Сейфуллина
г. Астана, Республика Казахстан

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ БОРЬБЫ С КОМПЬЮТЕРНЫМ ТЕРРОРИЗМОМ

Аннотация: *в данной статье приведены нормативно-правовые документы различных государств,отражающие успешное противодействие проявлениям компьютерного терроризма.*

Ключевые слова: *компьютерный терроризм, кибертерроризм, киберпреступность, кибербезопасность.*

Глобализация информационных процессов не только открыла новые возможности для прогрессивного развития человечества, но и вызвала ряд качественно новых глобальных угроз, в том числе уяз-вимость мирового сообщества перед преступными посягательства-ми в сфере информационной безопасности. Актуальность противо-действия террористическим угрозам, основанным на новых техноло-гиях, обуславливает тот факт, что вопросы возможного использова-ния террористами ресурсов сети Интернет постоянно находятся в по-ле зрения компетентных органов государств-участников СНГ. Широкое использование ПЭВМ, а также созданных на их основе компьютерных сетей, увеличение объемов обрабатываемой информации, постепенное вытеснение бумажной технологии обработки документации, расширение круга пользователей привело к качественно новым возможностям несанкционированного доступа к конфиденциальной информации и данным информационных сетей, к их высокой уязвимости. Появилось совершенно новое явление в сфере информационных технологий, как «компьютерный или кибер-терроризм».

Сложность противостояния терроризму в Интернете обусловлена рядом факторов:

– во-первых, пространство Интернета крайне обширно – предугадать характер информации, время, место, автора и ее цель практически невозможно. Современные технологии позволяют лишь частично отследить первоочередную информацию. Однако ряд программных средств, доступных обычному пользователю, позволяют обойти и эти технологии;

– во-вторых, террористы могут использовать для загрузки своих материалов ресурсы, не требующие регистрирующих данных, и, кроме того, популяризировать ссылки на них через социальные сети. В этом случае появляется масса пользователей, которые, просматривая новостные ленты, случайно получают доступ к тому или иному материалу;

– в-третьих, вероятность того, что опубликованный где-либо материал сразу же обнаружат и удалят, крайне мала;

– в-четвертых, единой законодательной базы, регулирующей содержание контента Интернета, пока не существует, хотя попытки ее создания предпринимались уже не раз.

В противовес этому со стороны государства требуется постоянная модернизация и совершенствование программ борьбы с терроризмом. Более того, регулярный контроль интернет-пространства должен стать неотъемлемой частью противодействия.

Между тем, мировым сообществом в данное время наработан определенный положительный опыт борьбы с кибертерроризмом

В частности, в Великобритании недавно вступил в действие закон о терроризме, который ставит компьютерных хакеров в один ряд с боевиками Ирландской республиканской армии. Данный норматив-ный акт призван ужесточить борьбу с различными группировками, которые используют территорию Соединенного Королевства для своей деятельности. В соответствии с ним, в случае взлома хакерами компьютерной системы, обеспечивающей национальную безопасность страны, а также попыток с их стороны каким-либо

образом оказать воздействие на государственные структуры или угрожать обществу, они могут быть обвинены в терроризме со всеми вытекающими последствиями [1].

Соединенные Штаты Америки достигли значительных успехов в сфере борьбы с терроризмом в сети Интернет. Количество организаций и ведомств, задействованных в работе по оказанию противодействия, довольно велико, что позволяет в более полной мере, чем в ряде других стран, контролировать интернет-пространство.

С 11 сентября 2001 года руководство США обратило внимание на появление в сети пропагандистских материалов террористической направленности. После трагических событий американские спецслужбы начали ограничивать доступ к страницам талибов, а именно блокировать их. Выяснив, что экстремисты поддерживали контакт друг с другом через электронную почту из места общественного пользования с доступом в Интернет, президент Дж. Буш в 2001 году утвердил закон «Об объединении и укреплении Америки путем задействования полномочий и инструментов, необходимых для борьбы с терроризмом». После принятия данного документа любое действие, которое ведет к нарушению работы ПК или незаконному проникновению в компьютер, классифицируется как терроризм, а првайдер (компания, представляющая доступ в Интернет) обязан по требованию ФБР предоставить всю известную ему информацию о пользователе.

В США в общественных местах доступа во «всемирную паутину», таких как библиотеки и школы, применяются фильтры, которые ограничивают доступ к сайтам, содержащим ненадлежащую информацию, в том числе экстремистские материалы.

В опубликованную в 2007 году «Национальную стратегию внутренней безопасности» администрацией президента Дж. Буша был внесен раздел «Защита государственного и частного секторов Интернета в США», в котором отмечается необходимость защиты интернет-пространства от действий террористов.

В Евросоюзе в качестве мер по противодействию пропаганды терроризма разработана Конвенция о киберпреступности, принятая комитетом министров Совета Европы в ноябре 2001 года. Она охватывает широкий круг вопросов, в том числе такие аспекты киберпреступности, как незаконный доступ к компьютерным системам, оказание воздействия на данные, на работу систем, противозаконное использование устройств, подлог и мошенничество с использованием компьютерных технологий и возможностей, правонарушения, связанные с терроризмом. Документ предусматривает также общие для интернет-провайдеров правила хранения личной информации их клиентов и пользователей на тот случай, если подобные сведения будут затребованы при расследовании нарушений в сфере кибербезопасности.

Согласно последним данным, конвенцию подписали 46 стран (38 государств – членов Совета Европы, а также Канада, Япония, ЮАР и США), хотя ратифицировали лишь 24 из них. К не подписавшим ее странам относятся Китай, несколько латиноамериканских государств и Россия.

В апреле 2008 года в Европейском союзе было принято решение об ужесточении законодательства по борьбе с терроризмом. Согласно поправкам, преступлением стало считаться любое побуждение к подобной деятельности, в том числе пропаганда терроризма в Интернете, а также вербовка террористов с помощью интернет-сайтов.

В Китайской Народной Республике система контроля глобальной сети представляет собой системный и эффективный комплекс мер. Фильтрация контента осуществляется как программными, так и аппаратными средствами. Кроме того, власти оказывают прямое давление как на самих пользователей, так и на владельцев сайтов и провайдеров.

С самого начала своего появления Интернет в Китае находится под тотальным контролем со стороны властей. Правительство имеет технические возможности блокировать сайты, на которых появляется информация, идущая вразрез с законами КНР. Периодически в этот «черный список» попадают и

некоторые иностранные электронные СМИ, в основном тайваньские и американские.

В республике введена обязательная регистрация пользователей в интернет-кафе, а также действует интернет-полиция, которая выявляет противозаконный контент, появляющийся в сети.

В 2005 году новостные сайты прошли перерегистрацию, согласно которой лично отвечают за публикуемую информацию. Общая цель правил – защита национальной безопасности и общественных интересов. Подобного рода меры китайских властей получили соответствующее название Great Firewall of China («firewall» – программное средство защиты от несанкционированных подключений к компью-теру).

С 1 июля 2009 года в Китае предусматривалась установка на все компьютеры интернет-фильтров, которые должны отсеивать сайты с ненадлежащим содержанием. Изначально фильтры должны были устанавливаться на все компьютеры, продающиеся в стране, еще до того как они покинут завод. Программа также должна интегрироваться в компьютеры, ввезенные в КНР и предназначенные для продажи. Однако насколько тщательно это контролируется, неизвестно.

Президент Республики Казахстан Н. Назарбаев в 2009 году подписал закон, приравнивавший все интернет-ресурсы к СМИ, которые стали нести уголовную и гражданскую ответственность наравне с традиционными средствами массовой информации. Действие закона «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам информационно-коммуникационных сетей» распространилось на сайты, блоги, чаты, интернет-магазины, электронные библиотеки и др.

Введение этой меры позволяет судебным органам требовать от владельцев сайтов удаления материалов, противоречащих законодательству. Кроме того, в казахстанский суд можно обратиться с жалобой на любой интернет-ресурс вне зависимости от того, где он расположен.

Президентом Республики Беларусь А. Лукашенко 1 февраля 2010 года подписан указ №60 «О мерах по совершенствованию использования национального сегмента сети Интернет», призванный защитить прежде всего рядовых пользователей от деструктивного воздействия экстремистских и аморальных сайтов [2].

В 2007 году в РФ по фактам совершения киберпреступлений было возбуждено почти 4,6 тысяч уголовных дел. Более половины из них по статье 272 УК РФ («Неправомерный доступ к компьютерной информации»). На втором месте – создание, распространение и использование вредоносных компьютерных программ, а также нарушение авторских прав.

Ежегодно МВД России выявляется около 150 ресурсов, содержащих материалы террористической и экстремистской направленности. Больше всего подобных сайтов было обнаружено в российском сегменте сети, их оказалось более 70. Мониторингом интернет-пространства круглосуточно занимаются специализированные подразделения МВД России, в соответствии с законодательством закрываются сайты с негативным контентом, а лиц, размещающих на них информацию, привлекают к уголовной ответственности. Однако около 15% закрытых сайтов появилось вновь под другими именами на хостинговых ресурсах как российских, так и зарубежных провайдеров. Чаще всего сайты, вытесненные из российского сегмента сети, мигрируют в другие страны. Поэтому повышение уровня международного сотрудничества в данной сфере представляется весьма актуальным [3].

В Турции закон №5651 «О порядке трансляции информации в сети Интернет и борьбе с совершаемыми в сети Интернет преступлениями» был принят в мае 2007 года. К преступлениям в виртуальном пространстве, за которые может последовать наказание, в данном законе отнесено распространение в сети Интернет информации, содержащей призывы к самоубийству, сексуальное насилие над детьми, поощрение использования наркотических и психотропных средств, распространение опасных для здоровья человека веществ, порнографические материалы, способствующие развитию

проституции, сведения и возможности для организации азартных игр, а также любые акции и инициативы против основателя Турецкой республики Мустафы Кемаля Ататюрка.

Компьютерные преступления упоминаются также в ст. 345 и ст. 350 УК Турции, предусматривающих различные наказания за «неправомерный доступ к компьютерной информации, осуществляемый для модификации, уничтожения указанной информации и/или для совершения мошенничества, в том числе с банковскими счетами и кредитными картами».

Как считают турецкие эксперты, немаловажное значение для успешного противодействия проявлениям компьютерного терроризма имеет уровень информированности рядовых граждан по данному вопросу и отношение общества в целом к этой проблеме. В связи с этим в Турции особое внимание уделяется контролю над интернет-кафе, которые рассматриваются спецслужбами как возможный фундамент для подготовки экстремистами крупной террористической кибератаки. По состоянию на 31 декабря 2007 года, в Турции насчитывалось более 8 тыс. таких заведений. 75% турецких пользователей получают доступ в сеть Интернет именно из интернет-кафе. МВД Турции постоянно обновляет циркуляры и директивы относительно предоставления и получения этих услуг. Главные принципы – недопущение к сайтам, содержание которых направлено на подрыв конституционных устоев государства, и запрет использования сети для нанесения вреда другим пользователям Интернета [4].

Ряд организационных и практических мер, позволивших создать определенные заделы для создания эффективной системы противодействия кибертерроризму принят и в Республике Казахстан. К примеру, в Уголовный кодекс РК внесены изменения, предусматривающие уголовную ответственность за совершение компьютерных преступлений, в частности, по статье 227 «Неправомерный доступ к компьютерной информации, создание и распространение вредо-носных программ для ЭВМ» предусмотрены штраф либо исправительные работы до одного года, либо лишение свободы на срок до пяти

лет. За сравнительно короткий срок правоохранительными органами Казахстана возбуждено порядка 20 уголовных дел по несанкционированному использованию компьютерных систем. Во избежание нанесения ущерба от кибератак на важные сетевые инфор-мационные ресурсы принято постановление Правительства РК, прямо предписывающее обязательное отделение сетей государственных органов и организаций от сети Интернет [5].

Исходя из вышеизложенного необходимо подчеркнуть, что вопросы отсутствия единого подхода без использования двойных стандартов при организации противодействия международному преступлению, каковым является кибертерроризм, остается открытой, а это не позволяет в полной мере организовать надежный заслон данной угрозе. Соответственно, решение проблемы борьбы с кибертерроризмом на сегодняшний день – это задача, которая требует объединения усилий всего мирового сообщества.

Список литературы

1. Завьялов С. Зарубежный опыт в области борьбы с пропагандой терроризма в интернете. Зарубежное военное образование.–2014 – №4.

2. Ахтырская Н. Противодействие компьютерному терроризму требует законодательного обеспечения. [Электронный ресурс] – Режим доступа: crime-research.ru.

3. Соловьев И.Н. Правовое обеспечение борьбы с преступлениями в сфере информационных технологий. Административное и муниципальное право – 2009 – №3.

4. Гурьев А.А. Меры Анкары по борьбе с компьютерным терроризмом. [Электронный ресурс] – Режим доступа: www.iimes.ru.

5. Уразбаев А. Кибертерроризм: проблемы противодействия [Электронный ресурс] – Режим доступа: www.atcsng.ru.