Понятие и место кибертерроризма в уголовном праве России
Диденко А. И.

Диденко Александр Игоревич / Didenko Aleksandr Igorevich – студент магистратуры,
Юридическая школа
Дальневосточный федеральный университет, г. Владивосток

Аннотация: *в статье рассмотрены основные подходы к определению кибертерроризма в литературе и законодательстве. Определены пути дальнейшего совершенствования уголовно-правовых способов борьбы с кибертерроризмом.*
Abstract: *the article considers the main approaches to the definition of cyber-terrorism in literature and law. The ways of further improving the criminal legal methods of combating cyber-terrorism.*

Ключевые слова: *кибертерроризм, Уголовный кодекс, компьютеры, информация.*
Keywords: *cyber-terrorism, criminal code, computers, information.*

В последнее время в СМИ вновь заговорили о проблеме кибертерроризма [16]. Данная проблема была также отмечена на проходившей в конце мая 2016 в городе Грозном VII международной встрече высоких представителей, курирующих вопросы безопасности. Так, участник указанного форума, спецпредставитель президента РФ по вопросам международного сотрудничества в области информационной безопасности, посол МИД РФ по особым поручениям Андрей Крутских отметил, что кибертерроризм — одно из наиболее страшных явлений, при этом оно совсем новое. Например, «Исламское государство» (запрещенное в России) уже влезло в информационное пространство и занимается кибертерроризмом. Плюс колоссальный ущерб планете наносит киберпреступность. Ежегодные объемы ущерба, согласно разным подсчетам, составляют от $500 млрд до $2–3 трлн [17].

Безусловно, проблема кибертерроризма носит комплексный характер, но, на наш взгляд, в авангарде борьбы с кибертерроризмом должно быть уголовное право. Поэтому необходимо подойти к этой проблеме с точки зрения уголовного законодательства.

Как не трудно заметить, термин «кибертерроризм» употребляется довольно часто как в СМИ, так и в юридической литературе, но каждый автор вкладывает в него что-то свое. Ситуацию усугубляет и тот факт, что это понятие нормативно не закреплено ни в Уголовном кодексе [1], ни в Федеральном законе от 06.03.2006 № 35-ФЗ (ред. 31.12.2014) «О противодействии терроризму» (далее - закон о противодействии терроризму) [2], ни в постановлении Пленума Верховного Суда РФ от 09.02.2012 № 1 «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности» (далее - постановление о преступлениях террористической направленности) [5], ни в постановлении Пленума ВС РФ от 09.02.2012 № 1 «О некоторых вопросах судебной практики по уголовным делам и о преступлениях компьютерной направленности» [6], ни в методических рекомендациях по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации (утв. Генпрокуратурой России) [7]. При этом нельзя сказать, что Российское государство не замечает такого явления как кибертерроризм. Так согласно п. 45, пп. «г» «Концепции противодействия терроризму в Российской Федерации» (утв. Президентом РФ 05.10.2009) (далее - концепция) кадровое обеспечение противодействия терроризму осуществляется по следующим основным направлениям: подготовка специалистов в специфических областях противодействия терроризму (противодействие идеологии терроризма, ядерному, химическому, биологическому терроризму, кибертерроризму и другим его видам) [4]. Таким образом, из анализа указанной нормы можно сделать вывод, что под кибертерроризмом в концепции понимается разновидность терроризма. Термин «терроризм» закреплен в ст. 3 закона о терроризме. Таким образом, исходя из системного толкования, кибертерроризм можно определить как разновидность идеологии насилия и практики воздействия на принятие решения органами государственной власти, органами местного самоуправления или международными организациями, связанные с устрашением населения и (или) иными формами противоправных насильственных действий в киберпространстве. Данные идеи не нашли своей более детальной реализации ни в Уголовном кодексе, ни в законе о противодействии терроризму, что на наш взгляд является упущением законодателя. На наш взгляд необходимо ввести термин «кибертерроризм» в закон о противодействии терроризму. При этом требуется добавить в гл. 24 УК РФ новый состав преступления, устанавливающий уголовную ответственность за «кибертерроризм», определив наказание за совершение указанного преступления свыше 10 лет лишения свободы. При этом полагаем возможным внести изменения в ст. 151 УПК РФ и отнести кибертерроризм к подследственности органов ФСБ РФ. Еще одной проблемой, на наш взгляд, является то, что нормативно не определены формы проявления такого явления как кибертерроризм. Разумно было бы издать соответствующее постановление Пленума Верховного Суда, этот шаг позволил бы излишне не

перегружать УК РФ и закон о противодействии терроризму.

В связи с тем, что легального определения кибертерроризма в Российском законодательстве нет, логично обратиться к науке. Различные авторы определяют кибертерроризм по разному. Так Усилинский Ф. А. определяет кибертерроризм как действия, выражающиеся в преднамеренной, политически мотивированной атаке на информацию, обрабатываемую компьютером и компьютерными системами, создающие 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 [8, с. 8]. Аналогичные определения дают и другие авторы: Паненков А. А. [9, с. 19], Ефремова М. А. [10, с. 11], и даже некоторые иностранные авторы, например, Деннинг Д. [11] считает, что под кибертерроризмом необходимо понимать как противоправную атаку или угрозу атаки на компьютеры, сети или информацию, находящуюся в них, совершенную с целью принудить органы власти к содействию в достижении политических или социальных целей. Таким образом, большинство авторов сводят кибертерроризм к разновидности терроризма, особенность которой заключается в том, что террористическая деятельность происходит в киберпространстве. На наш взгляд кибертерроризм следует определить как воздействие на компьютеры, компьютерные программы, компьютерные сети или обрабатываемую ими информацию в киберпространстве для целей осуществления или подготовки террористического акта. Понятие террористического акта содержится в ч. 3 ст. 3 Федеральный закон от 06.03.2006 N 35-ФЗ (ред. от 06.07.2016) «О противодействии терроризму». Сложнее предстоит дело с термином киберпространства. В связи с тем, что в российском законодательстве легального термина «киберпространства» нет, то на наш взгляд, необходимо воспользоваться международным опытом и имплементировать в российское законодательство определение киберпространства данное международным союзом электросвязи. В своем методическом пособии международный союз электросвязи определяет кибертерроризм как физическое и не физическое пространство, созданное и (или) сформированное следующим образом: компьютеры, компьютерные системы, сети, их компьютерные программы, компьютерные данные, данные контента, движение данных, и пользователи [12]. Данное определение как и термин киберпространство, на наш взгляд, также возможно закрепить в законе о противодействии терроризму.

Помимо ставшей традиционной формулы определения кибертерроризма через сочетание понятий терроризма и киберпространства, в литературе существуют иные подходы. Так Тропина Т. Л. предлагает выделить два вида кибертерроризма:

1) совершение с помощью компьютеров и компьютерных сетей террористических действий;

2) использование киберпространства в целях террористических групп, но не для непосредственного совершения терактов [14, с. 178].

Определенный интерес для изучения вызывает второй вид кибертерроризма. Так Тропина Т. Л., отмечает: вопрос отнесения к кибертерроризму использования киберпространства террористическими группами для осуществления и популяризации своей деятельности, но не для непосредственного совершения терактов, является спорным. Конечно, данные действия вряд ли можно квалифицировать по ст. 205 УК РФ в качестве терроризма, но если руководствоваться здравым смыслом, то причисление данных действий к кибертерроризму выглядит разумным. Мы уже оговорились, что терроризмом «в чистом виде», т. е. в том виде, в котором определяет его российский УК, данные действия не являются, хотя, на наш взгляд, вопрос их квалификации именно как террористических будет поднят в недалеком будущем [14, с. 179].

Как показывают происходящие в мире процессы, мнение Тропиной Т. Л. о необходимости борьбы с кибертерроризмом второго вида сегодня становятся актуальны как никогда, в связи с деятельностью террористических организаций, и начинают находить свое воплощение в деятельности законодателя. Так, Федеральный закон от 06.07.2016 N 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» в п. «б» ч. 15 ст. 1 изменяет диспозицию ч. 2 ст. 205.2 УК РФ, устанавливая уголовную ответственность за публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма, совершенные с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет» [3]. На наш взгляд, это позитивный момент для ответа на угрозы терроризма, который начинает использовать современные средства коммуникации для достижения своих целей.

Подтверждая вышесказанную позицию, хотелось бы привести слова директора ФСБ Бортникова А. В., который отметил, что международные террористические структуры научились эффективно управлять звеньями своих сетей дистанционно, в том числе с помощью интернета. «Они (террористические организации) активно используют программы зашифровки и мгновенного обмена сообщениями, в том числе популярные мессенджеры «Телеграм», Whatsapp, «Вайбер», с помощью которых рассылают своим сторонникам подробные инструкции по тематике ведения диверсионно-террористических действий, указывают конкретные цели для проведения терактов, а также предоставляют сведения о формах и

методах работы спецслужб», - заявил директор ФСБ [15].

В литературе есть различные мнения по поводу форм проявления кибертерроризма [13]. В связи с тем, что выше было предложено сформулировать их в постановлении о преступлениях террористической направленности, на наш взгляд, логично было бы ограничиваться типичным примерами, такими как:

- хищение или уничтожение информационного, программного и технического ресурсов, имеющих общественную значимость, путем преодоления систем защиты, внедрения вирусов, программных закладок и т.п.;

- воздействие на программное обеспечение и информацию в целях их искажения или модификации в информационных системах и системах управления;

- уничтожение или активное подавление линий связи, неправильная адресация, искусственная перегрузка узлов коммутаций;

- и др.

Важно, чтобы перечень оставался открытым, чтобы появления нового способа воздействия на компьютеры, компьютерные программы, компьютерные сети или обрабатываемую ими информацию в киберпространстве оставались наказуемы.

В итоге будем надеяться, что в недалеком будущем будут приняты соответствующие нормы, которые позволят эффективнее бороться с кибертерроризмом с помощью уголовного права.

Литература

1. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 06.07.2016). [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс»/ (дата обращения 10.08.2016).
2. Федеральный закон от 06.03.2006 № 35-ФЗ (ред. 31.12.2014) «О противодействии терроризму». [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс»/ (дата обращения 10.08.2016).
3. Федеральный закон от 06.07.2016 N 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности». [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс»/ (дата обращения 10.08.2016).
4. Концепция противодействия терроризму в Российской Федерации. (утв. Президентом РФ 05.10.2009). [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс»/ (дата обращения 10.08.2016).
5. Постановление Пленума Верховного Суда РФ от 09.02.2012 № 1 «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности». [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс»/ (дата обращения 10.08.2016).
6. Постановление Пленума ВС РФ от 09.02.2012 № 1 «О некоторых вопросах судебной практики по уголовным делам и о преступлениях компьютерной направленности». [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс»/ (дата обращения 10.08.2016).
7. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации (утв. Генпрокуратурой России). [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс»/ (дата обращения 10.08.2016).
8. *Усилинский Ф. А.* Кибертерроризм в России: его свойства и особенности. Право и кибербезопасность, 2014. № 1. С. 6-11.
9. *Паненков А. А.* Кибертерроризм как реальная угроза национальной безопасности России. Право и кибербезопасность, 2014. № 1. С. 12-19.
10. *Ефремова М. А.* Уголовно-правовое обеспечение кибербезопасности*:* некоторые проблемы и пути их решения. Информационное право, 2013. № 5. С.10-13.
11. *Denning D. E.* Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influen-cing Foreign Policy". [Электронный ресурс]. Режим доступа: http://www.nautilus.org/ info-policy/ workshop/ papers/ denning.html/ (дата обращения 07.08.2016).
12. ITU Toolkit For Cybercrime Legislation. ITU, 2011 [Электронный ресурс]. Режим доступа: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITU_Guide_A5_12072011.pdf./ (дата обращения 15.08.2016.).
13. *Сухаренко А.* Интернет на службе террористов. ЭЖ-Юрист. Из информационного банка «Юридическая пресса», 2012. № 46. С. 9-12.
14. *Тропина Т. Л. Киберпреступность* и кибертерроризм: поговорим о понятийном аппарате. Сборник научных трудов международной конференции «Информационные технологии и безопасность». Выпуск 3. Киев: Национальная академия наук Украины, 2003. С. 173-181.

15. Речь директора ФСБ Александра Бортникова 27.07.2016 на открытии 15-го совещания руководителей спецслужб, органов безопасности и правоохранительных органов. [Электронный ресурс]. Режим доступа: http://www.interfax.ru/russia/520709/ (дата обращения 17.08.2016).
16. Новостные сообщения. [Электронный ресурс]. Режим доступа: http://ria.ru/society/20160603/1442531794.html/ (дата обращения 10.08.2016).
17. Новостные сообщения. [Электронный ресурс]. Режим доступа: http://ria.ru/world/20160527/1439834739.html (дата обращения 10.08.2016).
18. Интервью с Андреем Крутским. [Электронный ресурс]. Режим доступа: http://www.kommersant.ru/Doc/2997208/ (дата обращения 11.08.2016).