СОВРЕМЕННЫЕ ТЕНДЕНЦИИ В ПРОТИВОДЕЙСТВИИ КИБЕРТЕРРОРИЗМУ

В.Е. Проваткина, *студент*
Т.В. Квасникова, *канд. юрид. наук, доцент*
Дальневосточный федеральный университет
(Россия, г. Владивосток)

DOI:10.24412/2500-1000-2023-7-2-226-230

Аннотация. *В данной статье раскрываются пути противодействия кибертерроризму, который сегодня полномасштабно развернулся в глобальном информационном пространстве сети интернет. Решение данной проблемы находится в интересах всего мирового сообщества, на местном же уровне организовать противодействие компьютерному терроризму в частности и компьютерным преступлениям в целом возможно при условии наличия в штате сотрудников высококвалифицированных специалистов в сфере IT, которые бы работали посредством специализированных защищенных каналов связи, оказывая поддержку в профилактике, предотвращении, расследовании и раскрытии киберпреступлений, а также в сборе доказательств причастности лиц к совершению конкретного компьютерного преступления.*

Ключевые слова: *кибертерроризм, киберпреступность, кибератака, вербовка, глобальная сеть.*

Терроризм – глобальная проблема, а значит говорить о противодействии данному явлению можно, лишь организовав международное сотрудничество, объединив усилия всех государств. Современные террористы не брезгуют ничем и в осуществлении своей преступной деятельности используют современные материально-технические средства и новейшие технологии. Высокая техническая оснащённость (использование современных подслушивающих устройств; поддельных документов высокого качества; использование автомобилей зарубежных производителей с высокими техническими характеристиками; использование огнестрельного оружия, электрошокеров и др. и служебной формы сотрудников правоохранительных органов и т.п.) свидетельствует о появлении новых форм терроризма. Наиболее популярной в последнее десятилетие является компьютерный терроризм (кибертерроризм). Связано это с тем, что совершенствование информационных технологий открывает для человечества не только новые возможности развития, но и способствует появлению новых глобальных угроз. Информационное пространство, в котором сейчас хранятся все данные мирового сообщества, становится очень уязвимым, а, следовательно, привлекает внимание преступного сообщества [1, 5].

Кибертеррористы совершают атаки на сайты государственных органов, вмешаются в работу систем странообразующих предприятий, взламывают базы данных, тем самым достигая главной цели терроризма – дезорганизация государственного устройства, нанесение значительного ущерба всем сферам жизни общества и полная дестабилизация ситуации в стране.

В соответствии с данными, представленными МВД России о состоянии преступности, число преступлений, свершенных с использованием информационных технологий, взросло на 68,5%. Кибертерроризм по масштабам, техническим возможностям и распространенности можно соотносить с организованной преступностью и традиционными формами терроризма, что свидетельствует о его повышенной опасности и актуальности изучаемой темы.

Одной из основных проблем противодействия киберпреступлениям, в том числе и кибертерроризму, является серьезное отставание законодательной базы от информационных технологий. Суть в том, что далеко не все компьютерные преступления

охватывают нормативные акты как международного, так и национального уровня.

В международном праве вопросы противодействия кибертерроризму имеют иной контекст, нежели в национальном законодательстве, включая в себя создание согласованного документа, который отражает формы взаимодействия государств в целях решения глобальной проблемы кибертерроризма. Однако основная проблема международного сообщества заключается в том, что международные акты и договоры заключаются и ратифицируются, охватывая не все государства, а лишь отдельные, исходя из этого, можно судить, что полного, всестороннего и грамотного сотрудничества в рамках противодействия кибертерроризму, добиться не удастся.

Возвращаясь к статистике, представленной МВД России, стоит отметить сложность установления доказательства причастности лиц к совершению компьютерных преступлений, в частности кибертеррористических атак [2, 4].

Одна из проблем состоит в том, что киберпространство гарантирует для преступников некую анонимность, при совершении тех или иных противоправных действий, а также обеспечивают мобильность террористам. Ярким примером является следующий прецедент: за последние годы резко увеличилось количество кибератак, которые были направлены, в том числе, и протии органов государственной власти и воинских частей Франции, причем хакеры-террористы действовали из Алжира и Туниса, то есть даже с другого континента. Исходя из этого, можно сделать вывод – использование информационных технологий при совершении противоправных действий позволяет преступнику скрываться где угодно, на территории любого региона, государства и континента, где есть доступ к глобальной сети. Для сотрудников органов внутренних дел это означает, что установить месторасположение преступника весьма затруднительно, ведь даже получение IP-адресов не позволит с точностью определить координаты. По сути, определить причастность того или иного лица к совершению кибертеррористического акта возможно только постфактум. То есть, предупредить совершение кибератаки оперативникам удастся только в том случае, если имеет место серия атак, совершенных одной группой лиц, лишь выяснив обстоятельства свершения одного или нескольких терактов из серии, можно не допустить совершение последующих.

Террористический акт в большинстве случаев организует группа лиц, которые взаимодействуют между собой по тем или иным каналам связи. Так вот если мы будем говорить о кибертерроризме, то установить и проследить каналы связи его организаторов еще более проблематично в силу того, что защитные контуры многих систем просто не позволяют осуществить вмешательство в них. Следовательно, установить причастность и доказать мотивы лица в организации кибертеррористического акта вызывает серьезные проблемы [5, 6, 8].

Исходя из вышесказанного, в силу стремительной глобализации общества и все более стремительного развития форм терроризма, оперативные службы и все мировое сообщество сталкивается с глобальной угрозой компьютерного терроризма. Кибертерроризм облегчает процесс вербовки людей, привлечения их к участию в террористических группировках, при этом скрывая самого организатора под маской «анонимности в Сети». Кибертеррористы организуют и проводят атаки, находясь в другой точке земного шара. Данные аспекты значительно усложняют работу оперативных сотрудников. Решение глобальной проблемы кибертерроризма находится в интересах всего мирового сообщества, на местном же уровне, организовать противодействие компьютерному терроризму в частности и компьютерным преступлениям в целом возможно при условии наличия в штате сотрудников высококвалифицированных специалистов в сфере IT, которые бы работали посредством специализированных защищенных каналов связи, оказывая поддержку в профилактике, предотвращении, расследовании и раскрытии киберпреступлений, а также в сборе доказательств причастности лиц к совершению конкретного компьютерного преступления [3, 6, 8].

Также следует заострить внимание на том, что в последние годы участились случаи использования возможностей сети интернет в качестве базы для подготовки экстремистов и террористов. Интернет изобилует огромным количеством информационных ресурсов, практических руководств в виде интерактивных учебных пособий, аудио- и видеоконтентов, методических материалов, инструкций на нескольких языках по вопросам вступления в террористические организации, изготовления взрывных устройств, приобретения огнестрельного оружия, планирования и совершения реальных террористических актов и хищения секретных материалов. Кроме того, встречается информационный обмен специальными знаниями, методами и приемами совершения указанных преступлений.

Современные Кибертеррористы планируют свои преступления путем дистанционного обмена сообщениями между несколькими сторонами. Определяется потенциальная цель нападения и разрабатываются наиболее эффективные средства достижения цели. Медиасети и блогерские платформы по неосмотрительности выкладывают конфиденциальную информацию, содержащую, событие, персонажей и место происшествия, которая мгновенно незаконно присваивается террористическими организациями. На этапе планирования атак террористы имеют возможность воспроизвести географические координаты местности, определить входы и выходы, отключить системы оповещения, что позволяет очень точно организовать выполнение задачи [6, 7].

Проблема уголовной ответственности за совершение террористического акта с использованием компьютерных технологий и сети Интернет не находит отражения в действующем российском законодательстве. 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). При этом используется обобщенный термин «средства массовой информации», к числу которых в соответствии с Законом РФ «О средствах массовой информации» [16] относится и сетевое издание, т.е. сайт в Интернете, зарегистрированный в качестве СМИ в соответствии с законом. 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

Современные ученые И.Г. Чекунов, Е.С. Саломатина предлагают дополнить ч. 2 ст. 205 пунктом, который устанавливал бы ответственность за террористический акт с несанкционированным доступом в сети Интернет, с целью нарушения функционирования производств и предприятий и создания аварийной ситуации и угрозы техногенной катастрофы.

Статьи 272-274 Уголовного кодекса, посвященные вопросам ответственности за преступления в сфере компьютерной информации, в настоящее время не содержат каких-либо упоминаний о террористической деятельности. Так, несмотря на то, что кибертерроризм может проявляться в виде кибератак посредством использования вредоносных программ, ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ» этого положения не учитывает. Для устранения данного пробела в праве представляется необходимым либо добавить в ст. 205 УК РФ квалифицированный состав (о чем говорилось ранее), либо внести в ч. 3 ст. 273 УК РФ в качестве особо квалифицирующего признака ответственность за создание и использование вредоносных компьютерных программ в террористических целях.

В качестве примера зарубежного опыта можно рассмотреть Уголовный кодекс Франции. Он устанавливает расширенную классификацию преступлений террористического характера. Причем процесс криминализации в этой сфере не считается

оконченным, что вызывает некоторые дискуссии в кругах современных ученых [9]. В то же время использование сети Интернет террористическими организациями рассматривается только в аспекте распространения запрещенной информации в цифровом пространстве (например, статья 421-2-5-2 Уголовного кодекса Франции, устанавливающая уголовную ответственность за распространение в сети Интернет сообщений, изображений, иных информационных действий, включающих показ преднамеренных нападений на жизнь, когда такое распространение сопровождается демонстрацией приверженности к такой террористической идеологии). Есть также общее уточнение, что признание преступления актом терроризма может происходить и в отношении действий, совершенных «в области информатики». Для этого необходимо соблюдение двух условий:

1) выполнение объективной стороны преступления, предусмотренного специальной Книгой III (преступления в сфере компьютерной информации);

2) совершение преступления в террористических целях.

Во Франции противодействие террористическим кибератакам рассматривается как особый вид повседневной деятельности спецслужб и правоохранительных органов, где обращение к уголовной ответственности выступает относительно редкой мерой. Такая тенденция оценивается как перевод всех мер борьбы с терроризмом из уголовного права в сторону административного. Это прослеживается и во многих законодательных инициативах, в которых превалирует предоставление органам государственной власти различных дополнительных административных полномочий (как, например, в Законе от 3 июня 2016 года № 2016-731 «Об усилении борьбы с организованной преступностью, терроризмом и их финансированием, а также о повышении эффективности и гарантий уголовного судопроизводства»). В 2021 году был подготовлен специальный Отчет о совершенствовании уголовного законодательства для предотвращения кибератак, но и в нем отсутствуют рекомендации о дополнении Уголовного кодекса Франции таким составом, как «Кибертерроризм» [10].

Таким образом, исследовав современную кибертеррористическую ситуацию, разворачивавшуюся в сети интернет, можно сделать вывод о готовящейся кибервойне. Однако, отсутствие единого понимания кибертерроризма детерминирует определенные сложности в разграничении понятий «кибертерроризм», «киберпреступность», «кибервойна». А учитывая схожую объективную сторону данных деяний доводится сталкиваться с путаницей понятий, и только при детальном изучении становится понятным, что основным критерием разграничения выступает цель совершения посягательства. Приходится констатировать, что главной проблемой для эффективного международного сотрудничества против кибертерроризма выступает пробел в законодательствах стран, включая Россию. Решение данной задачи лежит в плоскости разграничения вышеуказанных понятий, принимая во внимание специфику каждого из них, которая и станет платформой противодействия данному явлению. Вместе с тем объединив усилия в международном сотрудничестве в части нормативно-правового регулирования кибертерроризма повысятся шансы на его уничтожение [1, 4, 7]. И еще одним направлением, в котором необходимо вести борьбу выступают подкуп и вербовка сотрудников правоохранительных органов. Это позволит противодействовать выстраиванию террористическими сообществами собственной системы защиты, выражающейся в «срабатывании датчиков угроз» (например, информировании членов организованной группы завербованными сотрудниками правоохранительных органов в случае возникновения опасности для членов группы, выражающейся в задержании некоторых членов, осуществлении оперативно-розыскных мероприятий и др.).

Библиографический список

1. Абазов И.С. О путях противодействия кибертеррористическим угрозам // Журнал прикладных исследований. – 2022. – Т. 2. – № 6. – С. 178-181.
2. Кобец П.Н. Кибертерроризм – как важнейшая угроза национальной безопасности // Национальная безопасность и стратегическое планирование. – 2022. – № 1 (37). – С. 23-28.
3. Кумышева М.К. Противодействие кибертерроризму в цифровую эпоху // Евразийский юридический журнал. – 2022. – № 3 (166). – С. 417-418.
4. Ляхнов М.В. Кибертерроризм как наиболее опасная форма терроризма // Закон. Право. Государство. – 2022. – № 1 (33). – С. 283-286.
5. Малаев А.Х. Об актуальных проблемах противодействия кибертеррористическим угрозам в условиях цифровой трансформации // Пробелы в российском законодательстве. – 2022. – Т. 15. – № 4. – С. 214-218.
6. Овчинский В.С. Криминология цифрового мира: учебник для магистратуры. – М.: Норма: ИНФРА-М, 2018. – 352 с.
7. Сосновская Ю.Н., Маркина Э.В. Современный кибертерроризм как угроза национальной безопасности // Вестник Московского университета МВД России. – 2022. – № 2. – С. 206-210.
8. Теуважуков А.Х., Хитиева А.Ж. Совершение кибертеррористических преступлений в сети интернет: пути выявления и противодействия // Журнал прикладных исследований. – 2022. – Т. 1. – № 9. – С. 72-75.
9. Massé M. La criminalité terroriste / M. Massé // Revue de science criminelle et de droit pénal compare. 2012. – Vol. 1, № 1. – P. 89-107.
10. Мусаелян М.Ф. Террористический акт: уголовно-правовой аспект: автореф. дис. … канд. юрид. наук: 12.00.08. – Москва, 2007. – 28 с.

NEW TRENDS IN COUNTERING CYBERTERRORISM

V.E. Provatkina, *Student*
T.V. Kvasnikova, *Candidate of Legal Sciences, Associate Professor*
Far Eastern Federal University
(Russia, Vladivostok)

Abstract. *This article reveals ways to counteract cyberterrorism, which is now fully deployed in the global information space of the Internet. The solution to this problem is in the interests of the entire world community, at the local level, it is possible to organize counteraction to computer terrorism in particular and computer crimes in general, provided that there are highly qualified IT specialists in the staff who would work through specialized secure communication channels, providing support in the prevention, prevention, investigation and disclosure of cybercrimes, as well as in the collection of evidence of the involvement of persons in the commission of a specific computer crime.*

Keywords: *cyberterrorism, cybercrime, cyberattack, recruitment, global network.*