Международное сотрудничество в борьбе с киберпреступностью и кибертерроризмом

Атнашев В. Р.*, Яхъеева С. Н.

Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации (Северо-Западный институт управления РАНХиГС), Санкт-Петербург, Российская Федерация; * atnashev-vr@ranepa.ru

РЕФЕРАТ

В статье рассматриваются основные подходы к определению киберпреступности, сущность и особенности кибертерроризма, определяющие направления борьбы с этими преступлениями. Необходимость и актуальность сотрудничества в рамках международных организаций обусловлена глобальным распространением этого вида преступности. Обеспечение информационной безопасности в целом является одним из приоритетных направлений деятельности региональных объединений, всего международного сообщества. Международное сотрудничество по кибербезопасности должно носить системный, комплексный и последовательный характер, но оно будет эффективным и успешным лишь при участии всех государств.

Ключевые слова: терроризм, преступность, глобализация, телекоммуникационные технологии, Интернет, террористические организации, социальные сети

International Cooperation on Cybercrime and Cyberterrorism

Vadim R. Atnashev*, Sadaf N. Yakheeva

Russian Presidential Academy of National Economy and Public Administration (North-West Institute of Management, RANEPA), St. Petersburg, Russian Federation; * atnashev-vr@ranepa.ru

ABSTRACT

The article discusses main approaches to the definition of cybercrime, nature and characteristics of cyberterrorism, that determine directions of counteracting. The necessity and urgency of cooperation within international organizations are determined by the global spread of this type of crime. Ensuring information security is one of the priorities of regional international organizations and the entire international community. International cooperation on cyber security must be systemic, integrated and consistent, but it will be effective and successful only with the participation of all states.

Keywords: terrorism, crime, globalization, telecommunication technologies, Internet, terrorist organizations, social networks

Введение

В современных условиях глобализации и информатизации компьютеры и телекоммуникационные системы активно внедряются во все сферы жизнедеятельности как отдельного человека, так и государства в целом. В связи с развитием информационных технологией и сети Интернет набирает обороты киберпреступность и кибертерроризм. Многие юристы и должностные лица считают, что кибертерроризм представляет собой серьезную угрозу человечеству, сравнимую чуть ли не с оружием массового поражения. Однако кибертерроризм не является преступлением, относящимся именно к группе преступлений террористической направленности [5, с. 315]. Данная тема весьма актуальна, поскольку количество преступлений в киберпространстве стабильно растет и очевидна необходимость четкого регулирования и контроля данной сферы.

Кибертерроризм и киберпреступность

Термин «кибертерроризм» впервые был употреблен в 1980 г. Б. Коллином, являвшимся одним из специалистов Института безопасности и разведки в Калифорнии. Данным термином он обозначил возможность террористических атак в киберпространстве [9, с. 15]. Между тем международное сообщество до сих пор не выработало единого определения понятия «кибертерроризм». Данный факт замедляет разработку методов борьбы с данным видом преступления.

По мнению Р. Р. Абсатарова, кибертерроризм можно определить как использование компьютеров в качестве оружия или целей политически мотивированными международными или национальными группами, причиняющими или угрожающими причинить ущерб и посеять панику, с целью воздействия на население или правительство для изменения политики [1, с. 173].

В целом киберпреступность имеет масштабный эффект и способна причинить существенный материальный вред. Так, самым крупным киберпреступлением в истории стало распространение в 2017 г. опаснейшего вируса WannaCrypt, его создатели атаковали немалое количество компьютеров и требовали выкуп за полученные данные. Данная кибератака причинила огромные финансовые потери многим крупным компаниям по всему миру. Как отметил международный эксперт по гармонизации законодательства в сфере киберпреступности Штайн Шольберг, «киберпространство, как пятое общее пространство, после наземного, морского, воздушного и космического, требует координации, сотрудничества и особых правовых мер на международном уровне» [10]. Кибертерроризм имеет следующие отличительные признаки:

- международный характер, заключающийся в том, что преступники и жертвы могут находиться в разных государствах;
- высокий уровень латентности и низкий уровень раскрываемости;
- отсутствие больших финансовых затрат, при этом наличие возможности нанесения огромного материального ущерба;
- открытость, выражающуюся в привлечении внимания общественности [2, с. 35].

Международное сотрудничество в борьбе с кибертерроризмом осуществляется в рамках ООН, Совета Европы, Международной организации экспертов, Интерпола, Европола. Центральная роль в координации данной борьбы отводится ООН, в особенности ее главным органам: Генеральной Ассамблее, Совету Безопасности, а также различным многосторонним неформальным партнерствам. В рамках ООН принят ряд резолюций по различным аспектам предотвращения кибертерроризма.

Применительно к киберпреступности оказываются неэффективными традиционные методы и способы борьбы с преступностью, основанные на территориальном принципе, поскольку киберпространство имеет глобальный, международный характер. Эта борьба оказывается более эффективной на региональном уровне. Это объясняется существованием следующего парадокса: с одной стороны, государства вынуждены сотрудничать для борьбы с такой транснациональной угрозой, как киберпреступность, но, с другой стороны, такое сотрудничество затрагивает суверенитет государства, ограничивает его в области уголовного права и защиты информации. Поэтому сотрудничество оказывается успешным в регионах с высоким уровнем политического доверия между странами, как это происходит в Европейском союзе.

В 2001 г. Совет Европы принял Конвенцию о киберпреступности, представляющую собой единственный документ обязательного применения, который регулирует правоотношения в области эксплуатации компьютерной сети. Данная Конвенция весьма значима не только в рамках Совета Европы, но и на глобальном уровне. Она является одним из основополагающих документов в сфере противодействия киберпреступности. Конвенцию подписали не только страны Европы, но также Аргентина, Австралия, Израиль, Япония, США, в общей сложности более 50 государств.

Тем не менее Россия не участвует в данной Конвенции. По мнению противников присоединения нашей страны к Конвенции, ст. 32 Конвенции противоречит российскому законодательству и нарушает суверенитет государства, так как предусмотренные в ней действия могут совершаться без предварительного уведомления и согласия стороны, на территории которой эти действия совершаются.

Участники Конвенции соглашаются проводить общую политику в области борьбы с киберпреступностью, принимать соответствующие акты, укреплять международное сотрудничество, не допускать нарушений конфиденциальности, целостности и доступности компьютерных систем и компьютерной информации, выявлять и расследовать уголовные преступления в информационной сфере, привлекать к уголовной ответственности соответствующих лиц, разрабатывать договоренности относительно оперативного и надежного международного сотрудничества.

Гл. 3 Конвенции посвящена международному сотрудничеству в сфере борьбы с киберпреступностью. Оно основывается на предоставлении трансграничного доступа к хранящимся компьютерным данным и на оказании взаимной правовой помощи, в том числе по сбору данных о потоках в режиме реального времени и созданию круглосуточно действующей сети (24 / 7).

Несмотря на наличие в рассматриваемой сфере других международных актов, «Конвенция является единственным признанным международным договором, … содержит нормы материального и процессуального (процедурные) права в целях противодействия киберпреступности и защиты свободы, безопасности и прав человека в интернете» [6, с. 66].

Однако данная Конвенция в некоторой степени является устаревшей и не отвечающей актуальной ситуации в связи со стремительными темпами освоения цифрового пространства и внедрения новых технологий. Поскольку Конвенция разрабатывалась в 1997–2001 гг., многие угрозы в области киберпространства на тот момент не были известны либо им не уделялось должного внимания. Весьма сложным является эффективное ведение борьбы с новыми проявлениями терроризма в информационном пространстве без его юридического определения и, соответственно, криминализации как самого понятия, так и его составляющих.

В настоящее время открытость киберпространства означает практически всеобщий доступ к любому контенту. Насущным требованием является международное сотрудничество в сфере преодоления ряда негативных последствий такой полной открытости, прежде всего в сфере противодействия наиболее серьезным транснациональным преступлениям. Возможно, и в киберпространстве должно быть создано «пространство свободы, безопасности и правосудия» по аналогии с невиртуальным пространством ЕС (ст. 3 Договора о ЕС).

Для того чтобы международное сотрудничество стран в борьбе с киберпреступностью было эффективным, необходимо унифицировать правовые нормы различных государств при регламентации действий сторон в процессе использования средств в борьбе с киберпреступлениями.

Например, Центр передового опыта НАТО в области компьютерной безопасности выпустил сборник рекомендаций «Таллинское руководство по применению международного права в кибервойне». В качестве основных задач указаны «адаптация существующих правовых норм в отношении вооруженных конфликтов под специфику враждебной деятельности в виртуальном пространстве» и попытка разработать дефиниции основных понятий в сфере компьютерной безопасности [3, с. 15].

Международное сотрудничество

Одним из ключевых направлений международного сотрудничества в борьбе с киберпреступностью является создание специализированных органов. Такими органами являются Интерпол, Европол, Евроюст. Поскольку информационная безопасность государства связана с его суверенитетом, то на глобальном уровне создание единого органа, который бы координировал взаимодействие

государств по борьбе с киберпреступностью, затруднительно, однако создаются вспомогательные органы, руководствующиеся едиными стандартами деятельности, обобщающими практику разных стран по вопросам борьбы с киберпреступностью.

В рамках ЕС существенное значение имеет Европол и Евроюст. Работа Европола основана на системе аналитических рабочих картотек, формируемых из сосредоточенных в его информационной системе данных в целях анализа, определяемого как обработка или использование данных для поддержки уголовных расследований.

Евроюст координирует действия правоохранительных органов различных государств по вопросам расследования киберпреступности, оказывает помощь в проведении расследований по запросу соответствующего органа публичной власти стран — участниц ЕС, предоставляет правоохранительным органам этих стран информацию о проводимых расследованиях в отношении киберпреступников.

Как справедливо указывает в своей диссертации Е. А. Климова, основополагающие документы в сфере борьбы с преступностью должны быть максимально четкими, не противоречить Европейской Конвенции о защите прав человека и основных свобод 1950 г. и, напротив, расширять права, которые она предоставляет [4, с. 28–29].

В этой связи можно вспомнить, что еще в 2011 г., в преддверии первой международной конференции по киберпространству, Уильям Хейг отметил, что «репрессивные правительства используют передовые технологии в целях нарушения прав своих граждан, ограничения конфиденциальности информации и свободы слова, блокируя информацию, доступ к которой многие из нас считают само собой разумеющимся».

Международное противодействие киберпреступности ведется также в рамках НАТО. К примеру, в 2013 г. было завершено развертывание единой системы НАТО по реагированию на компьютерные угрозы, включающей центры по реагированию на угрозы в киберпространстве в Брюсселе и Монсе. Также осуществляются проверки эффективности уже созданной системы отражения кибератак, например, ежегодно проводятся учения «Киберкоалиция», «Защитный шар» [7, с. 370].

Международное сотрудничество в борьбе с киберпреступностью осложняется расхождением позиций различных государств мира, обусловленным базовыми различиями в подходах к определению понятий, отсутствием четкого понимания границ между различными явлениями, требующими разных механизмов сотрудничества, различием в подходах к обеспечению безопасности персональных данных, общим уровнем взаимного недоверия, что делает невозможным сотрудничество по вопросам трансграничного процессуального партнерства. В силу этого в ООН был отклонен предложенный Россией и Китаем проект глобальной Конвенции по киберпреступности в 2010 г. [8, с. 97].

Международное сотрудничество в данной сфере включает в себя также создание различных международных организаций, главной целью которых является пресечение действий организованных преступных сетей. Так, в 2013 г. в Гааге был открыт Европейский центр по борьбе с киберпреступностью, который собирает и обрабатывает материалы по киберпреступности, а также разрабатывает меры по их расследованию. В 2015 г. Интерпол инициировал открытие Международного центра по борьбе с киберпреступностью в Сингапуре. Перечисленные организации выявляют и проводят анализ киберугроз и IT-преступлений, а также обмениваются глобальным передовым опытом по борьбе с преступностью в киберпространстве.

Что касается России, то наша страна активно участвует в международном сотрудничестве по киберпространству, несмотря на то, что Стратегия национальной безопасности не содержит термина «кибертерроризм».

Еще в январе 2015 г. участники Шанхайской организации сотрудничества внесли на рассмотрение Генеральной Ассамблеи ООН Международный кодекс поведения в области информационной безопасности, являющийся первым международным документом, посвященным нормам поведения в информационной среде. Документ имеет следующие цели:

– определить права и обязанности государств в информационном пространстве;
– стимулировать конструктивное и ответственное поведения государства;
– укреплять сотрудничество против угроз и вызовов в информационном пространстве.

Наконец, в декабре 2018 г. ГА ООН приняла резолюцию «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», которая была поддержана 119 государствами, 46 стран проголосовали против, 14 воздержались. Поскольку содержащийся в резолюции кодекс поведения государств в интернете имеет рекомендательный характер, ведется работа по разработке конвенции ООН по международной информационной безопасности.

Результаты

Подводя итоги, стоит отметить, что угроза кибертерроризма будет возрастать и дальше, по мере развития информационных технологий. Кибертерроризм наносит вред как отдельным гражданам, так и различным организациям и даже государствам. Поэтому эффективное международное сотрудничество в обеспечении информационной безопасности имеет все большее значение. Весьма продвинулся в сфере борьбы с кибертерроризмом Европейский союз. Знания и опыт, накопленные Европейским союзом, могут сыграть важную роль в достижении глобальной международной безопасности.

Международное сотрудничество в борьбе с кибертерроризмом осложняется особенностями данного вида преступности. Для оптимизации борьбы с кибертерроризмом необходимо в первую очередь участие всех государств, поскольку кибертерроризм имеет транснациональный характер. Необходимо закрепление на международном уровне понятия «кибертерроризм», а также проведение унификации правовых норм в этой сфере с участием всех государств. Также необходимо создать систему координации и взаимодействия всех существующих служб противодействия кибертерроризму как внутри отдельного государства, так и на международном уровне. Только комплекс мер, включая вышеперечисленные, и участие каждого государства сделают международное сотрудничество в данной сфере эффективным и успешным.

Литература

1. *Абсатаров Р. Р.* Противодействие компьютерному терроризму // Современная юриспруденция: актуальные вопросы, достижения и инновации. Сборник статей VI Международной научно-практической конференции. 2018. С. 172–174.
2. *Бояркин А. И., Мокрецова Н. М.* К проблеме борьбы с киберпреступностью // Культура народов в социальном пространстве и времени. 2018. С. 33–38.
3. *Градов А.* Деятельность Североатлантического союза в сфере кибербезопасности // Зарубежное военное обозрение. 2014. № 7. С. 13–16.
4. *Климова Е. А.* Правовые основы полицейского и судебного сотрудничества по уголовным делам в праве Европейского союза / Автореферат дисс. к. ю. н. М., 2011.
5. *Романовский Г. Б., Безрукова О. В.* Проблемы противодействия терроризму в современном мире // Национальная безопасность в современной России: стратегия противодействия экстремизму и терроризму и перспективы преодоления глобальных проблем. Материалы Всероссийской научной конференции: в 2 томах. 2016. С. 310–318.
6. *Химченко И. А.* Информационное общество: правовые проблемы в условиях глобализации: дис. ... канд. юрид. наук: 12.00.13 / И. А. Химченко. М., 2014. 174 с.
7. *Якимова Е. М., Нарутто С. В.* Международное сотрудничество в борьбе с киберпреступностью // Всероссийский криминологический журнал. 2016. Т. 10. № 2. С. 369–378.
8. *Brenner S.* Cyberthreats and the Decline of the Nation-State. Routledge, 2014.
9. *Collin B. C.* The Future of Cyber Terrorism // Crime & Justice International. 1997. Vol. 13, No. 2. March. P. 15–18.
10. *Schjolberg Stein.* A Cyberspace Treaty — A United Nations Convention or Protocol on Cyber-Security and Cybercrime. Twelfth United Nations Congress on Crime Prevention and Criminal Justice. Salvador, Brazil, 12–19 April 2010.

Об авторах:

Атнашев Вадим Рафаилович, доцент кафедры международного и гуманитарного права Северо-Западного института управления РАНХиГС (Санкт-Петербург, Российская Федерация), кандидат филологических наук; atnashev-vr@ranepa.ru

Яхъеева Садаф Нумонжоновна, магистрант кафедры международного и гуманитарного права Северо-Западного института управления РАНХиГС (Санкт-Петербург, Российская Федерация); yakheevasn@gmail.com

About the authors:

Vadim R. Atnashev, Associate Professor, the North-West Institute of Management of RANEPA, Department of International and Humanitarian Law (St. Petersburg, Russian Federation), PhD in Philological Sciences; atnashev-vr@ranepa.ru

Sadaf N. Yakheeva, Graduate student of the Department of International and Humanitarian Law, the North-West Institute of Management of RANEPA (St. Petersburg, Russian Federation); yakheevasn@gmail.com