Секция «LegalTech. Цифровая криминалистика»

К вопросу о применении цифровых следов в криминалистике

Научный руководитель – Помогалова Юлия Викторовна

Прилепский Владислав Максимович
Студент (бакалавр)
Воронежский институт Федеральной службы исполнения наказания, Воронежская область, Россия
E-mail: prilepsky@list.ru

В настоящее время происходит информатизация всех сторон жизни общества. Развитие информационных технологий привело к увеличению числа киберпреступлений.

Понятийный аппарат законодателя, связанный с противодействием киберпреступлениям, довольно скуден, в соответствующих статьях Уголовного кодекса Российской федерации[1] от 13 июня 1996 г. № 63-ФЗ (далее - УК РФ) представлены отдельные составы, однако они не раскрывают сущность данного понятия. Изучение феномена «киберпреступность» привело к возникновению понятия «электронно-цифровой след». В научных источниках оно определяется как любая криминалистически значимая компьютерная информация, находящаяся в электронно-цифровом формате. Некоторые авторы признают необходимость выделения самостоятельной группы следов, определяя их как результат отражения на цифровом материальном носителе реального (физического) процесса или действия иной компьютерной системы, в виде цифрового образа формальной модели этого процесса.[4] В криминалистической науке уже около 20 лет объединяются преступления, совершаемые с использованием компьютерных средств и систем, к тому же применяется понятие «компьютерные преступления», которое употребляется не в уголовно-правовом аспекте, где это только затрудняет квалификацию деяния, а в криминалистическом, поскольку связано не с квалификацией, а со способом совершения преступления и, соответственно, с методикой его раскрытия и расследования.

Цифровые следы возможно определенным образом классифицировать. Содержательные следы создаются лицом сознательно, обладают криминалистически значимой информацией (текст электронного сообщения). Сопутствующие следы формируются без участия лица, при этом являясь метаданными (данные геолокации, сведения об устройстве, время отправки сообщения). Для того, чтобы использовать цифровые следы в качестве доказательства, необходимо проведение ряда судебных экспертиз. Основной целью данных действий будет являться доведение до субъектов уголовного судопроизводства, не обладающих специальными знаниями в сфере компьютерных технологий, тех или иных технических процессов, протекающих при использовании компьютерных технологий в преступных целях. В данном процессе главенствующую роль будет играть профессионализм и компетентность эксперта, участвующего в проведении судебной экспертизы. Кроме того, законодателю стоит обратить внимание на отсутствие правового регулирования, а также методических рекомендаций по исследованию цифровых следов. [3]

Стоит обратить внимание на то, что в Уголовно-процессуальном кодексе Российской Федерации[2] от 18 декабря 2001 г. № 174-ФЗ отсутствует перечень следственных действий, которые предоставят возможность удаленного получения компьютерной информации из компьютерных систем и сетей. Данная проблема формируется из-за использования шифрования преступниками в процессе совершения киберпреступления. Злоумышленники часто пытаются скрыть значимую для следствия информацию путем конспирации, а также шифрования, для чего используют специализированный программный софт, например TrueCrypt. Для получения доступа к зашифрованной информации необходимо ввести и

пароль либо использовать криптографический ключ, которыми следствие в большинстве случаев не располагает.

Иным способом извлечения информации является удаленное подключение к компьютеру в процессе его работы, что может быть реализовано только в рамках проведения оперативно-розыскных мероприятий по поручению следователя. Информация, полученная таким образом, может быть весьма полезна для следствия, однако вряд ли может быть признана доказательством, поскольку порядок ее процессуального оформления уголовно-процессуальным законодательством не регламентирован.[5]

Подобная экспертиза должна быть подкреплена созданием электронного учета, в котором могли бы содержаться ключи шифрования, данные о программно-техническом обеспечении, использовавшемся в процессе совершения того или иного преступления, а также иная информация, имеющая важное криминалистическое значение. Формирование подобного учета может кардинальным образом облегчить процесс сбора и анализа статистических данных, а также предоставит новые возможности для идентификации, поскольку программно-технические средства, создаваемые преступником самостоятельно, являются плодом высокоинтеллектуальной деятельности и практически также уникальны, как отпечатки пальцев.[6]

Таким образом, правовое и техническое обеспечение обнаружения, извлечения (фиксации), исследования и оценки цифровых следов в настоящее время не имеет должного развития. Данная проблема создает ряд трудностей в ходе рассмотрения и расследования киберпреступлений. Законодателю стоит обратить внимание на проблемы, возникающие вследствие информатизации всех сфер общественной жизни.

Источники и литература

1) Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 64-ФЗ ФЗ (ред. от 27.12.2019) // СЗ РФ. 2019. № 25. Ст. 2954.

2) Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (ред. от 27.12.2019) // СЗ РФ. 2019. № 25. Ст. 4156.

3) Гайсин Н. И. К вопросу о придании доказательственного значения цифровым следам: https://elibrary.ru

4) Россинская Е. Р. Проблемы использования специальных знаний в судебном исследовании компьютерных преступлений в условиях цифровизации: https://elibrary.ru

5) Семикаленова А. И. Использование специальных знаний при обнаружении и фиксации цифровых следов: анализ современной практики: https://elibrary.ru

6) Смахтин Е. В. Трансформация электронно-цифровых следов в электронноцифровые доказательства: вопросы теории и практики: https://elibrary.ru