# Противодействие кибертерроризму
# Диденко А. И.

*Диденко Александр Игоревич / Didenko Aleksandr Igorevich – студент магистратуры,*
*Юридическая школа*
*Дальневосточный федеральный университет, г. Владивосток*

***Аннотация:*** *в статье рассматриваются российская нормативно-правовая база и другие организационные меры в области противодействия кибертерроризму.*
***Abstract:*** *the article deals with the Russian legal framework and other arrangements in the field of countering cyberterrorism.*

***Ключевые слова:*** *кибертерроризм, противодействие кибертерроризму, компьютер, киберпространство, компьютерная сеть.*
***Keywords:*** *cyber-terrorism, countering cyber terrorism, computer, cyberspace, computer network.*

В период с 2000 по 2015 годы удельный вес пользователей интернета увеличился почти в семь раз − с 6,5 до 43 процентов мирового населения. По данным последнего пресс-релиза [8] Международного союза электросвязи (МСЭ) от 22.07.2016, количество пользователей интернета в мире составляет 3,5 миллиарда человек. Большинство пользователей приходится на развивающиеся страны – в них насчитывается 2,5 миллиарда пользователей, а в развитых странах – 1 миллиард [9]. Топ - 10 стран по числу пользователей интернета: Китай - 710 млн, Индия - 350 млн, США - 277 млн, Япония - 110 млн, Бразилия - 110 млн, Россия - 87,5 млн, Германия - 72 млн, Индонезия - 71 млн, Нигерия - 70 млн, Мексика - 59 млн (в отношении Китая по данным Информационного центра сети Интернет Китая (CNNIC); Индии - Internet and Mobile Association of India и KPMG; в отношении других стран по данным Internetworldstats.com) [9]. Таким образом, компьютер и интернет все больше проникают в нашу обыденную жизнь, а вместе с ними и преступления в области высоких технологий. Россию, как страну, входящую в 10-ку стран по количеству пользователей интернета, проблемы киберпреступности тоже не обходят стороной.

Одним из наиболее опасных преступлений, связанных с компьютерами, компьютерными сетями и киберпространством, является киберртерроризм. Это обусловлено значительным влиянием компьютерной техники и интернета как на повседневную жизнь людей, так и на объекты инфраструктуры. Компьютерная техника используются в различных сферах общественной жизни от библиотек до атомных электростанций и военных объектов. И если террорист, использующий в своих целях обычное вооружение, опасен для десятков или сотен людей, то кибертеррорист может представлять опасность для значительно большего числа людей, непосредственно не участвуя в террористическом акте, а находясь в безопасном месте. Так, например, в США неоднократно посторонние лица, в том числе из иностранных государств, получали доступ к управлению жизненно-важной инфраструктурой [13]. Поэтому очень важно обеспечить безопасность компьютерной техники и телекомуникационных сетей в сферах, влияющих на безопасность и жизнеобеспечение значительного числа людей. Несмотря на свою повышенную общественную опасность, Российское государство должного внимания данной проблеме не уделяет. И это все происходит на общем фоне усиления борьбы с терроризмом [2].

Фактор, который выделяет киберртероризм среди остального вида терроризма, - это среда, где он осуществляется - киберпространство. С этим связаны и определенные проблемы противодействия и выявления кибертерроризма. Например, Данильченко Э. Д. выделяет такие проблемы, как:

1. Отсутствие соответствующих законодательных актов, адекватных современному положению дел в сфере защиты компьютерной информации и регулирующих отношения в сети Интернет.
2. Отсутствие необходимых технических средств у следственных и оперативных органов не способствует своевременной фиксации фактов совершения актов кибертерроризма.
3. Недостаточное количество специально подготовленных кадров, специализирующихся на выявлении и раскрытии компьютерных преступлений, а также специализированных подразделений ПО.
4. Система защиты интернет-серверов и информационно-коммуникационных систем не успевает совершенствоваться вслед за все более совершенными способами и методами совершения актов кибертерроризма.
5. В случае совершения кибертеррористического акта трудно установить место его совершения, так как данные преступления отличаются своим трансграничным характером. Расположение компьютера, с помощью которого совершается преступление, крайне редко совпадает с местом расположения объекта посягательства и последствиями деяния. Кроме этого, проблему составляет сохранение следов совершения преступления, а также процесс розыска кибертеррористов, что существенно снижает шансы

привлечения преступника к уголовной ответственности [7].

На наш взгляд, основной проблемой, с которой сталкиваются при противодействии кибертерроризму, является его трансграничный характер. Это связано с тем, что отличительной чертой кибертерроризма является то, что насильственные действия производятся лицом не непосредственно на месте совершения теракта (путем взрыва, поджог и т.д.), а удаленно и через киберпространство. Кибертеррорист может находиться даже на территории другого государства. Поэтому для успешного противодействия кибертерроризму, на наш взгляд, необходим целый комплекс мер:

1) создать нормативно-правовую базу в Российской Федерации, которая бы закрепила термин кибертерроризм в уголовно-правовом смысле, а также способы его проявления;

2) разработать и принять международные документы универсального характера, которые определили термин кибертерроризм в максимально широком толковании и обязали бы государства закрепить кибертерроризм в национальном уголовном праве с учетом специфики внутреннего законодательства;

3) необходимо создать международные документы, закрепляющие обязанность государств оказывать правовую помощь при расследовании указанного преступления по запросу другого государства на взаимной основе в ускоренном порядке;

4) установить уголовную ответственность за кибертерроризм как за особо тяжкое преступление как в национальном законодательстве РФ, так и в международных документах;

5) определить государственную структуру, которая будет осуществлять борьбу с кибертерроризмом, с выделением данной структуре материальных, технических и кадровых ресурсов для осуществления противодействия кибертерроризму;

6) определить структуру, занимающуюся разработкой технических средств для противодействия кибертерроризму;

7) выделение материальных средств на освещение в СМИ кибертерроризма, как общественно-опасного явления, и выработки негативного отношения к нему как в обществе в целом, так и в профессиональном сообществе лиц, связанных с компьютерной техникой;

8) вести учет лиц, обладающих знаниями, умениями и навыками, необходимыми для осуществления кибертерроризма.

В 2001 году Советом Европы была принята «Конвенция о преступности в сфере компьютерной информации». Российская Федерация в данной конвенции не участвует. При этом попытки присоединиться к данной конвенции были [4]. Также опыт закрепления термина киберртероризм существует в национальном законодательстве. В 2001 году в ответ на совершение террористического акта известного как «9/11» или «11 сентября» Конгрессом США был принят федеральный закон Uniting and Strengthening Americaby Providing Appropriate Tools Requiredto Interceptand Obstruct Terrorism Act [6]. Данный закон в п. 814 закрепляет понятие «кибертерроризм» через различные формы его проявления - нанесение ущерба защищенным компьютерным сетям граждан, юридических лиц и государственных ведомств, включая ущерб, причиненный компьютерной системе, используемой государственным учреждением при организации национальной обороны или обеспечении национальной безопасности.

В Российской Федерации пока должного внимания указанной выше проблеме не уделяется. Термин кибертерроризм легально не закреплен ни в одном нормативно-правовом акте. Уголовная ответственность за совершение террористического акт предусмотрена ст. 205 УК РФ, при этом квалифицированного признака, связанного с осуществлением данного акта в киберпространстве российский Уголовный кодекс не предусматривает.

Нельзя сказать, что кибертерроризм вовсе отсутствует в нормативном поле Российской Федерации. Так кибертерроризм употребляется в контексте подготовки специалистов для противодействия терроризму [5].

Также Российская Федерация имеет множество двусторонних договоров о правовой помощи по уголовным делам с иностранными государствами [10]. При наличии между РФ и иностранным государством указанного выше соглашения на основании ст. 453 УПК РФ суд, прокурор, следователь, руководитель следственного органа, дознаватель при необходимости вносит запрос о производстве необходимого следственного или иного действия компетентным органом или должностным лицом иностранного государства в соответствии с международным договором Российской Федерации, международным соглашением или на основе принципа взаимности. Наличие договоров о правовой помощи является полезным элементом сотрудничества в вопросах борьбы преступности, но для борьбы с такой угрозой как кибертерроризм, на наш взгляд, требуется более гибкая структура, т.к. направление и исполнение запросов о правовой помощи довольно долгая процедура.

Определенная обеспокоенность угрозой кибертерроризма возникает у президента РФ. Еще в 2006 году президент РФ Путин В. В., выступая в Москве на конференции генеральных прокуроров европейских стран, предложил разработать глобальную стратегию по борьбе с кибертерроризмом [11]. В 2009 году появляется утвержденная президентом РФ «Концепции противодействия терроризму в Российской Федерации».

В 2013 году Президент РФ Путин В. В. своим Указом от 15.01.2013 № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» возложил на ФСБ РФ полномочия по созданию государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ - информационные системы и информационно-телекоммуникационные сети, находящиеся на территории Российской Федерации и в дипломатических представительствах и консульских учреждениях Российской Федерации за рубежом [3].

Основными задачами указанной структуры являются:

а) прогнозирование ситуации в области обеспечения информационной безопасности Российской Федерации;

б) обеспечение взаимодействия владельцев информационных ресурсов Российской Федерации, операторов связи, иных субъектов, осуществляющих лицензируемую деятельность в области защиты информации, при решении задач, касающихся обнаружения, предупреждения и ликвидации последствий компьютерных атак;

в) осуществление контроля степени защищенности критической информационной инфраструктуры Российской Федерации от компьютерных атак;

г) установление причин компьютерных инцидентов, связанных с функционированием информационных ресурсов Российской Федерации.

В структуре МВД тоже существует структура, осуществляющая противодействие преступлениям в сфере компьютерной информации. Так основными направления работы Управления «К» БСТМ МВД России [12]:

1. Борьба с преступлениями в сфере компьютерной информации:

- выявление и пресечение фактов неправомерного доступа к компьютерной информации;
- борьба с изготовлением, распространением и использованием вредоносных программ для ЭВМ;
- противодействие мошенническим действиям с использованием возможностей электронных платежных систем;
- борьба с распространением порнографических материалов с участием несовершеннолетних через сеть Интернет.

2. Пресечение противоправных действий в информационно- телекоммуникационных сетях, включая сеть Интернет:

- выявление и пресечение преступлений, связанных с незаконным использованием ресурсов сетей сотовой и проводной связи;
- противодействие мошенническим действиям, совершаемым с использованием информационно-телекоммуникационных сетей, включая сеть Интернет;
- противодействие и пресечение попыток неправомерного доступа к коммерческим каналам спутникового и кабельного телевидения.

3. Борьба с незаконным оборотом радиоэлектронных и специальных технических средств.

4. Выявление и пресечение фактов нарушения авторских и смежных прав в сфере информационных технологий.

5. Борьба с международными преступлениями в сфере информационных технологий:

- противодействие преступлениям в сфере информационных технологий, носящим международный характер;
- взаимодействие с национальными контактными пунктами зарубежных государств.

6. Международное сотрудничество в области борьбы с преступлениями, совершаемыми с использованием информационных технологий.

Информации о деятельности указанных структур в открытом доступе не так уж много, но даже не смотря на это можно сделать вывод, что с организационной стороны противодействие как кибертерроризму, так и иным преступлениям в области высоких технологий в Российской Федерации осуществляется. Причем из анализа задач указанных выше структур и действующего уголовно-процессуального законодательства, можно сделать вывод, что противодействие кибертерроризму отнесено к компетенции органов ФСБ. Это обусловлено тем, что расследование преступлений в области террористической деятельности ст. 151 УПК РФ возлагает на следователей ФСБ [1].

Таким образом, в Российской Федерации системного противодействия киберртероризму не ведется. Существуют разрозненные попытки осуществлять борьбу с данным видом проявлением терроризма. Отсутствует необходимая нормативно-правовая база. При этом, как было сказано выше, для эффективного противодействия кибертерроризму необходимы совместные усилия всех членов мирового сообщества.

***Литература***

1. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 06.07.2016) (с изм. и доп., вступ. в силу с 01.09.2016). Доступ из справ.-правовой системы «КонсультантПлюс».
2. Федеральный закон Российской Федерации от 06.07.2016 № 374-ФЗ о внесении изменений в закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности». [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс»/ (дата обращения 22.09.2016).
3. Указ Президента РФ от 15.01.2013 № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (Выписка). Доступ из справ.-правовой системы «КонсультантПлюс».
4. Распоряжение Президента РФ от 15.11.2005 N 557-рп и Распоряжением Президента РФ от 22.03.2008 № 144-рп. Доступ из справ.-правовой системы «КонсультантПлюс».
5. Концепция противодействия терроризму в Российской Федерации (утв. Президентом РФ 05.10.2009). Доступ из справ.-правовой системы «КонсультантПлюс».
6. Uniting and Strengthening Americaby Providing Appropriate Tools Requiredto Interceptand Obstruct Terrorism Act of 2001: [Electronic resource]. URL: http://www.selectagents.gov/resources/USApatriotAct.pdf/ (date of access: 26.09.2016).
7. *Данильченко Э. Д.* Правовая основа противодействия правоохранительных органов кибертерроризму «Транспортное право», 2015. № 4. С. 27-32.
8. Пресс-релиз МСЭ за 2016 год. [Электронный ресурс]. Режим доступа: http://www.itu.int/net/pressoffice/press_releases/2016/pdf/30-ru.pdf/ (дата обращения: 28.09.2016).
9. Пользователи интернета в мире. [Электронный ресурс]. Режим доступа: http://www.bizhit.ru/index/polzovateli_interneta_v_mire/0-404/ (дата обращения 26.09.2016).
10. Двусторонние международные договоры Российской Федерации о правовой помощи. [Электронный ресурс]: Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=126898&fld=134&dst=1000000001,0&rnd=0.8760678508705084/ (дата обращения 28.09.2016).
11. Выступление Путина В. В. на конференции генеральных прокуроров европейских стран. [Электронный ресурс]. Режим доступа: https://lenta.ru/news/2006/07/05/putin/ (дата обращения: 28.09.2016).
12. Основные направления работы Управления «К» БСТМ МВД России. [Электронный ресурс]: Режим доступа: https://мвд.рф/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii/ (дата обращения: 28.09.2016).
13. Русская служба BBC: Иранские хакеры взломали компьютеры ГЭС под Нью-Йорком. [Электронный ресурс]. Режим доступа: http://www.bbc.com/russian/news/2015/12/151218_iran_hackers_us_dam/ (дата обращения: 28.09.2016).