Терлыч Илья Анатольевич
магистрант
ФГБОУ ВО «Кубанский государственный
аграрный университет им. И.Т. Трубилина»
г. Краснодар, Краснодарский край

УГОЛОВНО-ПРАВОВОЙ АСПЕКТ БОРЬБЫ С КИБЕРТЕРРОРИЗМОМ В КИТАЕ

Аннотация*: в статье рассматривается соотношение понятий «киберпреступление» и «кибертерроризм». Анализируется законодательство Китая в сфере противодействия совершению кибертерроризма.*

Ключевые слова*: Китай, уголовное право, киберпреступность, кибертерроризм, квалификация преступлений, уголовное право.*

Как в отечественных, так и в зарубежных научных трудах и средствах массовой информации в последнее время стали использоваться различные термины, обозначающие криминальные проявления в информационной сфере. Можно встретить такие термины, как «компьютерная преступность», «кибербандитизм», «киберпреступность» и другие. Термин «киберпреступность», зачастую, употребляется наряду с термином «компьютерная преступность». Однако, нередко эти понятия используются как синонимы. Данные понятия близки по смыслу, но все же не являются тождественными. Понятие «киберпреступность» (в англоязычном варианте – cybercrime) шире, чем «компьютерная преступность» (computer crime), и более точно отражает природу такого явления, как преступность в информационном пространстве. Оксфордский толковый словарь определяет приставку «cyber-» как компонент сложного слова. Ее значение – относящийся к информационным технологиям, сети Интернет, виртуальной реальности. Схожее по смыслу определение содержит Кембриджский словарь. Таким образом, «cybercrime» – это преступность, связанная как с использованием компьютеров, так и с использованием информационных технологий и глобальных сетей. В то же время термин «computer crime» в основном относится к

преступлениям, совершаемым против компьютеров или компьютерных данных [1, с. 67–68].

Стремительное развитие информационных технологий привело к массовому использованию во всем мире Интернета. С развитием киберпреступлений стали формироваться ее различные направления, в том числе кибертерроризм. Впервые понятие «кибертерроризм» было использовано старшим научным сотрудником Калифорнийского института безопасности и разведки Барри Коллином в 1980 году, считающим, что в будущем Интернет и киберсети будут охватывать весь мир и станет объектами террористических атак.

Подходы к определению преступлений террористического характера в уголовном законодательстве множества зарубежных стран вызывают интерес теоретиков уголовного права на всем протяжении становления рассматриваемой категории уголовно наказуемых деяний [7, с. 30–33].

В настоящее время кибертерроризмом, то есть, терроризмом в сети Интернет, можно рассматривать с нескольких точек зрения. Во-первых, совершение терактов через информационные сети, когда Интернет выступает как способ и средство совершения преступления. Во-вторых, деятельность, содействующая терроризму, в том числе, вербовка в террористические организации, сбор средств для террористов и многое другое [2, с. 3–9]. Практика совершения терактов через Интернет и иные информационные сети еще не получила широкого применения, однако, использование сети Интернет в качестве вспомогательного средства совершения преступлений применяется террористическими организациями в их деятельности.

Китай является одной из первых стран в мире по числу пользователей сети Интернет, как среди физических, так и юридических лиц, что делает ее уязвимой к любым проявлениям киберпреступности, в том числе кибертерроризму. Именно поэтому в КНР приняты и широко используются различные меры по защите от киберпреступлений. Впервые уголовная ответственность за посягательства на компьютерную безопасность была введена Постановлением Государственного Совета Китайской Народной Республики «О компьютерной

безопасности информационных систем» от 18 февраля 1994 г. №147. Следующим шагом по борьбе с киберпреступлений стало вступление в силу новой редакции Уголовного кодекса Китая, принятого в 1997 году [3, с. 12–16].

Одной из самых известных мер, принятых для противодействия киберпреступлениям, в том числе, кибертерроризму, является так называемый «Золотой щит». Это электронный барьер, действующий на территории всей страны и фильтрующий потоки информации, так, что данные пользователей проходят через ограниченное число контрольно-пропускных пунктов (шлюзов), управляемых ограниченным числом компаний, предоставляющих доступ в Интернет [4, с. 1–20]. Проект был запущен еще в 1998 году и полностью завершен в 2006 году, когда весь Интернет в стране оказался под контролем государства. С этого времени любой интернет-пользователь, находящийся на территории Китая, не может получить доступ к сайтам, распространяющим террористические сведения или призывы, а также к любой другой информации протеррористического толка.

По обзору статистических данных, как отметил в октябре 2017 года представитель Генпрокуратуры Китая Ван Сунмяо, можно обнаружить рост числа возбужденных дел по киберпреступлениям. Так, за первые девять месяцев 2017 года ведомство предъявило обвинение по 334 делам, что на 82,5% больше, чем год назад. Анализируя же в географическом разрезе страны, из которых осуществляются сетевые атаки, можно увидеть, что за 2015 год Первые четыре места не изменились по сравнению с 2014 г.: США (24,15%), Германия (13,03%), Нидерланды (10,68%) и Россия (8,98%). Показатель каждой из этих стран уменьшился на несколько процентных пунктов. Франция (5,07%) набрала 2,08 п.п. и поднялась с седьмого места на пятое, Украина (4,16%) опустилась с пятого на седьмое место. Выбыли из top-10 Канада и Вьетнам, а новички – Китай (2,97%) и Швеция (1,95%) – разместились на девятом и десятом месте соответственно [5, с. 36–38].

Также законодательство Китая активно развивается в сфере противодействия киберпреступлений. На сегодняшний день в УК КНР значительное количество статей полностью или частично посвящено киберпреступлениям [6, с. 64–

72]. Кроме статей, включенных в УК КНР в 1997 г., изменена ст. 246 кодекса. Она предусматривает ответственность за оскорбление через информационные сети, повлекшие серьезные последствия. Статья 287а устанавливает уголовную ответственность за пособничество в совершении преступлений через информационные сети.

Таким образом, на основании проведенного исследования можно сделать следующие выводы: Кибертерроризм является разновидностью киберпреступлений, и с активным развитием Интернета начинает представлять серьезную общественную опасность во всем мире. Китай, столкнувшийся с кибертерроризмом раньше многих стран, показал, что противодействие терроризму в Интернете возможно и необходимо антитеррористическое законодательство, а также улучшать и развивать антитеррористическую практику в указанной сфере.

Список литературы

1. Журавленко Н.И. Проблемы борьбы с киберпреступностью и перспективные направления международного сотрудничества в этой сфере / Н.И. Журавленко, Л.Е. Шведова // Общество и право. – 2015. – №3 (53). – С. 67–68.

2. Федоров А.В. Основные тенденции международного терроризма и меры борьбы с ним / А.В. Федоров, Д.Н. Сергеев // Российский следователь. – 2016. – №24. – С. 3–9.

3. Li P. Ordinance of the People's Republic of China on the Protection of Computer Information System Security / P. Li // Chinese Law & Government. – 2010. – Vol. 43, iss. 5. – P. 12–16.

4. Navarria G. China: the Party, the Internet, and power as shared weakness / G. Navarria // Global Change, Peace and Security. – 2016. – Vol. 29. – P. 1–20.

5. Валько Д.В. Киберпреступность в России и мире: сопоставительная оценка // Управление в современных системах. – 2016. – №3 (10). – С. 36–37.

6. Шивдяков Л.А. Кибертерроризм как новая и наиболее опасная форма терроризма / Л.А. Шивдяков // Защита информации. Инсайд. – 2009. – №2 (26). – С. 64–72.

7. Сильченко Е.В. Сравнительно-правовая характеристика преступлений, предусмотренных ст.205 (Террористический акт) Уголовного кодекса Российской Федерации и ст. 289 (Акт терроризма) Уголовного кодекса Республики Беларусь / Е.В. Сильченко, Н.А. Наджаф // Наука сегодня: глобальные вызовы и механизмы развития: материалы международной научно-практической конференции: в 2 ч. – Научный центр «Диспут», 2017. – С. 30–33.