Этот метод позволяет впоследствии избежать неоднократного исследования одних и тех же участков и оставления без исследования других площадей. В связи с применением этого метода на заранее подготовленном плане, схеме, чертежах территория делится на участки (секторы, квадраты, сегменты). Впоследствии при разбивке участков их границы определяются друг от друга вешками, лентами, колышками, или естественными рубежами и ориентирами (например, края оврага, берега ручья или иного водоема и т. д.).

Длина участка намечается в пределах от 50 до 100 метров, чтобы при обследовании территории были видны действия участников обыска и просматривалось расположение объектов. Обыскивающие последовательно переходят с одного участка на другой после тщательного осмотра местности [2, с. 115].

На этом же этапе собирается и анализируется информация о местах вероятного сокрытия искомых объектов, сведений о конструкциях и наличии различных ограждений, охране, режиме пропуска, наличии отдельных строений.

Определяется состав участников следственной группы, в которую кроме следователя, специалистов, работников дознания, понятых, могут быть включены значительные силы в виде воинских формирований (ввиду большого участка местности), групп дружинников и т. д. В отдельных случаях их инструктируют до выезда к месту обыска, при этом им раздают фотографии с приметами искомых объектов, схемы и чертежи местности, в то же время им разъясняют, какие предметы они должны искать, как с ними обращаться в случае обнаружения. Если имеется информация, что на месте обыска могут находиться взрывные устройства, взрывчатые, легковоспламеняющиеся, ядовитые и другие опасные для жизни и здоровья вещества и материалы, то об этом сообщается при инструктаже участникам обыска, и затем на рабочем этапе в первую очередь проводятся действия по их обнаружению и обезвреживанию.

Подготавливаются различные научно-технические средства, которые могут быть использованы при исследовании большой территории: средства освещения, поисковые приборы (щупы, магнитоискатели, металлоискатели, аппаратура для отыскания взрывчатых, наркотических веществ, для регистрации гамма-излучения; дефектоскопы, фото-, видеоаппаратура, ультрафиолетовые осветители, инструменты для раскопок и вскрытия хранилищ, тралы, багры, буры, рентгеновская аппаратура, трупоискатели, видеоэндоскопы и т. д.) [3, с. 917].

Проблемы, освещенные в данной статье, подлежат обдумыванию и решению до начала производства обыска участков местности, даже в

тех случаях, когда на подготовку к обыску остается мало времени. Полагаем, учитывая особенности подготовительного этапа производства обыска участков местности, можно достичь эффективного, положительного результата.

1. Луценко, О.А. Обыск и выемка. Процессуальный порядок, тактика и доказательственное значение / О.А. Луценко. – Ростов н/Д : Феникс, 2005. – 63 с.

2. Бедняков, Л.И. Обыск: проблемы эффективности и доказательственного значения / И.Л. Бедняков. – М. : Юрлитинформ, 2010. – 176 с.

3. Корчагин, А.А. Особенности тактики проведения обыска по делам об убийствах / А.А. Корчагин // Фундамент. исслед. – 2013. – № 10-4. – С. 916–920.

4. Давыдов, В.И. Наиболее распространенные способы сокрытия ценностей, нажиты преступным путем : в кн. «Проблемы предварительного следствия» / В.И. Давыдов. – Волгоград, 1977. – Вып. 6. – С. 95–96.

5. Леви, А.А. Обыск. Справочник следователя / А.А. Леви, А.И. Михайлов. – М. : Юрид. лит.,1983. – С. 35–51.

6. Варданян, А.В. Тактико-психологические основы производства обыска : дис. … канд. юрид. наук : 12.00.09 / А.В. Варданян. – Волгоград, 2008. – 224 л.

7. Бедняков, И.Л. Обыск: проблемы эффективности и доказательственного значения : дис. ... канд. юрид. наук : 12.00.09 / И.Л. Бедняков. – Самара, 2009. – 228 л.

УДК 343.985

И.В. Пашута

НЕКОТОРЫЕ АСПЕКТЫ КЛАССИФИКАЦИИ ЦИФРОВЫХ СЛЕДОВ В КРИМИНАЛИСТИКЕ

Классификация как способ систематизации объектов и явлений объективной действительности служит одним из средств познания в любой науке, в том числе и криминалистике. Многообразие цифровых следов также требует их определенного упорядочивания, исходя из целей и задач быстрого и эффективного раскрытия и расследования преступлений, тем или иным образом связанных с компьютерной техникой и компьютерной информацией. Классификация цифровых следов в криминалистическом аспекте означает прежде всего их дифференциацию с точки зрения таких критериев, которые в максимальной степени отвечают практическим потребностям субъектов выявления (раскрытия), расследования и предупреждения преступлений.

Анализ специальной литературы свидетельствует о наличии различных подходов относительно классификации цифровых следов [1, с. 159–160; 2, с. 44; 3, с. 17; 4, с. 103; 5, с. 53–56; 6, с. 44–45].

Исходя из потребностей правоприменительной практики, наиболее прикладной (адаптивной к нуждам деятельности органов уголовного преследования) представляется классификация цифровых следов по следующим основаниям.

В зависимости от места нахождения выделяются цифровые следы, обнаруживаемые на так называемых оконченных и промежуточных электронно-цифровых устройствах. К оконченным устройствам относятся компьютерная система (отдельный компьютер (ноутбук, планшет, смартфон) или совокупность компьютеров, взаимосвязанных и взаимодействующих как единое целое) и машинный носитель (материальные носители, используемые для записи и хранения информации). На таких устройствах цифровые следы могут быть обнаружены, например, на жестком диске (винчестере – HDD), твердотельном накопителе (SSD), гибком полимерном магнитном диске (дискете), магнитной ленте (стримере), жестком оптическом или магнитооптическом диске (CD, DVD), микроконтроллере – программном управляемом микроэлектронном устройстве (SIM-карты, карты памяти (флеш-карты), USB-драйверы и др.), в оперативных запоминающих устройствах (ОЗУ) компьютерной системы, а также периферийных компонентов (принтере, сканере и др.). А.Б. Смушкин указывает на следующие цифровые следы, отображаемые в памяти компьютера: а) включение, выключение, различные операции с содержимым памяти компьютера (отображаются в журналах администрирования, безопасности, приложений и т. д.); б) действия с наиболее важными для работы компьютера программами (установка, удаление и т. д.), отражаемые в реестре компьютера (reg-файлах); в) сведения о работе в сети Интернет, локальных и иных сетях, содержащихся в log-файлах, истории журналов браузеров пользователя; г) операции с файлами (отражаются в их свойствах, например, время создания, последнего открытия, изменения файла и др.) [6, с. 44].

Промежуточными устройствами являются компоненты сетевого оборудования, необходимые для функционирования локальных сетей или глобальной компьютерной сети Интернет. К цифровым следам на промежуточных электронно-цифровых устройствах относятся следы, которые могут быть обнаружены в коммутаторе (сведения о подключаемых устройствах, содержащихся в таблице MAC-адресов), маршрутизаторе (роутере) и межсетевом экране (сведения о передаваемых пакетных данных в локальных сетях или сети Интернет).

По мнению В.Е. Козлова, цифровые следы в зависимости от размещения следует дифференцировать на локальные и внешние файловые следы [7, с. 152].

Устанавливая место нахождения цифровых следов, следует иметь в виду, что они могут «состоять из большого количества отдельных информационных элементов, которые могут быть записаны как на одном, так и на нескольких электронных носителях информации, подключены как к одному, так и к нескольким (возможно территориально расположенным на значительных расстояниях) компьютерам, объединенным в информационную систему или информационно-телекоммуникационную сеть [8, с. 269]. Так, например, если документ распечатывается непосредственно с USB-накопителя (съемного жесткого диска и т. п.), то искомые цифровые следы могут быть обнаружены в ОЗУ компьютера, ОЗУ периферийного устройства (принтера) и на самом накопителе.

По характеру происхождения цифровые следы могут быть оставленными лицом непосредственно (любые создаваемые файлы с какой-либо информацией: электронный договор, текстовый документ, сообщения в мессенджерах, записи в социальных сетях и др.) либо опосредованно (данные телеметрии, файлы регистрации, атрибуты создаваемых файлов). Следы первой группы могут быть исследованы в ходе производства следственных действий (например, в ходе осмотра компьютерной информации, компьютерной техники). Для исследования следов второй группы, как правило, требуется использование специальных знаний в форме компьютерно-технической и иных экспертиз [9].

В зависимости от формы представления цифровые следы могут быть в виде текста, графики (PNG-, JPEG-, GIF-изображения и многие др.) или мультимедиа (различное сочетание звука, анимированной компьютерной графики и видеоряда).

В зависимости от принадлежности оконченных (промежуточных) устройств цифровые следы подразделяются на физически находящиеся на компьютерных устройствах потерпевшего (например, функционирующее вредоносное программное обеспечение), подозреваемого или обвиняемого (например, исходный код вредоносного программного обеспечения, шаблоны для изготовления поддельных документов), иных лиц (например, электронная почта на сервере организации, предоставляющей подобные услуги). Следует отметить, что цифровые следы могут одновременно располагаться на устройствах, относящихся ко всем трем группам [9]. Такие следы могут быть обнаружены в таблице расширения файлов (FAT, NTFS или другой в зависимости от типа используемой операционной системы); системном реестре операционной системы; отдельных кластерах магнитного носителя (винчестера, дискеты), в которых записываются фрагменты исполняемых файлов (программ) и файлов конфигурации; файлах и каталогах (папках) хранения

входящей электронной почты и прикрепленных исполняемых файлах, конфигурации почтовой программы; файлах конфигурации программ удаленного соединения компьютера с информационной сетью [5].

По степени видимости цифровые следы бывают видимыми (электронные документы, записи в социальных сетях, электронной почты и др.), скрытыми (это составляющие файловой системы, которые не видны в фоновом (обычном) режиме) и зашифрованными (особый тип данных, кодируемых с помощью алгоритма из соображений конфиденциальности, для чего используются различные программы шифрования). Скрытые файлы создаются для того, чтобы ограничить доступ к определенной информации для других лиц, имеющих доступ к компьютерной системе. Зашифрованные файлы могут хранить важную информацию об интересуемом лице: его персональные данные, сведения о паролях к электронной почте, социальным сетям, мессенджерам и т. д.

Таким образом, представленная классификация направлена на систематизацию знаний о цифровых следах, создающих основу для более глубокого понимания сущности изменений, происходящих в результате совершения преступлений, связанных с компьютерной техникой и компьютерной информацией. Это в целом способствует более эффективной и тактически грамотной деятельности органов уголовного преследования по собиранию, исследованию, оценке и использованию в процессе доказывания таких следов.

1. Волеводз, А.Г. Противодействие компьютерным преступлениям : правовые основы международного сотрудничества / А.Г. Волеводз. – М. : Юрлитинформ, 2002. – 496 с.

2. 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.

3. 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. – 24 с.

4. 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.

5. 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. 53–56.

6. Смушкин, А.Б. Виртуальные следы в криминалистике / А.Б. Смушкин // Законность. – 2012. – № 8. – С. 43–45.

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

8. Мещеряков, В.А. Следы преступлений в сфере высоких технологий / В.А. Мещеряков // Б-ка криминалиста. – 2013. – № 5. – С. 265–270.

9. Бахтеев, Д.В. Криминалистические особенности производства процессуальных действий с цифровыми следами [Электронный ресурс] / Д.В. Бахтеев, Е.В. Смахтин // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

УДК 343.98

Н.Н. Пашута

О СООТНОШЕНИИ ПОНЯТИЙ «КРИМИНАЛИСТИЧЕСКАЯ ДЕЯТЕЛЬНОСТЬ» И «КРИМИНАЛИСТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ»

Борьба с преступностью – сложная, многогранная деятельность, обусловленная межотраслевым характером и, как следствие, многообразием приемов, методов и средств, обеспечивающих эффективное осуществление данного процесса. Вместе с тем указанная деятельность тогда является эффективной, когда она надлежащим образом организована.

Анализируя различные точки зрения относительно содержания организации раскрытия и расследования преступлений, следует отметить, что оно включает в себя ряд элементов: уголовно-процессуальную, оперативно-розыскную, судебно-экспертную и криминалистическую деятельность. Последний вид деятельности, по мнению А.Ф. Волынского и И.В. Тишутиной, осуществляется в форме криминалистического обеспечения раскрытия и расследования преступлений [1, с. 27].

Анализ научной литературы свидетельствует о том, что во многих случаях эти понятия смешивают, неверно трактуют. В этой связи представляется необходимым рассмотреть вопрос об их соотношении.

Впервые понятие «криминалистическая деятельность» было введено в научный оборот на рубеже 70-х гг. XX в. Р.Г. Домбровским, который, с одной стороны, различает ее как совокупность приемов и методов практического действования (практическое познание), а с другой – как совокупность методов научного познания (научная криминалистическая деятельность) [2, с. 10, 12].

Несколько позже В.Я. Колдин, рассматривая вопросы системно-деятельностного подхода в криминалистике, высказал мнение о том, что основным объектом криминалистического исследования является человеческая деятельность. С одной стороны, это поведение преступни-