УДК 343.13.5

Кильмаматова Э.Р.
студентка 2 курса,
ФГБОУ ВО Башкирский
государственный университет
Россия, г. Уфа
Научный руководитель: Шагеева Р.М.,к.ю.н., доцент
кафедры уголовного права и процесса
ФГБОУ ВО Башкирский
государственный университет

АКТУАЛЬНЫЕ ПРОБЛЕМЫ РАССМОТРЕНИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ КИБЕРТЕРРОРИЗМА

Аннотация: *В данной статье освящается нарастающая угроза кибертерроризма в России, а также проблемы, связанные с рассмотрением и расследованием данной категории дел, в частности, вопросы, связанные со сбором доказательственной базы в виртуальном пространстве.*

Ключевые слова: *кибертерроризм, электронное доказательство, терроризм, уголовный процесс, расследование уголовных дел.*

Annotation: *In this article, the growing threat of cyberterrorism in Russia, as well as the problems associated with the examination and investigation of this category of cases, in particular, issues related to the collection of evidence base in the virtual space.*

Keywords: *cyberterrorism, electronic evidence, terrorism, criminal process, investigation of criminal cases.*

Для современного мира преступления в компьютерной сфере становятся все более актуальными. Развитие информационных и компьютерных технологий, внедрение их во все сферы жизни общества, принесли социуму как ряд преимуществ, так и множество недостатков.

На данный момент всемирная сеть Интернет нашла широкое распространение в сфере частного использования, а также в государственных целях, включая промышленные, оборонные и иные стратегически важные для каждого государства области.

Неудивительно, что преступники не прошли мимо прогресса и стали активно использовать новейшие достижения для противоправной деятельности. Современные IT-технологии открыли для них столь большие возможности, что преступления в компьютерной сфере стали проблемой государственной важности.

Если в конце 20 века в России выявленных преступлений в сфере компьютерных технологий было 10-12 в год, то с 2005 года их число достигло 15000[1], а к концу 2017 года этот показатель превысил 80000[2], и продолжает расти.

Мировое сообщество, в том числе и наша страна, не могут не реагировать на это. Масштабы проблемы требуют совместной борьбы всеми странами, а также принятия адекватных мер, включающих внесение изменений в уголовное и уголовно-процессуальное законодательство, в целях предотвращения данных преступлений, а также для их эффективного расследования и рассмотрения.

С начала 2000 –х годов идет активная работа по совершенствованию законодательства в отношении преступлений в сфере IT-технологий.

Так, в 2001 году в г. Будапеште была принята Конвенция Совета Европы по киберпреступлениям (далее – Конвенция), которая является многосторонним, юридически обязательным договором, касающимся преступной деятельности в сфере информационных технологий.

Конвенция предусматривает единообразие материального уголовного законодательства по борьбе с киберпреступностью и уголовно-

[1] Securelist: сайт. URL: https://securelist.ru/kiberprestupnost-v-tsifrah/6625/ (дата обращения 25.04.2018).
[2] Безнал.Про: сайт. URL: http://www.beznal.pro/news/14185-CHislo-kiberprestuplenijj-v.html (дата обращения 25.04.2018).

процессуального законодательства, содействие взаимной правовой помощи, кодификацию международного права, обеспечение правовой базы для содействия развитию и пониманию вопросов, связанных с киберпреступностью[3]. На сегодняшнее время данная Конвенция является основополагающим документом в области борьбы с преступлениями в компьютерной сфере.

Современная киберпреступность имеет огромное множество форм и способов осуществления, в числе которых: причинение ущерба отдельным физическим элементам информационного пространства (разрушение сетей электропитания, наведение помех, использование химических средств для разрушения элементной базы и др.), кража или уничтожение информационных, программных и технических ресурсов, имеющих особую социальную значимость, с помощью вирусов, программных закладок, влияние на программное обеспечение и информацию с целью их изменения, раскрытие и опубликование закрытой информации, включая информацию, составляющую государственную и коммерческую тайну, захват каналов средств массовой информации с целью распространить дезинформацию и свои террористические требования, уничтожение или подавление линий связи, искусственную перегрузку узлов коммутации, содействие проведению информационно-психологических операций, распространение ложной информации об угрозе кибертерроризма, воздействие на операторов, разработчиков информационных и телекоммуникационных сетей и систем путем насилия или угрозы насилия, шантаж, подкуп, использование нейролингвистического программирования, гипноза, средств создания иллюзий, мультимедийных средств для ввода информации в подсознание или ухудшения здоровья человека и др.[4]

[3] Convention on Cybercrime. Конвенция Совета Европы о предупреждении терроризма. Ратифицирована Федеральным законом РФ от 20 апреля 2006 года № 56-ФЗ// Собрание законодательства РФ, № 17 (ч.I), 24.04.2006, ст.1785
[4] Мазуров В.А. Кибертерроризм: понятие, проблемы противодействия // Доклады ТУСУР. 2010. №1-1 (21). С.41-45

Как можно заметить, преступления в компьютерной сфере достаточно разнообразны, при этом, постоянно обновляются и совершенствуются.

В связи с этим законодатель не всегда успевает вовремя изменить закон под быстро меняющиеся способы и формы совершения киберпреступлений, суды неоднозначно квалифицируют такие деяния, а в деятельности сотрудников правоохранительных органов возникают существенные трудности при их выявлении и раскрытии.

Наибольшие сложности возникают при сборе доказательной базы, так как следы информационных преступлений, как правило, существуют в виде цифровой информации, на электронных носителях.

В соответствии с Уголовно-процессуальным кодексом Российской Федерации (далее - УПК РФ) каждый вид доказательства имеет свой процессуальный порядок закрепления. При этом использование цифровых данных также требует придание им процессуальной формы.

Действующий уголовно-процессуальный закон определяет понятие электронного носителя информации, который согласно п.5 ч. 2 ст. 185 УПК РФ является одним из видов вещественных доказательств.[5] Вместе с тем, зачастую, при установлении обстоятельств уголовного дела интерес представляет не сам носитель, а находящаяся на нем информация. К сожалению, данный аспект вопроса на законодательном уровне в должной мере не урегулирован.

За последние несколько лет законодателем были внесены изменения, которые способствуют реальному применению электронных доказательств в уголовном процессе. Так, в 2012 году Федеральный закон «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации РФ» № 143 от 28 июля 2012 года внес серьезные поправки, закрепившие термин «электронный носитель информации», определивший порядок изъятия такой

[5] Уголовно-процессуальный кодекс РФ от 18 декабря 2001 года №174-ФЗ (с изм. от 19 февраля 2018.) //Российская газета, № 249, 22.12. 2001, ст. 2861

информации и способы ее фиксации[6]. Изменения, которые были внесены данным законом, содействовали дальнейшему развитию электронных доказательств и их применению в уголовно-процессуальном законодательстве.

На сегодняшний момент, чтобы электронная информация стала доказательством по уголовному делу ей необходимо обрести свойство допустимости, а для достижения данной цели цифровые (электронные) сведения должны быть получены: 1) надлежащим субъектом доказывания; 2) надлежащим способом собирания доказательств; 3) из надлежащего источника доказательств[7].

Собирание таких электронных доказательств наряду с другими способами доказательств осуществляется путем проведения следственных и иных процессуальных действий. Наибольший интерес представляют обыск, выемка и осмотр. Обнаружение в данном случае возможно путем выявления носителей компьютерной информации: личный компьютер, телефон, флеш-карта, съемный жесткий диск и другие.

Вместе с тем существуют трудности с обнаружением информации, хранящейся на материальном носителе, находящемся на значительном удалении от места производства предварительного расследования или судебного разбирательства, либо в случае иных препятствий к изъятию. Например, интернет-сайта или базы данных организации. В случае с сайтом, который фактически может существовать за пределами Российской Федерации, изъять и приобщить к материалам дела носитель данной информации довольно проблематично. Базы данных организаций зачастую достаточно объемны и защищены от несанкционированного доступа. Поэтому при работе с такими доказательствами, как правило, ограничиваются только их осмотром.

[6] Федеральный закон от 28 июля 2012 г. № 35-ФЗ «О внесении изменений в уголовно-процессуальный кодекс Российской Федерации»// Собрание законодательства РФ,№ 31, 30.07.2012, ст. 4332

[7] LIVEJOURNAL: сайт. URL: https://popcrim.livejournal.com/29778.html (дата обращения 25.04.2018).

Так, одним из доказательств вины в совершении преступления, предусмотренного ч. 3 ст. 138 УК РФ, по делу, рассмотренному мировым судьей судебного участка 9 по Кировскому району г. Уфы Республики Башкортостан, стал протокол осмотра интернет-сайта «N» от 7 мая 2010 г. Согласно данному протоколу гражданин А. в присутствии понятых и условного покупателя посетил интернет-ресурс «N». В ходе посещения установлено, что на главной странице сайта имеется вкладка «Оформить заказ». При входе в данную вкладку появляются данные об отсутствии каких-либо заказов. При выборе в «Каталоге товаров» позиции «Шпионские устройства» отображаются текстовая информация об устройстве «GSM аудиопередатчик (шпион)», фотография устройства, его цена. Данный заказ был направлен в «корзину». В процессе осмотра условный покупатель оформил на вышеуказанном сайте заказ на приобретение «GSM аудиопередатчик (шпион)».[8]

Компьютерная экспертиза при установлении обстоятельств, подлежащих доказыванию по рассматриваемой категории дел, имеет огромное процессуальное значение.

В компетенцию эксперта входит консультирование о наличии тех или иных документов на электронном носителе, дате их создания, изменении и удалении, ведении переписки, отправлении и принятии различных сообщений, аудио-, фотодокументов и видеозаписей.

На наш взгляд, целесообразно проведение компьютерной экспертизы компетентным специалистом, а осмотр сайта должен осуществляться уполномоченным на то следователем, дознавателем с участием специалиста и понятых, ход и результаты следственного действия должны быть отображены и зафиксированы в соответствующем протоколе и др.

К электронным доказательствам должны предъявляться весьма жесткие требования, поскольку данный вид доказательств не овеществлен, т.е. его

[8]Бикмиев Р. Г., Бурганов Р. С. Собирание электронных доказательств в уголовном судопроизводстве //Информационное право. 2015. № 3. С. 17–21

невозможно изучить в общем порядке, и для их оценки нужны специальные устройства, а зачастую и лица, обладающие специальными знаниями в компьютерной сфере.

Кроме того, электронные доказательства легко могут быть подвергнуты изменениям и уничтожению. В связи с чем особенную важность приобретают своевременная и правильная фиксация полученных данных.

В заключении следует отметить, что статистика совершенных киберпреступленний неуклонно растет, все чаще в данной деятельности используется и компьютерная информация, соответственно, использование электронных доказательств в уголовном судопроизводстве является перспективным направлением раскрытия и расследования уголовных дел, в частности, именно для данной категории преступлений.

При изучении данной темы мы обнаружили, что законодатель зачастую не совсем оперативно реагирует на быстроменяющиеся способы и формы совершения кибберпреступлений, что отрицательно сказывается на расследовании и рассмотрении таких дел.

Последние изменения в части электронных доказательств были внесены в УПК РФ почти шесть лет назад и не соответствуют современным информационным реалиям.

Библиографический список

1. Securelist: сайт. URL: https://securelist.ru/kiberprestupnost-v-tsifrah/6625/ (дата обращения 25.04.2018).

2. Безнал.Про: сайт. URL: http://www.beznal.pro/news/14185-CHislo-kiberprestuplenijj-v.html (дата обращения 25.04.2018).

3. Convention on Cybercrime. Конвенция Совета Европы о предупреждении терроризма. Ратифицирована Федеральным законом РФ от 20 апреля 2006 года № 56-ФЗ// Собрание законодательства РФ, № 17 (ч.I), 24.04.2006, ст.1785.

4. Мазуров В.А. Кибертерроризм: понятие, проблемы противодействия // Доклады ТУСУР. 2010. №1-1 (21). С.41-45.
5. Уголовно-процессуальный кодекс РФ от 18 декабря 2001 года №174-ФЗ (с изм. от 19 февраля 2018.) //Российская газета, № 249, 22.12. 2001, ст. 2861.
6. Федеральный закон от 28 июля 2012 г. № 35-ФЗ «О внесении изменений в уголовно-процессуальный кодекс Российской Федерации»// Собрание законодательства РФ, № 31, 30.07.2012, ст. 4332.
7. LIVEJOURNAL: сайт. URL: https://popcrim.livejournal.com/29778.html (дата обращения 25.04.2018).
8. Бикмиев Р. Г., Бурганов Р. С. Собирание электронных доказательств в уголовном судопроизводстве //Информационное право. 2015, № 3. С. 17−21.