К ВОПРОСУ О КИБЕРТЕРРОРИЗМЕ И КИБЕРПРЕСТУПНОСТИ

А.А. Галушкин

Кафедра судебной власти, правоохранительной и правозащитной деятельности
Российский университет дружбы народов
ул. Миклухо-Маклая, 6, Москва, Россия, 117198

В статье автор анализирует угрозы современного общества, вызванные широким распространением информационных технологий и смещением части правонарушений в глобальную информационно-телекоммуникационную сеть Интернет.

Ключевые слова: кибертерроризм, киберпреступность, информационная безопасность, режим доступа, угрозы.

Не единственной, но одной из важных составляющих национальной информационной безопасности является безопасность в сфере глобальной информационно-телекоммуникационной сети Интернет.

В отличии от классических правонарушений, совершаемых обычно в конкретном месте в пространстве, правонарушения, совершаемые с использованием глобальной информационно-телекоммуникационной сети Интернет, подчас не только не привязаны к конкретной географической точке, но и не представляется возможным определить, в каком государстве они совершены.

«Сегодня можно говорить, что Интернет охватывает все страны мира, так как с применением новых технологий (использование мобильных спутниковых устройств связи) возможно подключение к сети Интернет с любой точки земного шара. Если же говорить о развернутой инфраструктуре, то в таком контексте Интернет охватывает сегодня более 150 стран мира» [2]. При этом как международные [3], так и национальные [8] и локальные акты [5], а также обычаи [4. С. 3–4] регулируют в той или иной мере деятельность в информационно-телекоммуникационной сфере. Некоторые авторы придерживаются мнения, что «организационно-правовые основы обеспечения информационной безопасности исходят из того, что информация подпадает под нормы вещного права» [7].

Несмотря на то, что большая часть граждан и организаций пользуется услугами связи крупных провайдеров, предоставляющих телематические услуги, услуги связи и передачи данных полностью официально и открыто, существует значительное количество организаций, предоставляющих услуги связи анонимно.

В основном к таким организациям относятся иностранные дата-центры, хостинг-компании и интернет-провайдеры, официально предоставляющие услуги по анонимизации соединения (VPN, Proxy, Socks и др.), а также предоставляющие антиабузный (безабузный) виртуальный хостинг, виртуальный выделенный сервер, а также предоставляющие в аренду оборудование и каналы связи.

Безусловно, цены данных услуг на порядок выше цен на аналогичные белые услуги (услуги, предоставляемые компаниями, отслеживающими цели использования данных услуг и реагирующих на заявления граждан и организаций о нарушении их прав), однако клиенты получают полную анонимность и фактическую безнаказанность (обычно максимальное наказание, которое ожидает правонарушителей — это прекращение предоставления им услуг в данной организации).

Но далеко не всегда правонарушители пользуются услугами иностранных организаций. Часто в России значительно проще приобрести SIM-карту, оформленную на подставное лицо или вовсе безымянную. В этом случае бесполезно отслеживать номинального абонента, а специальными средствами возможно отследить только MAC-адрес устройства, места подключения к сети провайдера, а также в ряде случаев отследить трафик с устройства.

Также, в последнее время приобретают все большую популярность точки бесплатного доступа к Интернету через Wi-Fi, что позволяет правонарушителю анонимно подключаться к сети Интернет, чаще всего фактически не оставляя следов.

Лица, обладающие достаточными знаниями в сфере информационно-телекоммуникационных технологий и обладающие достаточным опытом их применения, активно используют различные технологии по маскировке и/или фальсификации их личности, таким образом избегая наказания за противоправные действия.

В то же время отечественное законодательство, равно как и законодательство многих зарубежных стран, отстает от скорости развития информационных технологий и не дает правоохранителям, сотрудникам юстиции и др. достаточно правовых инструментов для обеспечения должного уровня законности и правопорядка, а также оперативного расследования правонарушений и привлечения виновных лиц к установленной законом и справедливой ответственности.

К сожалению, у ряда законодателей и прочих граждан бытует ошибочное мнение об отсутствии необходимости дополнительно законодательно регулировать правоотношения в сети Интернет и вводить административную или уголовную ответственность, что подчеркивает их непонимание ситуации и слабую осведомленность в данной области.

По данным проведенного автором опроса, из 1000 опрошенных в Москве, Санкт-Петербурге и Нижнем Новгороде россиян — физических лиц 84% опрошенных хотя бы раз в течение последних пяти лет сталкивался с правонарушениями в сети Интернет, а 68% опрошенных пострадало от противоправных действий, и лишь 3% сообщили, что виновные лица были найдены и понесли наказание за свои действия. При этом большинство опрошенных отметили, что соответствующие государственные органы не были заинтересованы в расследовании правонарушений.

Опрошенными были отмечены такие правонарушения, как:

– несанкционированное использование персональных данных;

– нарушение авторских прав;

– несанкционированный доступ к информации (в том числе повлекший хищение денежных средств);

– незаконное предпринимательство;

– клевета; и др. [1].

Между тем еще с большими угрозами сталкиваются коммерческие компании, некоммерческие, государственные и муниципальные организации и учреждения, международные организации, общественные организации. Правонарушители часто безнаказанно получают несанкционированный доступ к их сетям, серверам, сайтам, учетным записям, что, в свою очередь, влечет несанкционированный доступ к информации (в том числе чтение, изменение, удаление), хищение персональных данный клиентов, получение информации, составляющей коммерческую тайну или ноу-хау, хищение денежных средств, наносит вред имиджу и приносит к невозвратным потерям упущенной выгоды.

Органы государственной власти и местного самоуправления подчас подвергаются еще большему воздействию киберпреступников и кибертеррористов, организующих хищение данных из государственных информационных систем и/или препятствующих их нормальной работе. В качестве примера, «одна из первых подобных кибервойн произошла в апреле 2007 г., когда в связи с решением эстонского правительства о переносе памятника Воину-Освободителю организованным атакам подверглись сайты государственных структур этой страны. Крайне болезненным этот удар стал вследствие наличия в Эстонии развитой системы так называемого электронного государства, к которой так активно стремятся перейти не только европейские, но и ведущие азиатские страны. Благодаря ей большая часть государственного делопроизводства в этой балтийской стране ведется в электронном виде: через Интернет транслируются заседания правительства, здесь можно заполнить анкету на получение паспорта, оплатить коммунальные счета и даже проголосовать…» [6].

Для лучшего понимания проблемы видится целесообразным более подробно остановиться на понятии кибертерроризма и кибепреступности.

В отечественной научной литературе определение компьютерного терроризма (кибертерроризма) и правонарушений, равно как и преступлений в сфере высоких технологий (киберпреступлений), а также взаимосвязанных вопросов рассматриваются достаточно слабо. Следует отметить труды В.И. Антюхова, Ю.В. Гаврилова, В.А. Голубева, Ю.И. Жукова, В. Замкового, М. Ильчикова, В.Е. Кадулина, Е.П. Кожушко, В.А. Мазурова, А.И. Примакина, Л.В. Смирнова и др.

По мнению автора, особый интерес вызывает мнение В.А. Голубева, считающего, что «под компьютерным терроризмом (кибертерроризмом) следует понимать преднамеренную, политически мотивированную атаку на информацию, обрабатываемою компьютером, компьютерную систему и сети, которая создает опасность для жизни или здоровья людей или наступления других тяжких последствий, если такие действия были содеяны с целью нарушения общественной безопасности, запугивания населения, провокации военного конфликта. Под компьютерным терроризмом (кибертерроризмом) следует понимать запугивание населения и органов власти с целью достижения преступных намерений. Это проявляется в угрозе насилия, поддержания состояния постоянного страха с целью достижения определенных политических или иных целей, принуждения к определенным действиям, привлечения внимания к личности кибертеррориста или террористической организации, которую он представляет. Причинение или угроза причинения вреда есть своеобразным предупреждением о возможности причинения более тяжких последствий, если условия кибертеррориста не будут выполнены.

Характерной особенностью кибертерроризма и его отличием от киберпреступности есть его открытость, когда условия террориста широко оповещаются. Кибертерроризм — это серьезная угроза человечеству, сравнимая с ядерным, бактериологическим и химическим оружием, причем степень этой угрозы в силу своей новизны не до конца еще осознана и изучена. Опыт, который уже имеется у мирового сообщества в этой области, со всей очевидностью свидетельствует о несомненной уязвимости любого государства, тем более что кибертерроризм не имеет государственных границ, кибертеррорист способен в равной степени угрожать информационным системам, расположенным практически в любой точке земного шара. Обнаружить и нейтрализовать виртуального террориста весьма сложно из-за слишком малого количества оставляемых им следов, в отличие от реального мира, где следов содеянного остается все же больше. Особую озабоченность у правоохранительных органов вызывают террористические акты, связанные с использованием глобальной сети Интернет, из открытых источников которой, как утверждает ФБР, можно получить технологию изготовления биологического, химического и даже ядерного оружия террористов [2].

Как справедливо отметил Советник Президента Российской Федерации В.Ф. Яковлев, «у нас сейчас есть две важные социальные сферы, в которых право пока еще, к сожалению, слабо представлено. Первая — это Интернет. Интернет — величайшее благо, пока оно не превратилось в величайшее зло» [9].

С учетом вышеизложенного возникает необходимость обеспечения должного уровня правового регулирования глобальной информационно-телекоммуникационной сети Интернет на международном уровне и российского сегмента информационно-телекоммуникационной сети Интернет на национальном уровне, в том числе принятия Федерального закона «О Российском сегменте информационно-телекоммуникационной сети Интернет».

Законодательное определение базовых норм и принципов работы в российском сегменте информационно-телекоммуникационной сети Интернет, с одной стороны, позволит определить круг дозволенного поведения пользователей, а с другой стороны, установить уголовную и административную ответственность, соответствующую современным реалиям и уровню развития общества. Без должного уровня правовой культуры пользователей российского сегмента информационно-телекоммуникационной сети Интернет и наличия реально действующих механизмов привлечения правонарушителей к ответственности невозможно полноценное существование цивилизованного гражданского общества в современном глобализированном мире информационных технологий.

ЛИТЕРАТУРА

[1] *Галушкин А.А.* К вопросу о преступлениях и правонарушения в отечественном сегменте глобальной информационно-телекоммуникационной сети Интернет // Правозащитник. — 2014. — № 1.
[2] *Голубев В.А.* Кибертерроризм как новая форма терроризма // Центр исследования проблем компьютерной преступности (Crime-reserarch.org). URL: http://www.crime-research.org/library/Gol_tem3.htm.
[3] *Гусева К.А.* Конвергенция международного и национального права; глобализация? // Правозащитник. — 2012. — № 1.
[4] *Енгибарян Р.В.* Исламский вызов // Право и управление. XXI век. — 2013. — № 2 (27).
[5] *Итиуридзе Л.А.* Управление политикой доступа к информации // Правовая инициатива. — 2013. — № 8.
[6] *Ревский А.* Кибертерроризм — виртуальный инструмент реальной войны. URL: http://www.ia-centr.ru/expert/14170.
[7] *Чесноков Н.А.* Правовые основы информационной безопасности в современных условиях // Правовая инициатива. — 2013. — № 4.
[8] *Шилов С.А.* КоАП РФ: проблематика, правоприменительная практика // Правозащитник. — 2012. — № 1.
[9] *Яковлев В.Ф.* Публичный доклад советника Президента Российской Федерации по правовым вопросам // Правовая инициатива. — 2013. — № 2.

TO THE QUESTION OF CYBERTERRORISM AND CYBERCRIME

A.A. Galushkin

The Department of Judicial Authority, Law-Enforcement and Human Rights Activity
Peoples' Friendship University of Russia
6, Miklukho-Maclaya st., Moscow, Russia, 117198

In the present article author analyzes threats of modern society caused by a wide circulation of information technologies and shift of the part of offenses in the global information and telecommunication network Internet.

Key words: cyberterrorism, cybercrime, information security, mode of access, threat.

REFERENCES

[1] *Galushkin A.A.* K voprosu o prestuplenijah i pravonarushenija v otechestvennom segmente global'noj informacionno-telekommunikacionnoj seti Internet // Pravozashhitnik. — 2014. — № 1.

[2] *Golubev V.A.* Kiberterrorizm kak novaja forma terrorizma // Centr issledovanija problem komp'juternoj prestupnosti (Crime-reserarch.org). URL: http://www.crime-research.org/library/Gol_tem3.htm.

[3] *Guseva K.A.* Konvergencija mezhdunarodnogo i nacional'nogo prava; globalizacija? // Pravozashhitnik. — 2012. — № 1.

[4] *Engibarjan R.V.* Islamskij vyzov // Pravo i upravlenie. XXI vek. — 2013. — № 2 (27).

[5] *Itiuridze L.A.* Upravlenie politikoj dostupa k informacii // Pravovaja iniciativa. — 2013. — № 8.

[6] *Revskij A.* Kiberterrorizm — virtual'nyj instrument real'noj vojny. URL: http://www.ia-centr.ru/expert/14170.

[7] *Chesnokov N.A.* Pravovye osnovy informacionnoj bezopasnosti v sovremennyh uslovijah // Pravovaja iniciativa. — 2013. — № 4.

[8] *Shilov S.A.* KoAP RF: problematika, pravoprimenitel'naja praktika // Pravozashhitnik. — 2012. — № 1.

[9] *Jakovlev V.F.* Publichnyj doklad sovetnika Prezidenta Rossijskoj Federacii po pravovym voprosam // Pravovaja iniciativa. — 2013. — № 2.