МЕЖГОСУДАРСТВЕННОЕ СОТРУДНИЧЕСТВО В БОРЬБЕ С МЕЖДУНАРОДНЫМ КИБЕРНЕТИЧЕСКИМ ТЕРРОРИЗМОМ НА ПРИМЕРЕ ЕВРОПЕЙСКОГО СОЮЗА

© 2017 Дмитриева Вера Владимировна
Институт законодательства и сравнительного правоведения
при Правительстве Российской Федерации
117218, г. Москва, Б. Черемушкинская ул., д. 34
E-mail: dmitrieva-vv@list.ru

Выполнен анализ отличия международного кибернетического терроризма от иных видов компьютерных преступлений. Определено понятие международного кибернетического терроризма. Приведены основные формы межгосударственного сотрудничества стран Европейского союза в борьбе с международным кибернетическим терроризмом. Дана оценка эффективности такого сотрудничества.

Ключевые слова: терроризм, международный терроризм, международный кибернетический терроризм, кибертерроризм, киберпреступность, Европейский союз, межгосударственное сотрудничество в борьбе с кибертерроризмом.

Как угроза международного терроризма в целом, так и угроза международного кибернетического терроризма в частности приобретают все большее значение в наши дни. События террористических акций во Франции, Турции, Египте и других странах в 2015-2016 гг. отражают актуальность вопросов обеспечения международной безопасности и достижения наиболее эффективного межгосударственного сотрудничества.

Интернет обладает свойством экстерриториальности и позволяет регистрировать доменное имя сайтов в одном государстве, а распространять информацию посредством использования данного сайта по всему миру. Такая деятельность на пространствах Интернета может способствовать формированию общественного мнения и, как результат, влиять на отдельные социальные процессы. Это естественным образом открывает дополнительные возможности для террористической деятельности.

Все большую роль в процессе осуществления своих преступных действий террористические группировки отводят техническому обеспечению с использованием электронных средств коммуникации для вербовки новых членов в свои ряды, запугивания общественности, нарушения работы государственных и банковских компьютерных систем, компьютерных систем международных органов. И если ранее основной целью преступников было нарушение работы национальных компьютерных систем для достижения личных целей, то сегодня террористы активно используют глобальные компьютерные сети для охвата как можно большей аудитории в целях запугивания и, как итог, достижения своих локальных и международных политических целей.

Отличительной особенностью компьютерных преступлений от иных преступлений являются сложность и быстрота действий, которые впоследствии приведут к нарушению прав отдельных лиц, интересов государств и международных сообществ, и сравнительно невысокая вероятность возможности пресечения готовящихся нарушений. Так, в литературе выделяют два вида компьютерных нарушений: непосредственную атаку на компьютерные системы и использование компьютерных данных. И если меры, направленные на пресечение первого вида преступлений, заключаются в дополнительном техническом и программном оснащении компьютерных систем и подготовке квалифицированных кадров, то в случае с использованием компьютерных данных недобросовестные лица могут годами производить пополнение своих информационных носителей, прежде чем владелец информации, чьи права были нарушены, обнаружит несанкционированную утечку[1].

Технические сложности зачастую приводят не только к спланированным, но и к случайным ошибкам в работе систем. Так, регулярно возникают ситуации, при которых снижается работа сети Интернет, происходит блокировка спутниковых сигналов, случаются аварии в работе транспортных систем, которые приводят к летальным исходам.

Все сказанное создает уязвимости, которыми могут воспользоваться лица, обладающие специ-

альными знаниями, для применения компьютерных систем в непредусмотренных целях. К слову, небезызвестный сценарий поражения иранской атомной станции вирусом STUXNET в 2010 г., чудом не приведший к катастрофическим последствиям, планировался и для терактов в Европе в 2016 г.[2]

Активное развитие технологий требует все более детальной проработки вопросов защиты информации, создания эффективной национальной правовой базы, а также взаимодействия государств на международном уровне.

К настоящему моменту понятие кибернетического терроризма не получило своего закрепления в международном договоре, который был бы согласован большинством стран.

Одним из основополагающих документов в отношении киберпреступности стала Конвенция о преступности в сфере компьютерной информации 2001 г. (далее - Конвенция), разработанная Советом Европы, а также Дополнительный протокол 2003 г. К международному договору присоединились 54 страны, в том числе США и Великобритания. В Конвенции были нормативно закреплены и систематизированы правонарушения в кибернетическом пространстве, включая: подлог с использованием компьютерных технологий; мошенничество с использованием компьютерных технологий; правонарушения, связанные с детской порнографией; правонарушения, связанные с нарушением авторских и смежных прав.

В то же время за пределами нормативного регулирования Конвенции остались многие другие действия в сфере киберпространства, наносящие ущерб информационным отношениям и их субъектам. Так, не было закреплено понятие международного кибернетического терроризма. Вместе с тем сам документ позволяет осуществлять взаимодействие государств в борьбе с преступлениями в информационной сфере.

Терроризм представляет собой действия, создающие опасность гибели людей, причинения значительного ущерба либо наступления иных общественно опасных последствий, является преступлением против общественной безопасности[3]. Международный терроризм характеризуется трансграничностью, угрожая безопасности сразу нескольких стран. А в случае использования сети Интернет границы охватываемой сферы и вовсе стираются. Под угрозой оказывается весь мир. Согласно Федеральному закону “О противодействии терроризму” от 6 марта 2006 г. № 35-ФЗ под террористической деятельностью понимается деятельность по подстрекательству, планированию и финансированию терроризма, вербовке и обучению террористов, пропаганде. Под террористическими актами понимается непосредственное совершение действий, приведших (или могущих привести) к гибели лиц, причинению урона жизненно важной инфраструктуре или наступлению иных общественно опасных последствий. Этот подход представляется правильным и для описания международной террористической деятельности. Все это применимо и к кибернетическому терроризму. В сети Интернет террористы общаются, осуществляют планирование, вербуют новых сторонников, обучают новобранцев, проводят пропаганду терроризма, захватывают отдельные компьютерные системы и выводят их из строя.

Для того чтобы разобраться в данной проблеме, остановимся на понятии кибернетического терроризма и постараемся разграничить кибернетический терроризм и киберпреступность. К сожалению, международное право пока не знает точного определения этого понятия. Ряд отечественных и зарубежных ученых при этом имеют свое особое мнение. Так как терроризм зародился задолго до появления Интернета, а единого определения терроризма так и не было выработано международным сообществом, дать четкое определение кибернетического терроризма представляется затруднительным. Однако существует ряд отличительных особенностей. Так, судья Стейн Шёльберг из Норвегии указывает на то, что кибертерроризм включает в себя и терроризм, и киберпреступность. Он отмечает, что кибертерроризм сопряжен с “координированными компьютерными атаками на жизненно важную информационную инфраструктуру страны”[4]. В.А. Голубев определяет кибернетический терроризм как “преднамеренную, политически мотивированную атаку на информацию, обрабатываемую компьютером, компьютерную систему и сети”[5], которая сопряжена с возникающей опасностью для жизни или здоровья людей. Такая атака направлена на запугивание населения (и даже, как результат, на достижение военного конфликта). Террористы могут угрожать применением насилия для поддержания состояния страха с целью достижения политических целей, а также с целью привлечения внимания к деятельности террористической организации. Кроме того, Голубев отмечает, что характерной особенностью кибертерроризма является его гласность и широкое освещения кибертеррористических актов.

Существует подход, согласно которому киберпреступников разделяют по характеру их мотиваций. Так, американские ученые, Аллан Фридман и Питер Сингер, помимо террористов в сети Интернет, выделяют среди хакеров, совершающих преступления, активистов и патриотов. Если первые используют компьютер и свои навыки для достижения целей своей группы, как правило политических, то вторые совершают противоправные действия на основании национальных и патриотических идей. Так, к активистам они относят ставшую уже известной в мире группу Анонимус[6]. В этом ключе есть основания согласиться с авторами. Действия Анонимус не были направлены на применение насилия или причинение вреда жизни и здоровью отдельных лиц. Группа лишь осуществляла блокировку отдельных правительственных сайтов.

Таким образом, представляется, что международный кибернетический терроризм характеризуется следующими аспектами:

- осуществляется в электронных системах передачи данных и обладает свойством экстерриториальности;
- обладает гласностью и широко освещается для охвата как можно большей аудитории;
- направлен на запугивание и поддержание состояния страха среди как можно большей массы населения;
- имеет целью достижение политических интересов (при этом их достижение осуществляется посредством применения насилия и запугивания насилием);
- сопряжен с угрозой жизни и здоровью людей, жизнедеятельности отдельных государств;
- поражает наиболее значимые объекты инфраструктуры стран мира.

Важность урегулирования возникающих вопросов в данной сфере требует вовлечения всех сторон международного сообщества. При этом сотрудничество государств в борьбе с международным кибернетическим терроризмом осуществляется в основном на региональном уровне.

Здесь уместно сказать об отграничении понятия "борьба" от понятия "противодействие", которое также часто используется в уголовном праве. Так, согласно Федеральному закону "О противодействии терроризму" от 6 марта 2006 г. № 35-ФЗ под противодействием терроризму понимается деятельность органов государственной власти и органов местного самоуправления, а также физических и юридических лиц по предупреждению терроризма, выявлению, предупреждению, пресечению, раскрытию и расследованию террористического акта, минимизации и ликвидации последствий проявлений терроризма. При этом в литературе выделяют позицию, согласно которой термин "борьба" более применим к социальному явлению, "противодействие" же - к отдельному социально опасному акту[7]. Представляется, что термин "борьба" будет более корректен в отношении межгосударственного взаимодействия, которое должно быть направлено: на выработку национальных принципов и норм, развитие сотрудничества правоохранительных органов отдельных стран, а также на противодействие отдельным социально опасным актам. При рассмотрении проблемы межгосударственного взаимодействия в борьбе с международным кибернетическим терроризмом в данном случае будут пониматься: развитие и унификация национального уголовного законодательства стран, разработка и осуществление межгосударственного взаимодействия по линии правоохранительных органов и непосредственное отражение происходящих кибертеррористических атак.

Значительный вклад в развитие национального законодательства и создание межгосударственного взаимодействия в борьбе с международным кибернетическим терроризмом вносит Европейский союз.

Представляется, что сотрудничество в борьбе с международным кибернетическим терроризмом невозможно без сближения и, в ряде случаев, без унификации национальных правовых систем в части установления уголовной ответственности за использование киберпространства в террористических целях. Однако законодательства стран Европейского союза не только разнятся в части установления ответственности за преступления в киберпространстве, зачастую законодатель не предусматривает ответственности за кибертерроризм. Чаще всего такие преступления квалифицируют как кражу и использование компьютерной информации, несанкционированное проникновение в компьютерные системы. То есть в большинстве случаев аспект "террористической деятельности" теряется. В то же время ряд стран выработали свою, уникальную систему выявления и преследования таких преступлений. В частности, уголовное законодательство Германии знает следующие составы преступлений: атака программного и аппаратного обеспечения (включая хищение (компьютерной) информации (section 202a), перехват данных (section 202b), подготовка к хищению (компьютерной) ин-

формации и перехвату данных (section 202c)[8]. Кроме того, Уголовный кодекс Германии вводит понятия "подделка компьютерных данных" и "компьютерный саботаж" (sections303a, 303b)[9]. Названные деяния наказываются лишением свободы на срок до пяти лет.

Согласно Закону Великобритании о неправомерном использовании компьютерных технологий (Computer Misuse Act) 1990 г. лицо совершает преступление, когда использует компьютер для выполнения функции с намерением получить доступ к программе или данным, хранящимся на каком-либо компьютере, если такой доступ является неправомерным, и лицо, осуществляющее такие действия, знает об этом (section 1 (1) Computer Misuse Act)[10]. За совершение этого преступления предусмотрено наказание в виде штрафа или заключения на срок до 6 месяцев. Отражая важность угроз, исходящих из киберпространства, английский законодатель затронул вопросы использования компьютерных систем в террористических целях в Законе о терроризме (TerrorismAct) 2000 г. Согласно документу правоохранительные органы вправе считать террористическими действия, которые "серьезно вмешиваются или серьезно нарушают работу какой-либо электронной системы"[11].

Аналогичное закрепление на уровне уголовного кодекса получили противоправные действия в киберпространстве в других странах. Так, Нидерланды указали, что любое лицо, которое умышленно и незаконно перехватывает и записывает с помощью технического устройства данные, не предназначенные для него, и обрабатывает или передает посредством радиосвязи либо с помощью компьютерного устройства или системы, подлежит тюремному заключению на срок не более одного года или штрафу (section 139c)[12].

В Бельгии в марте 2005 г. была создана рабочая группа по проблеме киберпреступности в рамках плана действий по борьбе с радикализмом, принятом на уровне Правительственного комитета разведки и безопасности (Ministerial Intelligence and Security Committee)[13]. Как итог, понятия преступлений в сфере киберпреступности были включены в Закон о киберпреступности 2000 г. и нашли свое отражение в уголовном кодексе страны. Среди них: компьютерный подлог, компьютерное мошенничество и преступления против конфиденциальности, целостности и доступности компьютерных систем и данных, хранящихся, или обрабатываемых, или передаваемых ими.

Однако, несмотря на то, что на уровне некоторых государств уже ведется работа по определению понятия кибертерроризма, в большинстве своем национальные законодательства рассматривают борьбу с кибертерроризмом как борьбу с преступностью в сфере киберпространства в целом.

Отдельно стоит упомянуть об Эстонии, которая среди других стран Европейского союза занимает одно из ведущих положений в области разработки мер, направленных против кибертерроризма. Согласно данным, предоставленным страной в отчете о киберпреступности Совета Европы 2007 г., Эстония более всех стран Европейского союза пострадала от массированных кибератак в 2007 г., что подтолкнуло правительство к разработке защитных мер[14]. В этой связи именно в Эстонии был развернут Центр киберзащиты (далее - Центр) Организации Североатлантического договора (НАТО) в Таллине, которому был присвоен статус международной военной организации. Центр играет важную роль в обучении и обеспечении безопасности стран альянса. В работе Центра принимают участие 18 стран, в том числе 14 стран Европейского союза: Эстония, Германия, Франция, Великобритания, Словакия, Италия, Литва, Латвия, Испания, Венгрия, Чехия, Польша, Голландия, Греция. Австрия и Финляндия участвуют в работе Центра в статусе партнеров.

Рассмотрим деятельность институтов Европейского союза в борьбе с международным кибернетическим терроризмом.

В 2004 г. в соответствии с регламентом ЕС № 460/2004 (Regulation (EC) No 460/2004) было создано Европейское агентство по безопасности сетей и информационной безопасности (The European Network and Information Security Agency, далее - ENISA) со штаб-квартирой в г. Ираклион (Крит)[15]. В рамках деятельности данной организации проводятся учения по обеспечению кибернетической безопасности. В состав ENISA входят: аппарат управления, группы постоянных представителей от стран-участниц, по одному офицеру по связям от каждой из стран-участниц, а также временные рабочие группы по отдельным специальным вопросам. Офицеры связи стран-участниц совместно образуют объединение национальных офицеров по связи (National Liaison Officers Network). Целями ENISA, в числе прочего, являются: приобретение опыта прогнозирования угроз и защиты информа-

ции; выработка политики продвижения сетевой и информационной безопасности в качестве приоритетных направлений политики Европейского союза; укрепление сотрудничества на уровне Европейского союза между государствами-членами; усиление воздействия ENISA посредством совершенствования управления ее ресурсами и более эффективного взаимодействия с заинтересованными сторонами, включая государства-члены и институты Союза, а также на международном уровне[16].

ENISA реализует программы повышения осведомленности по вопросам кибербезопасности, проводит межгосударственные учения по вопросам кибербезопасности. При проведении этих мероприятий к работе привлекаются также следующие организации: Европейское оборонное агентство (European Defense Agency), Институт Европейского союза по изучению вопросов безопасности (European Union Institute for Security Studies), Спутниковый центр Европейского союза (European Union Satellite Centre), Евроюст, Европол, Исполнительное агентство по образованию, аудиовизуальным средствам и культуре (Education, Audiovisual and Culture Executive Agency) и др. Также к работе привлекается созданный в 2013 г. Европейский центр по борьбе с киберпреступностью (European Cyber Crime Centre), который является органом Европола в Европейском союзе (штаб-квартира в Гааге) и координирует трансграничную правоохранительную деятельность по борьбе с компьютерной преступностью, выступает в качестве центра технической экспертизы по данному вопросу.

К настоящему моменту ENISA разработал ряд основополагающих документов в борьбе с кибертерроризмом. Так, были разработаны пошаговое руководство по созданию групп компьютерной безопасности и реагирования на инциденты (Computer Security and Incident Response Team), универсальный сборник упражнений для служб реагирования на компьютерные инциденты, проект национальной Стратегии кибербезопасности в рамках Европейского союза.

В целях предоставления национальным государственным органам информации о проблемах и значении создания защиты облачных технологий ENISA в 2013 г. подготовила отчет об инцидентах облачной безопасности (Cloud Security Incident Reporting) с выработкой ряда рекомендаций[17]. Так, было указано на необходимость установления немедленного информирования об инцидентах кибератак на облачные технологии.

Страны Европейского союза ведут активную деятельность по разработке и принятию национальных Стратегий кибербезопасности, разрабатываемых на основе рекомендаций, предложенных ENISA. Так, по данным ENISA, к настоящему времени Стратегии кибербезопасности приняли 25 из 28 стран Европейского союза[18]. В Швеции, Болгарии и Греции документы еще находятся в стадии разработки. Это также говорит о признаваемой странами - членами Европейского союза высокой важности обеспечения кибернетической безопасности.

Основой национальных стратегий является формирование национального информационного общества, где особое внимание будет уделяться безопасности граждан и защите информационно-телекоммуникационных ресурсов в сети Интернет. Так, Германия, выделяет среди основных целей необходимость предотвращения и уголовного преследования кибератак, создания эффективной системы взаимодействия силовых ведомств. Кроме того, Европейский союз ведет активную подготовку и обучение судей и следователей в области кибербезопасности.

Итак, межгосударственное взаимодействие стран Европейского союза осуществляется на уровне его институтов. Однако это взаимодействие осуществляется в отношении обеспечения кибербезопасности в целом. Созданный в 2013 г. Европейский центр по борьбе с киберпреступностью также основное внимание уделяет киберпреступности. Кибертерроризму отводится лишь роль одного из преступлений в сфере высоких технологий.

Представляется, что такой подход создает ряд ограничений в расследовании и пресечении кибертерроризма. Кибернетические террористические атаки на компьютерные системы могут привести не только к разрушению компьютерных систем, порче или закрытию доступа к компьютерной информации, блокируя и нарушая работу, таким образом, банковских систем или государственных органов. Такие атаки могут нанести также физический вред и привести к человеческим жертвам, если, например, атакованные компьютерные системы связаны с работой атомных электростанций, систем управления полетами, компьютерных систем медицинских учреждений, компьютерных систем, осуществляющих управление военным оружием.

Еще одной особенностью международного кибернетического терроризма является то, что такие преступления, помимо очевидной общественной

опасности, обладают высокой скоростью подготовки и совершения, а значит, с учетом фактора экстерриториальности сети Интернет требуют немедленного реагирования совместными усилиями правоохранительных органов стран мира. А для этого требуется и соответствующее техническое оснащение, и оперативное взаимодействие между правоохранительными органами.

Без создания должной правовой базы, криминализации понятия кибернетического терроризма, создания комплексного подхода по обеспечению безопасности в борьбе с кибертерроризмом невозможно эффективное сотрудничество в этой области.

Очевидна необходимость выработки единого документа, который бы определил понятие международного кибернетического терроризма и механизм осуществления межгосударственного взаимодействия в борьбе с ним.

Нельзя сказать, что опыт, приобретенный Европейским союзом, не является существенным. Международный кибернетический терроризм представляет собой новое явление. Международное сообщество еще не успело выработать единое понимание по этому вопросу. Однако актуальность угроз, которые несет использование кибертехнологий террористами, выявляет высокую необходимость скорейшего его разрешения. К сожалению, сегодня наиболее эффективная деятельность в проработке вопросов межгосударственного сотрудничества осуществляется на региональном уровне. Однако полученный опыт требует детального изучения и применения в деятельности как отдельных государств, так и всего международного сообщества. Знания и опыт, накопленные Европейским союзом, играют не последнюю роль в достижении глобальной международной безопасности.

[1] Goldsmith J. (2013) How Cyber Changes the Laws of War. *The European Journal of International Law*, vol. 24, 1, pp. 130-131.

[2] Координатор ЕС считает, что АЭС Бельгии могут угрожать кибератаки // РИА новости. 26.03.2016. URL: http://ria.ru/world/20160326/1397664506.html.

[3] *Абдурахманов М.И., Баришполец В.А., Манилов В.Л.* Военная безопасность России : слов.-справ. / под общ. ред. В.Л. Манилова. Москва, 2000. С. 325.

[4] Договор о киберпространстве - Конвенция или Протокол Организации Объединенных Наций о кибербезопасности и киберпреступности. Подготовлено Стейном Шёльбергом. Справочные документы, полученные от отдельных экспертов // Двенадцатый Конгресс Организации Объединенных Наций по предупреждению преступности и уголовному правосудию (Сальвадор, 12-19 апр. 2010 г.) : сб. документов / сост.: А.Г. Волеводз, С.М. Тарасенко, В.А. Ализаде. Т. 2. Москва, 2011. С. 274-275.

[5] *Голубев В.* Кибертерроризм как новая форма терроризма / Центр исследования проблем компьютерной преступности. URL: http://www.crime-research.org/library/Gol_tem3.htm.

[6] Singer P.W., Friedman A. (2014) *Cybersecurity and Cyberwar*. New York, pp. 77-85.

[7] *Вишневецкий К.В., Трофименко С.В.* О терминах "борьба" и "противодействие" в уголовно-правовой лексике // Теория и практика общественного развития. 2013. № 3. С. 225-230.

[8] *Зигмунд О.А., Петровский А.В.* Кибер- и интернет-преступность в Германии и России: возможности сравнительного исследования // Юридическая наука и правоохранительная практика. 2015. № 4 (34). С. 180-188.

[9] German Criminal Code / European Commission. Available from: https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/criminal_code_germany_en_1.pdf.

[10] Computer Misuse Act 1990. *The National Archives*. Available from: http://www.legislation.gov.uk/ukpga/1990/18/section/1.

[11] *Громов Е.В.* Развитие уголовного законодательства о преступлениях в сфере компьютерной информации в зарубежных странах (США, Великобритании, Нидерландах, Польше) // Вестник Томского государственного педагогического университета. 2006. № 11 (62). С. 32.

[12] Criminal Code of the Netherlands. *The European Judicial Training Network (EJTN)*. Available from: http://www.ejtn.eu/PageFiles/6533/2014%20seminars/Omsenie/WetboekvanStrafrecht_ENG_PV.pdf.

[13] Cyberterrorism - the use of Internet for terrorist purposes. Council of Europe, December 2007, p. 119.

[14] Ibid, p. 161.

[15] Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency. *EUR-Lex*. Available from: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML.

[16] Mission and Objectives // European Union Agency for Network and Information Security. Available from: https://www.enisa.europa.eu/about-enisa/mission-and-objectives.

[17] Cloud Security Incident Reporting. *Sobre ISMS*. Available from: https://www.ismsforum.es/ficheros/descargas/incident-reporting-for-cloud-computing1392993762.pdf.

[18] National Cyber Security Strategies. *European Union Agency for Network and Information Security*. Available from: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map.

Поступила в редакцию 04.12.2016 г.