УДК 343.9.67

КИБЕРТЕРРОРИЗМ КАК ОДНА ИЗ ФОРМ ПРОЯВЛЕНИЯ СОВРЕМЕННОГО ТЕРРОРИЗМА

Ю.Е. Паламарчук

магистрант направления подготовки 40.04.01 Юриспруденция,

ЧОУ ВО ЮУ (ИУБиП), e-mail: palamarchuk.elena76@mail.ru

Научный руководитель: Фоменко А.И., к.ю.н., доцент.

Аннотация: Статья посвящена рассмотрению вопросов, регламентирующих привлечение виновного лица, осуществляющего деятельность террористического характера с использованием информационных технологий к уголовной ответственности. Также будет проведен анализ несовершенства уголовного законодательства по данному вопросу и предложены пути для их решения

Ключевые слова: кибертерроризм, терроризм, проблема, информационная безопасность, киберпреступность, кибератака.

CYBERTERRORISM AS A FORM OF MODERN TERRORISM

Y. E. Palamarchuk

Abstract: The article is devoted to the consideration of issues regulating the criminal prosecution of a guilty person who carries out activities of a terrorist nature using information technologies. It will also analyze the imperfections of criminal legislation on this issue and suggest ways to solve them.

Keywords: cyberterrorism, terrorism, problem, information security, cybercrime, cyber-attack.

На рубеже современности, самым суровым и глобальным видом преступлений во всем мире является кибертерроризм. И не все такие преступления становятся достоянием общественности в силу различных обстоятельств и причин их совершения. Только за 2019 год было зафиксировано более двадцати тысяч кибератак, что на 20% больше, чем было совершено в 2018 году. В пятерку наиболее актуальных отраслей, где совершались кибератаки вошли: государственные учреждения, медицинские, промышленность, образовательные и военные[9].

Для того, чтобы научиться противостоять кибертерроризму необходимо разработать ряд как профилактических мероприятий, так и мероприятий, который будут направлены на пресечение и противодействие кибертерроризму.

Для начала необходимо разобраться в чем отличие понятий «кибертерроризм» и «киберпреступность» их сходства и отличия.

Под кибертерроризмом понимают совокупность противоправных действий в киберпространстве, с использованием компьютерных и (или) телекоммуникационных технологий (в основном в информационно-телекоммуникационной сети «Интернет») в террористических целях, совершение которых, создает угрозу безопасности личности, общества и государства [5, С. 191-194].

А под киберпреступностью понимается преступления, совершенные с применением и использованием информационных технологий для достижения преступных целей. Следовательно, можно сделать вывод о том, что киберпреступность и кибертерроризм соотносятся как целое и частное.

Как правило преступления в сфере информационных технологий совершаются в международном масштабе. Обычно жертва и мошенник являются гражданами разных государств и не задумываются о существовании друг друга. Поэтому, для того чтобы оказывать эффективное противодействие таких преступлениям необходим опыт сотрудничества между государствами на международной арене.

Именно для этого Совет Европы в ноябре 2001 года принял конвенцию о преступности в сфере компьютерной информации, которая классифицирует преступления, совершенные на просторах киберпространства на такие категории [4]:

1. незаконный доступ в базы данных;
2. распространение вирусов, вредоносных программ, взлом паролей и личной конфиденциальной информации;
3. кража номеров кредитных карточек, банковских реквизитов и другой важной информации.

По действующему Уголовному законодательству Российской Федерации под преступлениями в сфере компьютерной информации понимают совершаемые в сфере информационных технологий и посягающие

на информационную безопасность общественно-опасные деяния, предметом посягательства которых является компьютерная информация [7, С. 546-551].

Федеральный закон «О противодействии терроризму» определяет «терроризм» как идеологию насилия и практику воздействия на органы государственной власти и местного самоуправления, которые направлены на достижение преступников определенной преступной цели [2]. Таким образом, можно говорить о том, что кибертерроризм является современной формой проявления терроризма в классическом виде, т.к. оба этих явления направлены на совершение противоправных действий в целях побудить различные структуры выполнить их распоряжение.

Обратим внимание на способ совершения преступлений террористического характера. Самым распространенным способом совершения таких преступлений является информационно-телекоммуникационная сеть «Интернет». Что же привлекает потенциальных террористов в мировой паутине? А.А. Фоменко выделяет ряд таких причин[8, С. 64–66]:

1. отсутствие цензуры со стороны государства;
2. доступность;
3. множество пользователей по всему миру;
4. сложная идентификация личности;
5. быстрота распространения нужной информации.

Для того, чтобы эффективно противодействовать как преступлениям с использованием высоких технологий, так и терроризму необходимо:

1. Необходимо создать эффективный механизм как правого, так и технического воздействия на потенциальных «киберпреступников», который бы контролировал распространение и незаконное получение конфиденциальной информации. Для этого необходимо иметь хорошо разработанную систему идентификации пользователей информационно-телекоммуникационной сети «Интернет». Который бы заключался не только в идентификации пользователей по IP-адресу, но и по ряду других значимых

критериев. Чтобы каждый пользователь такой информационной системы знал, что в случае совершения им противоправного действия он будет и идентифицирован. На данный момент в Российской Федерации не существует законодательного определения таких важных понятий как «кибертерроризм» и «киберпреступления». Законодательное закрепление таких понятий, поможет ускорить процесс привлечения к уголовной ответственности таких лиц.

2. Необходимо производить подготовку квалифицированных специалистов, которые бы с легкостью пресекали такие виды преступлений. Таким специалистом не должен быть работник правоохранительных служб, который имеет базовое высшее юридическое образование. В подготовку таких специалистов должны входить технические (информационные) дисциплины, которые бы позволили бы ему не только понимать законодательную составляющую совершенных преступлений, но и в совершенстве знать и уметь работать с компьютерными программами, чтобы понимать будущую схему действий потенциального преступника. Именно подготовка таких кадров упростит задачи правоохранительных органов и снизит уровень распространения такого вида преступления как «кибертерроризм».

Одной из главных проблем, с которой на сегодняшний день сталкивается действующее уголовное законодательство, это отсутствие конкретного состава преступления за совершение терактов с использованием информационно-телекоммуникационной сети «Интернет».

Наказуемыми считаются лишь деяния, совершенные с использованием СМИ, в форме публичных призывов к осуществлению террористической деятельности или публичного оправдания терроризма (ч. 2 ст. 205.2 УК РФ) [1]. При этом используется обобщённый термин «средства массовой информации», к числу которых в соответствии с Законом РФ «О средствах массовой информации» относится и сетевое издание, т. е. сайт в Интернете, зарегистрированный в качестве СМИ в соответствии с законом [3].

Однако создание сайта, содержащего информацию террористического характера, незаконно, поэтому регистрироваться указанный информационный ресурс в качестве средства массовой информации априори не может, а, следовательно, и рассматриваться в качестве СМИ он не должен. Получается, что отсутствие упоминания Интернета в ст. 205.2 Уголовного кодекса РФ влечет неоднозначные подходы в юридической практике при квалификации данного преступного посягательства [6, С. 510-515].

Исходя из вышесказанного можно сделать вывод о том, что действующее Российского уголовное законодательство нуждается в актуальных на сегодняшний день изменениях, направленных на предостережение в будущем от совершения таких преступлений как «кибертерроризм».

Следовательно, если такие изменения в ближайшее время будут приняты, то ситуация со статистикой совершаемых преступлений в данной сфере стабилизируется в лучшую сторону.

Библиографический список

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от. 27.10.2020 года) [Электронный ресурс] // КонсультантПлюс. – Режим доступа: http://www.consultant.ru (Дата обращения 14.12.2020).
2. Федеральный закон «О противодействии терроризму» от 06.03.2006 года № 35-ФЗ (ред. от. 08.12.2020 года) [Электронный ресурс] // КонсультантПлюс. – Режим доступа: http://www.consultant.ru (Дата обращения 14.12.2020).
3. Закон Российской Федерации «О средствах массовой информации» от 27.12.1991 года №2124-1 (ред. от. 01.03.2020 года) [Электронный ресурс] // КонсультантПлюс. – Режим доступа: http://www.consultant.ru (Дата обращения 14.12.2020).
4. Конвенция о преступности в сфере компьютерной информации от 23.11.2001 года [Электронный ресурс] // КонсультантПлюс. – Режим доступа: http://www.consultant.ru (Дата обращения 14.12.2020).
5. Авчаров И.В. Борьба с киберпреступностью / И.В. Авчаров. // Информатизация и информационная безопасность правоохранительных органов. XI межд. конф. - М., 2019. – С. 191-194.
6. Кунделеев С.В., Коханова В.С. Криминологические аспекты совершенствования системы противодействия преступности в сети Интернет // Интеллектуальные ресурсы – региональному развитию. – 2020. – №2. – С. 510-515.
7. Семиёхин В.А. Проблемы использования уголовного права России в условиях развития цифровой экономики // Интеллектуальные ресурсы – региональному развитию. – 2020. – №2. – С. 546-551.

8. Фоменко А.И. Преступления в области современных технологий: кибертерроризм как глобальная угроза современного общества // Рос. акад. журнал – 2014. — № 4. — Т. 30. — С. 64–66.
9. Статистика совершения кибератак в Российской Федерации за 2019 год // URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2019/#id3.