ПОНЯТИЕ КИБЕРТЕРРОРИЗМА В ЗАКОНОДАТЕЛЬСТВЕ РОССИИ И РЕСПУБЛИКИ ИРАК

THE TERM OF CYBER TERRORISM IN THE LEGISLATION OF RUSSIA AND THE REPUBLIC OF IRAQ

M. Madjid

Summary. The relevance of this article is associated with an increasing number of terrorist acts, which in recent years cover an increasing number of countries, mostly in the Middle East. This article discusses the term of "cyber terrorism" and its difference from other forms of terrorism. The features of the Russian and Iraqi legislation in terms of the definition of this concept are analyzed. In conclusion, the author proposed in Russian legislation to toughen criminal liability for the recruitment of persons for terrorist acts.

Keywords: terrorism, cyber terrorism, terrorist organization, recruitment, Law on the fight against terrorism.

Маджид Мохаммед Али
Аспирант, Нижегородский государственный университет им. Н. И. Лобачевского, г. Нижний Новгород, Россия
mamh35@yahoo.com

Аннотация. Актуальность данной статьи связана с возрастающим количеством террористических актов, которые в последние годы охватывают все большее количество стран, особенно на Ближнем Востоке. В данной статье рассмотрено понятие «кибертерроризм» и его отличие от иных форм терроризма. Анализируются особенности российского и иракского законодательства в части определения данного понятия. В заключении, автором предложено в российском законодательстве ужесточить уголовную ответственность за вербовку лиц для совершения террористических актов.

Ключевые слова: терроризм, кибертерроризм, террористическая организация, вербовка, Закон о борьбе с терроризмом.

Стремительное развитие информационных технологий оказало влияние на все сферы жизни общества. В результате одним из распространенных способов совершения преступлений стало использование сети Интернет, при котором преступнику для совершения деяния необязательно входить в прямой контакт с жертвой, а достаточно просто воспользоваться электронной сетью. При этом преступник может оказывать влияние не только на одного конкретного человека, но и на группы людей. Таким образом, научно-техническая революция вместе со всеми преимуществами принесла и серьезные проблемы в сфере общественной безопасности. Именно к использованию электронной сети зачастую прибегают представители террористических групп для вербовки людей. В связи со сложностями государственного контроля за интернет-информацией сайты социальных сетей (Facebook, Twitter, YouTube, Instagram и другие) стали важным инструментом террористических групп для распространения своих идей и вербовки новых членов.

Сетевые преступления называют электронными преступлениями, или «киберпреступлениями». В общем смысле, киберпреступление можно определить, как преступление, совершенное в электронной сфере посредством электронной системы или сети Интернет против общественных интересов [6].

Суть кибертерроризма заключается в осуществлении противоправного воздействия на цифровые системы, совершенного в целях создания опасности причинения вреда жизни, здоровью или имуществу неопределенного круга лиц путем создания условий для аварий и катастроф техногенного характера либо реальной угрозы такой опасности [1].

Характеризуя особенности электронных преступлений, в первую очередь, можно выделить чрезвычайную скрытность деяний, которая достигается посредством применения механизмов анонимности и шифрования. Также можно выделить трансграничность, под которой подразумевается удаленность преступника от жертвы во время совершения деяния [9]. В качестве специфических особенностей можно выделить автоматизированность и нестандартность методов совершения деяния. В рамках настоящей статьи речь пойдет о такой разновидности электронных преступлений, как «кибертерроризм».

Российские эксперты рассматривают кибертерроризм как преднамеренные атаки на информационные данные, обрабатываемые компьютером, компьютерную систему или сеть, которая создает опасность для жизни и здоровья людей или наступления других тяжких последствий, если такие действия были совершены с целью нарушения общественной безопасности, запугивания населения или провокации военного конфликта [2].

Кибертерроризм можно разделить на два вида [3]:

- совершение с помощью компьютеров и компьютерных сетей террористических действий;

- использование киберпространства в целях террористических групп, но не для непосредственного совершения терактов.

Причины и мотивы электронного терроризм многочисленны и разнообразны, однако в целом они схожи с причинами обычного терроризма, поскольку электронный терроризм является одной из форм терроризма в целом. Существует ряд факторов, которые делают электронный терроризм удобным и простым оружием для террористических групп и организаций.

Наиболее важными проявлениями и формами кибертерроризма являются следующие: обмен террористической информацией и ее распространение через информационные сети, создание пропагандистских веб-сайтов, атаки на веб-сайты и электронные данные, информационные системы, запугивание и промышленный шпионаж [7; 10; 11].

Террористические атаки в цифровую эпоху обычно направлены на достижение трех основных целей: военных, политических и экономических.

Террористические группировки постоянно нуждаются в пополнении своих рядов. По статистике срок активной деятельности одного террориста составляет около трёх лет. Затем террорист либо погибает, выполняя очередную «миссию», либо его удается привлечь к уголовной ответственности [16]. Иными словами, террористические организации на постоянной основе теряют сторонников. Для пополнения своих рядов террористические группировки осуществляют вербовку людей. Вербовку можно определить, как привлечение людей к участию в террористическом акте, его подготовке, а также к пропаганде терроризма.

В виртуальном пространстве наблюдается тенденция, при которой целенаправленно ведется психологически грамотная работа «идеологов» международного терроризма в отношении наиболее уязвимых групп населения, когда в сети представители террористических групп создают аккаунты и входят в доверие к обычным гражданам. Так, например, под контролем террористической организации «ИГ» («Исламское государство», запрещена в РФ) находится целый ряд информационных агентств, печатных и электронных средств массовой информации Сирии, Ирака, Саудовской Аравии и ряда других стран. Данной террористической организацией создана разветвленная сеть интернет-ресурсов, насчитывающая более пятисот сайтов и тысячи аккаунтов в социальных сетях, которые содержат информацию террористического и экстремистского характера. В основном данная информация направлена на ознакомление с историей возникновения данной террористической организации, ее основными целями, наиболее «известными делами» и биографией ключевых представителей террористической организации [16].

Можно выделить две основные группы людей, которые вербуются в террористические организации. К первой группе относятся люди, обладающие знаниями в инженерии. Данные специалисты необходимы террористическим группам для разработки средств совершения террористических актов. Ко второй группе можно отнести обычных, некомпетентных, неквалифицированных людей, которых используют именно для совершения террористических актов [4].

Способы борьбы с кибертерроризмом не разработаны в полной мере. В большинстве стран за совершение террористических киберпреступлений законодательство устанавливает уголовную ответственность.

Так в части 2 статьи 205.2 Уголовного Кодекса Российской Федерации (далее — УК РФ) установлена повышенная уголовная ответственность за публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганду терроризма с использованием электронных или информационно-телекомуникационных сетей, в том числе сети интернет. На наш взгляд, это существенный шаг в борьбе с кибертерроризмом в России [12].

Однако в статье 205.1 УК РФ, устанавливающей уголовную ответственность за вербовку лиц для совершения террористических преступлений, повышенная ответственность при использовании электронных или информационно-телекомуникационных сетей, в том числе сети Интернет, не установлена, что можно рассматривать в качестве недоработки российских законодателей.

Законодательство Ирака не содержало понятия терроризма до 2005 г., в котором был принят закон № 13 о борьбе с терроризмом. Принятие этого закона было необходимо в обстоятельствах, сложившихся в Ираке после событий 2003 г., что вызвало значительный рост числа террористических операций. Согласно статье 1 Закона № 13 от 2005 г., под террористическим преступлением следует понимать «создание террора, страха и паники среди людей или хаоса в рамках государственной или частной собственности с целью нарушения правопорядка, безопасности или дестабилизации национального единства» [5; 14].

Иракские законодатели предлагают отнести к электронному терроризму агрессию, запугивание или угрозы через использование электронных средств, с учетом всех видов агрессии и форм коррупции.

Заключение

Следовательно, терроризм является общественно-опасным явлением, который приобретает новые формы. Терроризм получил широкое распространение посредством сети Интернет, что представляет угрозу для общества не только одного государства, но и мира в целом. Самой главной проблемой является вербовка людей в террористические организации посредством Интернета, в связи с чем, необходимо применение мер по минимизации воздействия террористических организаций на население.

Можно утверждать, что электронный терроризм — это терроризм ближайшего будущего в силу своей универсальности и разнообразия его методов и целей, которые могут быть атакованы с помощью информационно-коммуникационных технологий в достаточно спокойной обстановке, вдали от самого места свершения терактов, зачастую в режиме «инкогнито», что обеспечивает безопасность и защиту для террористов. Данный вид терроризма направлен на разрушение ИКТ инфраструктуры и подвергает современное общество неожиданным и мало предсказуемым рискам.

Высокая степень зависимости современных государств от информационно-коммуникационных сетей станет тем фактором, который позволит террористам достигать своих целей и подрывать сущность современных технологий, которые должны быть служить человечеству и способствовать распространению знаний, а также научной и культурной коммуникации.

Как было показано, в российском законодательстве требуется ввести повышенную уголовную ответственность вербовку лиц для совершения террористических преступлений с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети Интернет.

Иракское законодательство также нуждается в доработке с целью законодательного отделения понятия «кибертерроризм» от «терроризма» и установления повышенной уголовной ответственности за вербовку лиц для совершения террористических актов. По мнению автора, данные меры будут способствовать снижению количества таких актов, которые негативно отражаются как на экономическом состоянии, так и на инвестиционном климате страны.

ЛИТЕРАТУРА

1. Будник Г. И. Кибертерроризм как угроза основам конституционного строя Российской Федерации: понятие, сущность и проблемы противодействия // Молодой ученый. — 2016. — № 8. — С. 725–728.
2. Голубев В. А. Кибертерроризм. Угроза национальной безопасности [Электронный ресурс] // URL: www.crive-research.ru (дата обращения: 10.09.2019).
3. Морозова А. П. Кибертерроризм и информационный терроризм как новые формы проявления терроризма // Научные труды северо-западного института управления Ранхигс, 2017. — Том 8. — № 2 (29). — С. 154–163.
4. Мохаддам Ф. Терроризм с точки зрения террористов. Что они переживают и думают и почему обращаются к насилию. — М.: Форум, 2011. — 288 с.
5. Мунтер А. Правление сдерживания и авангарда в военных преступлениях (терроризм) // Журнал факультета Исламского университета, 2018. — Том 13. — № 48. С. 615–651.
6. Нуждин Л. Информационный терроризм. — М.: Икар, 2014. — 276 с.
7. Степанов О. А. Развитие информационно-электронных средств как объект правового анализа в условиях нарастания угрозы кибертерроризма // Государство и право. — 2008. — № 8. — С. 82–85
8. Ткаченко, В. В. Российский терроризм. Проблемы уголовной ответственности / В. В. Ткаченко, С. В. Ткаченко. — Москва: Наука, 2015. — 110 с.
9. Томчак Е. В. Из истории компьютерного терроризма // Новая и новейшая история. — 2007. — N1. — С. 134–148
10. Чуфаровский, Ю. В. Терроризм. Особенности международного противодействия / Ю. В. Чуфаровский. — М.: Центр стратегической конъюнктуры, 2014. — 156 с.
11. Шатен, Пьер-Лоран Предотвращение отмывания денег и финансирования терроризма. Практическое руководство для банковских специалистов / Пьер-Лоран Шатен и др. — М.: Альпина Паблишер, 2015. — 316 с.
12. Поисковый юридический сайт // URL: www.findlaw.com (дата обращения: 19.06.2019)
13. Справочная правовая система «КонсультантПлюс» [Электронный ресурс] / URL: http://www.consultant.ru/search/?q=%D0%B4%D0%BE%D0%B3%D0%BE%D0%B2%D0%BE%D1%80 (дата обращения: 10.09.2019)
14. Уголовный Кодекс Республики Ирак. [Электронный ресурс]: https://yandex.ru/turbo?text=https%3A%2F%2Fwiselawyer.ru%2Fpoleznoe%2F75556-ugolovnyj-kodeks-respubliki-irak-kharakteristika-obshhej-chasti (дата обращения: 10.09.2019]
15. Anti-Terrorism_Law. [Электронный ресурс]: http://www.vertic.org/media/National%20Legislation/Iraq/IQ_Anti-Terrorism_Law.pdf. Русский перевод закона сделан авторами настоящей статьи (дата обращения: 10.09.2019)
16. Military Arms.ru [Электронный ресурс]: https://militaryarms.ru/armii-mira/islamskoe-gosudarstvo/ (дата обращения: 10.09.2019)

Журнал «Современная наука: актуальные проблемы теории и практики»