10. Поляков В.В. Следственные ситуации по делам о неправомерном удаленном доступе к компьютерной информации // Доклады Томского государственного университета. 2010. N1(21). С. 46 - 50.

КИБЕРТЕРРОРИЗМ: МЕРЫ ПРОТИВОДЕЙСТВИЯ В АСПЕКТЕ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА РОССИИ И СТРАН ЗАРУБЕЖЬЯ

М.Н. Кутявина, Т.И. Рыбина, АлтГУ,
юридический факультет, 4 к.
Научный руководитель – ***В.А. Мазуров,*** к.ю.н., доцент.

Сегодня интернет широко используется не только обычными гражданами, но различными террористическими и экстремистскими организациями и играет большую роль в их деятельности, которая не ограничивается лишь пропагандистской и разъяснительной работой, публикацией материалов определенной направленности и др.

Посредством интернет-ресурсов осуществляется привлечение к подобной деятельности «волонтеров», вербовка новых членов, сбор финансовых средств, планирование и координация совместных действий.

Не вызывает сомнения, что компьютерные преступления во всем мире имеют устойчивую тенденцию к росту, поскольку растет и аудитория пользователей высокими технологиями и Интернет-ресурсами. Ключевым положением борьбы с кибертерроризмом является интеграция правовых систем различных стран (например, сближение уголовного законодательства стран Евросоюза). На первый план, по сравнению с национальным законодательством, выходят инструменты межгосударственного (международного) регулирования, поскольку данная проблема не носит, как правило, каких-либо географических или политических границ.

При этом речь идет не столько о включении международных актов в национальное законодательство путем их ратификации, сколько о добровольном и рациональном учете рекомендаций международных (межправительственных) организаций (ЕС, ООН,

АТР и др.) и опыта развития специального законодательства в других странах.

Для совершенствования российского законодательства это особенно важно, поскольку объективную проблему представляет новизна сферы правового регулирования, отсутствие устоявшейся теоретической основы, что, прежде всего, сказывается на понятийном аппарате по рассматриваемому вопросу.

Между тем, мировым сообществом в данное время наработан определенный положительный опыт борьбы с кибертерроризмом. На международном и межгосударственном уровне принят ряд нормативных правовых актов, регламентирующих данную проблему.

Так, Генеральной Ассамблеей ООН в резолюции 53/70 от 4 декабря 1998 года [1] были затронуты вопросы целесообразности разработки общепринятых международных принципов организации противодействия кибертерроризму, предусматривающих усиление безопасности глобальных информационных и телекоммуникационных систем и борьбу с информационным терроризмом и преступностью.

Значительным шагом в формировании международной правовой базы в данном направлении стало подписание 23 ноября 2001 года представителями стран - членов Совета Европы, США, Канады и Японии Конвенции Совета Европы «О киберпреступности» [2]. Она определяет приблизительный перечень преступлений, совершенных в информационной сфере, против информационных ресурсов или с помощью информационных средств и признает их киберпреступлениями. На сегодняшний день Конвенция подписана 43 членами ЕС и 15 другими странами, включая США. РФ не вошла в число государств, подписавших Конвенцию. В настоящее время это единственный международный акт, содержащий закрепление основ по защите прав человека в киберпространстве. Россия, по всей видимости, пока не готова к полноценному сотрудничеству в данном направлении с зарубежными партнерами. При этом следует отметить, что мировое сообщество также еще находиться в процессе выработки единой политики в указанном вопросе, о чем свидетельствует непрекращающаяся работа представителей различных государств в борьбе с кибертерроризмом.

В последние годы активно прорабатываются вопросы совершенствования нормативной правовой базы стран СНГ в данном направлении. Так, Указ Президента России «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена» от 12 мая 2004 года N 611 [3] запрещает госорганам пользоваться Интернетом без средств защиты и регламентирует, какие спецслужбы должны за это отвечать. Указ направлен главным образом на обеспечение защиты российского сегмента сети Интернет, в первую очередь - сетевых ресурсов государственных органов, от внешних угроз несанкционированного воздействия. При этом речь идет, в первую очередь, о предотвращении возможных попыток компьютерного «взлома» и получения контроля над сетевыми ресурсами органов власти России с террористическим умыслом.

Россией также была разработана концепция Конвенции об обеспечении международной информационной безопасности 2011 г. Конвенция предполагает полное сохранение государственных суверенитетов и границ национального регулирования в виртуальном пространстве.

В качестве еще одного шага на пути к обеспечению информационной безопасности можно назвать проект «Правил поведения в области обеспечения международной информационной безопасности» [4]. Этот кодекс в сентябре 2011 года Россия, Китай, Узбекистан и Таджикистан предложили распространить в качестве официального документа 66-й сессии Генеральной ассамблеи ООН. Государствам, присоединившимся к правилам, предлагается сотрудничать в борьбе с преступной или террористической деятельностью с использованием информационно-коммуникационных технологий, уважать права и свободы граждан в информационном пространстве, а также способствовать формированию культуры информационной безопасности и защите объектов критической информационной инфраструктуры.

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 «Непра-

вомерный доступ к компьютерной информации, создание и распространение вредоносных программ для ЭВМ» предусмотрены штраф либо исправительные работы до одного года, либо лишение свободы на срок до пяти лет [5]. В структуре спецслужб образовано специализированное подразделение по борьбе с киберпреступностью. В МВД РК созданы Национальный контактный пункт по борьбе с преступностью в сфере высоких технологий и управление специальной оперативно-аналитической работы и раскрытия преступлений в сфере высоких технологий.

Так же хотелось бы затронуть регулирование исследуемой проблемы в субъектах РФ, в частности в Алтайском крае. Нормативных актов, направленных на регулирование данной проблемы нет, но весьма богата практическая деятельность разных структур: в АК, в различных правоохранительных органонах, существует так называемый отдел «К», отвечающий за компьютерную безопасность. В Алтайском Крае и Республике Алтай существует уникальное коммерческое лицо, единственное на названных территориях, которое оказывает различные услуги по информационной безопасности (выдача лицензий, техническое сопровождение и администрирование сетей передачи данных, защита персональных данных, конфиденциальной информации). Речь идет о Центре информационной безопасности АК. Кроме того показательна тенденция работы органов прокуратуры: активно ведется работа в сфере выявления информационных ресурсов экстремистского и террористического содержания. Всего, в период с 2013 – 14 гг. прокурорами нашего края было подано 20 исковых заявлений об ограничении к разным интернет - ресурсам такого характера. На первый взгляд данная цифра является небольшой, однако, с другой стороны, это немалое количество исков, особенно в виду того, что зачастую правонарушители добровольно удаляют такую информацию или закрывают свой ресурс.

Резюмируя изложенное необходимо подчеркнуть, что кибертерроризм представляет собой глобальную проблему, для решения которой необходима международная координация усилий. Наиболее эффективный способ борьбы с компьютерными преступлениями сегодня - объединение опыта на международном уровне, как правоохранительных органов, так и компаний, специа-

лизирующихся в области информационной безопасности, и их активное тесное сотрудничество.

Предлагаемые нами меры противодействия и предупреждения кибертерроризму:

1. разработка на международном уровне комплексной программы, включающей в себя возможные формы и методы борьбы с кибертеррором (юридические, программные, технологические, организационные, экономические, политические и т.д.);
2. криминализация международного кибертерроризма, законодательное закрепление такого состава преступления как «Международная кибератака»;
3. антитеррористические акции: пропаганда в общественных местах посредством размещения плакатов, баннеров, распространения аудио-, видеоинформации, брошюр и листовок;
4. создание единого списка организаций, деятельность которых признана кибертерроризмом;
5. паспортизация объектов, наиболее подверженных компьютерному террору, разработка паспортов защищенности объектов, информационной (компьютерной) безопасности на основе международного соглашения.

Все эти меры в совокупности между собой и с другими существующими на сегодняшний момент позволят не только снизить уровень ущерба, причиненного киберпреступлениями, но и предупредить кибертеррористов, тем самым даже не допуская осуществления начальных действий кибератак.

Список литературы

1. Генеральная Ассамблея ООН в резолюции 53/70 от 4 декабря 1998 года //Права человека: Сборник международных документов. - М., 1998. – 314 с;
2. Конвенция Совета Европы «О киберпреступности» (Будапешт, 23 ноября 2001 года) // Международное сотрудничество в борьбе с преступностью. Сборник международно-правовых актов.- М., 2000. – 248 с;
3. Указ Президента России «О мерах по обеспечению информационной безопасности Российской Федерации в сфере междуна-

родного информационного обмена» от 12 мая 2004 года N 611// Собрание законодательства РФ, 17.05.2004, № 20, Ст. 1938;
4. Тропинина Т. Л. Киберпреступность и кибертерроризм: поговорим о понятийном аппарате: Сборник научных трудов международной конференции «Информационные технологии и безопасность». Выпуск 3. – К.: Национальная академия наук Украины, 2003. – 178-179 с;
5. Уголовный Кодекс Республики Казахстан от 16.07.1997 № 167-I (в ред. 07.03.2014) // «Ведомости Парламента», 1997 г., № 15, Ст. 211.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПДнВ ВУЗе

К.В. Масалова, АлтГТУ, факультет информационных технологий, 5 к.
Научный руководитель – ***Е.В. Шарлаев,*** к.т.н., доцент.

В силу своей специфики в ВУЗе хранится и обрабатывается огромное количество информации, в том числе персональные данные (ПДн) различных категорий субъектов ПДн. ВУЗы являются операторами ПДн, и соответственно, на них распространяется действие закона о 152-ФЗ «О персональных данных» [1].

Выполнив анализ нормативно-правовой базы, а также практического опыта в области информационной безопасности становится очевидным, что разработать эффективную систему защиты информационных систем можно только в соответствии с требованиями руководящих документов и рекомендаций.

ВУЗы, как правило, обращаются к коммерческим организациям, оказывающим услуги в области защиты информации. Это увеличивает расходы на защиту ПДн, но гарантирует наличие отлаженной системы защиты информации с полным пакетом документации.

Основными проблемами, с которыми сталкиваются при организации защиты ПДн в ВУЗе, являются: территориальная рассредоточенность ресурсов информационных систем, большое количество серверов, к которым привязаны ИСПДн, порой с разными уровнями защищенности, выход многих ИСПДн в глобальные инфо-телекоммуникационные сети и сети общего пользования.