Перечисленные обстоятельства влияют на способы обеспечения безопасности. Например, команда «Заряжай!» в зависимости от вида оружия, выполняемого стрелкового упражнения подразумевает различное положение оружия и готовности для его применения, однако согласно национальным Правилам эта команда трактуется однозначно. Аналогично можно говорить и о команде «Разряжай!».

Обеспечение безопасности в указанных условиях устанавливается правилами международных федераций стрелковых видов спорта, что в отдельных случаях идет в противоречие, либо не отражено в национальных Правилах применения гражданского оружия при занятии спортом. Представляется, что Правила должны соответствовать современному этапу развития спорта, обеспечивать его безопасность, в то же время содержать установленный перечень действий, контроль выполнения которых вменен в обязанности руководителя занятия.

УДК 343.9

А.И. Чурносов

НЕКОТОРЫЕ АСПЕКТЫ КРИМИНАЛИСТИЧЕСКОГО ИССЛЕДОВАНИЯ ЦИФРОВЫХ СЛЕДОВ

В настоящее время вопрос классификации цифровых следов не менее значимый, чем определение самой их сущности. Значение решения данного вопроса заключается в том, что классификация позволит систематизировать имеющиеся знания и выявить особенности отдельных категорий цифровых следов, разработать методические рекомендации по работе с ними, а также определить типичные проблемы, которые могут возникнуть в ходе расследования преступлений, при которых образуются цифровые следы. В науке существует множество подходов к классификации цифровых следов, которые предложены учеными-криминалистами, а также формировались параллельно с исследованием теоретических основ и сущности цифровых следов. Так, вопрос классификации был изучен учеными-криминалистами, а именно В.А. Мещеряковым [1, с. 103], А.Г. Волеводз [2, с. 159–161], В.Е. Козловым [3, с. 91], А.Ю. Семеновым [4, с. 54], Л.Б. Красновой [5, с. 25–72], В.П. Леонтьевым [6, с. 264], А.Б. Смушкиным [7, с. 43–48], В.Б. Веховым [8, с. 44], Е.А. Гамбаровой [9] и др.

В.Б. Вехов полагает целесообразным использовать понятие «цифровой след». По его мнению, им является «любая криминалистически

значимая компьютерная информация, т. е. сведения (сообщения, данные), находящиеся в электронно-цифровой форме, зафиксированные на материальном носителе с помощью электромагнитных взаимодействий либо передающиеся по каналам связи посредством электромагнитных сигналов» [10, с. 156], что, на наш взгляд, наиболее точно отражает природу такого рода следов.

Говоря о специфике цифровых следов, возникающих при совершении преступлений в сфере информационных технологий, отметим, что они являются результатами не непосредственного взаимодействия с материальными объектами, а опосредованного отражения материальных объектов, процессов и результатов ввода, обработки, передачи информации. Часто преступления в рассматриваемой сфере носят латентный характер. Например, при расследовании преступлений могут отсутствовать видимые следы, а сам процесс раскрытия и собирания доказательственной информации может быть затруднен в связи с широким применением средств удаленного доступа, шифрования и парольной защиты. Для наглядности обратимся к примеру электронного документа как цифрового следа. В сфере уголовно-процессуальной деятельности электронный документ определяют как информацию, полученную с использованием информационных технологий и представленную документом в электронной форме, которая имеет значение при расследовании по уголовному делу. Сама среда существования электронного документа определяет технологические особенности таких документов, и данные особенности выражаются в следующем: 1) у электронных документов отсутствует жесткая привязка к материальному носителю (документ отделим от него); 2) чтобы электронный документ стал доступен для восприятия человеком, необходимо создать определенные условия (наличие технических и программных средств); 3) сложный процесс идентификации автора электронного документа (документ нельзя собственноручно подписать без соответствующего программного обеспечения); 4) электронный документ подвержен разного рода модификациям. Ввиду такой специфики при работе с информацией, представленной в электронном виде, необходимо придерживаться определенных правил: информация должна быть получена с соблюдением требований уголовно-процессуального закона; исходная информация должна фиксироваться на физических носителях таким образом, чтобы обеспечивалась ее целостность, надежное хранение и возможность проверки в последующем; цифровая аудиоинформация, видео-, фотоизображения должны сохраняться вместе с информацией относительно их создания; цифровая аудиоинформация, видео-, фотоизображения, сохраняемые в виде файла, должны быть сохранены

в оригинальных форматах файлов, обусловленных использованием конкретных технических средств; при хранении или обработке цифровой информации на компьютере (в том числе и на сетевой рабочей станции или выделенном сервере) необходимо разграничить доступ; различного рода исследованиям должны подвергаться не исходные оригиналы цифровой информации, а их копии; допущенные к обработке цифровой информации лица должны иметь опыт производства таких операций и четко представлять ее последствия, чтобы не нанести ущерб обрабатываемой информации; при обработке цифровой информации должно осуществляться протоколирование совершаемых операций [11]. Применение перечисленных правил на практике позволит увеличить эффективность использования информации, представленной в цифровом виде, в целях доказывания по уголовному делу. Однако данные решения не являются исчерпывающими. Анализ правоприменительной практики показывает, что существует множество проблем, которые настоятельно требуют своего разрешения. Так, в частности, это касается вопроса участия специалиста при проведении следственного осмотра.

Необходимо акцентировать внимание на том обстоятельстве, что цифровые следы должны обладать свойствами, обеспечивающими их законность. Так, они должны быть получены уполномоченным субъектом доказывания, надлежащим способом собирания доказательств и из достоверного источника доказательств.

Список использованных источников

1. Мещеряков, В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования / В.А. Мещеряков. – Воронеж : Изд-во Воронеж. гос. ун-та, 2002. – 407 с.

2. Волеводз, А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества / А.Г. Волеводз. – М. : Юрлитинформ, 2002. – 314 с.

3. Козлов, В.Е. Теория и практика борьбы с компьютерной преступностью / В.Е. Козлов. – М. : Горячая линия – Телеком, 2002. – 336 с.

4. Семенов, А.Ю. Некоторые аспекты выявления, изъятия и исследования следов, возникающих при совершении преступлений в сфере компьютерной информации / А.Ю. Семенов // Сиб. юрид. вестн. – 2004. – № 1. – С. 53–55.

5. Краснова, Л.Б. Компьютерные объекты в уголовном процессе и криминалистике : автореф. дис. ... канд. юрид. наук : 12.00.09 / Л.Б. Краснова ; Воронеж. гос. ун-т. – Воронеж, 2005. – 202 с.

6. Леонтьев, В.П. Большая энциклопедия компьютера и Интернета / В.П. Леонтьев. – Москва : Просвещение, 2006. – 1121 с.

7. Смушкин, А.Б. Виртуальные следы в криминалистике / А.Б. Смушкин // Законность. – 2012. – № 8 (934). – С. 43–48.

8. Вехов, В.Б. «Электронная криминалистика»: понятие и система / В.Б. Вехов // Криминалистика: актуальные вопросы теории и практики : материалы Междунар. науч.-практ. конф. – Ростов н/Д, 2017. – С. 40–46.

9. Гамбарова, Е.А. Проблемы и перспективы применения социальных медиа и мессенджеров в расследовании преступлений / Е.А. Гамбарова // Юрид. вестн. Самар. ун-та. – 2016. – Т. 2, № 1. – С. 145–150.

10. Вехов, В.Б. Понятие, виды и особенности фиксации электронных доказательств / В.Б. Вехов // Расследование преступлений: проблемы и пути их решения. – 2016. – № 1 (11). – С. 155–158.

11. Григорьев, А.Н. Использование в раскрытии и расследовании преступлений информации, представленной в цифровой форме / А.Н. Григорьев // Актуальные проблемы раскрытия и расследования преступлений по горячим следам: вопросы взаимодействия и применения современных технических средств : материалы Всерос. науч.-практ. конф. – Калининград : Калининград. ЮИ МВД России, 2004. – С. 69–75.