УДК 343.98

М. М. Льянов

СОВРЕМЕННЫЙ ПОДХОД К КЛАССИФИКАЦИИ ВИРТУАЛЬНЫХ СЛЕДОВ[1]

В статье рассмотрен актуальный в настоящее время вопрос классификации виртуальных следов. Актуальность данной темы обусловлена активным развитием компьютерных технологий, появлением новых способов совершения преступлений с их помощью. В связи с этим формируются новые разновидности следов, что требует их постоянного изучения. Автором статьи были исследованы существующие подходы к классификации виртуальных следов. Сделан вывод о том, что в науке существует большое количество классификаций виртуальных следов, каждая из которых по-своему является правильной, так как развитие компьютерных технологий способствует появлению новых категорий для деления виртуальных следов. Автором статьи были предложены следующие критерии для деления виртуальных следов: в зависимости от электронного носителя информации, на котором находится виртуальный след, по месту нахождения виртуальных следов, в зависимости от обстоятельств, подлежащих доказыванию по уголовному делу, в зависимости от структуры и содержания информации в виртуальном следе. По мнению автора статьи, выделение классификаций по указанным основаниям поможет оптимизировать работу по их изучению и, как следствие, практическую деятельность по расследованию преступлений.

Ключевые слова: виртуальный след, классификация, компьютерные технологии, электронные носители информации, электронные сети, информационно-телекоммуникационная сеть «Интернет».

M. M. Lyanov

A MODERN APPROACH TO THE CLASSIFICATION OF VIRTUAL TRACES

The article is devoted to the currently topical issue of the classification of virtual traces. The relevance of this topic is connected with a fast development of computer technologies, and the development of new methods of committing crimes using them. This leads to the emergence of new types of traces, which should be constantly examined. The author analyzed the existing approaches to the classification of virtual traces and concluded that each of the numerous existing scientific classifications of virtual traces is correct in its own way because the development of computer technologies contributes to the emergence of new categories for classifying virtual traces. The author suggested using the following criteria for the classification of virtual

[1] Слова «виртуальный», «цифровой», «электронный» рассматриваются автором как синонимы.

traces: based on the electronic medium that contains the virtual trace; based on the place where those traces can be found; based on the circumstances subject to proof in a criminal case; based on the structure and contents of information in the virtual trace. According to the author, the classifications using these criteria will help optimize the work on their examination and, consequently, the practical work of crime investigation.

Keywords: virtual trace, classification, computer technologies, electronic information media, electronic networks, information and telecommunications network the Internet.

Одним из перспективных направлений исследований в криминалистике является изучение виртуальных следов, практики работы с ними, а также теоретические разработки в данной области. В настоящее время вопрос классификации виртуальных следов не менее спорный и значимый, чем вопрос определения самой сущности виртуальных следов. Значение решения данного вопроса заключается в том, что классификация позволит систематизировать имеющиеся знания и выявить особенности отдельных категорий виртуальных следов, разработать методические рекомендации по работе с ними, а также определить типичные проблемы, которые могут возникнуть в ходе расследования преступлений, при которых образуются виртуальные следы.

Работа в данной области криминалистики ведется уже достаточно давно. В науке существует множество подходов к классификации виртуальных следов, которые предложены учеными-криминалистами, а также формировались параллельно с исследованием теоретических основ и сущности виртуальных следов. Так, вопрос классификации был изучен учеными-криминалистами 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;] и др. [9].

Приведенными выше авторами предложены такие критерии классификации следов на электронных носителях информации как деление в зависимости от характера вносимых изменений, в зависимости от совершаемых с информацией операций и т.д. Стоит отметить, что при многообразии подходов к классификации виртуальных следов, есть и такие критерии для классификации, которые повторяются в работах разных авторов и являются наиболее распространенными основаниями для классификации. Такие критерии можно считать устоявшейся основой, содержание которой, тем не менее, имеет свои теоретические проблемы. Основанием (критерием) деления виртуальных следов можно считать электронный носитель информации, местонахождение виртуального следа, форму отображения следа.

Исходя из проведенного исследования, был сделан вывод, что многообразие подходов классификации виртуальных следов является вполне обоснованным, поскольку развитие компьютерных технологий требует выделения новых критериев для разделения виртуальных следов. Полагаем, что, помимо существующих в криминалистике критериев деления виртуальных следов, можно предложить дополнительные классификации виртуальных следов, в связи с

этим в настоящей статье будут представлены новые классификации и описана необходимость их выделения. Классификации по уже известным основаниям также необходимы, так как, на наш взгляд, они требуют дополнительного исследования, доработок, уточнения, а их изменение – обоснования [10].

Первым основанием для классификации виртуальных следов необходимо выделить вид электронного носителя информации, на котором находится виртуальный след. На наш взгляд, данный критерий является ключевым, поскольку, разбирая вопрос устройства электронных носителей информации и механизмов их работы, можно решить множество теоретических и практических вопросов, таких как сущность виртуальных следов, различия в необходимых процедурах при обнаружении и изъятии следов. На наш взгляд, классификацию можно представить следующим образом:

1. Магнитные носители информации.

а) встроенные в системный блок жесткие диски;

б) переносные жесткие диски.

2. Оптические носители информации.

а) диски, предназначенные только для чтения (CD-ROM, DVD-ROM);

б) диски, предназначенные для однократной записи (CD-R, DVD-R, и т.д.);

в) диски, которые предусматривают многократную запись информации (CD-RW, DVD-RW и т.д.).

3. Полупроводниковые носители информации.

а) устройства флеш-памяти;

б) SSD-диски.

4. Оперативные запоминающие устройства.

Выделение виртуальных следов по данному критерию позволяет сформировать общие рекомендации по работе со следами, так как особенности носителей информации влияют на процесс обнаружения и изъятия виртуальных следов, а также получение информации из этих следов.

Изучая механизм записи на магнитные носители информации, видно, что он предполагает образование виртуальных следов в результате электромагнитного воздействия на ферромагнитное покрытие. В процессе такого воздействия на ферромагнитном покрытии формируются устойчивые, положительно и отрицательно заряженные зоны, последовательность которых и несет в себе информацию. В связи с этим, данные на таком носители информации могут храниться продолжительный промежуток времени, однако при работе с этим видом электронных носителей информации необходимо избегать воздействия на него электромагнитного излучения, а также средств экстренного уничтожения информации.

Напротив, особенностью оперативных запоминающих устройств является свойство энергозависимости памяти, которое предполагает хранение информации до тех пор, пока подаётся непрерывный источник электроэнергии. При прекращении подачи энергии информация стирается. Зная данные особенности, можно создать рекомендации по работе с каждым электронным носителем информации. В связи с этим данный критерий классификации виртуальных сле-

дов представляет особую важность, как при рассмотрении теоретических проблем, так и при практическом применении различных методов работы с виртуальными следами.

Следующий критерий классификации виртуальных следов, который необходимо выделить, является их местонахождение, поскольку это определяет особенности проведения следственных действий, позволяет определить их сложность и возможные трудности. Классификацию по месту нахождения виртуальных следов можно представить следующим образом:

1) следы, содержащиеся на электронном устройстве лица, совершившего преступление;

2) следы, содержащиеся на электронном устройстве потерпевшего от преступления или иных лиц;

3) следы, содержащиеся на серверах электронных сетей.

Выделение в данной классификации следов, содержащихся на устройстве лица, совершившего преступление, обусловлено тем, что на практике могут возникать ситуации различной сложности, связанные с обнаружением и изъятием таких следов, с обеспечением их сохранности. При подготовке следственных действий необходимо проанализировать всю имеющуюся информацию о лице, свершившем преступление, его навыках и возможных способах противодействия доступу к следам. Так, при наличии у лица, совершившего преступления, высокого уровня навыков и знаний в области компьютерных технологий, велика вероятность использования им средств, предназначенных для экстренного уничтожения информации в случае несанкционированного доступа.

Следы, обнаруженные на устройстве потерпевшего от преступления или иных лиц, способствуют установлению фактов подлежащих доказыванию, такие как характер и размер вреда, причиненного преступлением, способ совершения преступления и т.д. Кроме того, найденные следы могут содержать информацию о лице, совершившем преступление, а также о его навыках в работе с компьютерными технологиями. Данные сведения также позволят спланировать дальнейшие следственные действия, в ходе которых будет проводиться работа с виртуальными следами.

Следы, содержащиеся на серверах электронных сетей, имеют определенную специфику. В связи с особенностями доступа к информации, содержащейся в информационно-телекоммуникационных сетях, на наш взгляд, обосновано выделить в отдельную группу следы, содержащиеся на серверах электронных сетей. Вопросы собирания доказательств в электронных сетях в настоящее время актуальны и являются предметом исследования в научных работах. Так, к примеру, особенности собирания информации из сети интернет рассмотрены в научной статье О.В. Овчинниковой [11, с. 67–70]. Так как количество преступлений, совершенных с использованием информационно-телекоммуникационных технологий составляет значительную часть от общей массы преступлений, данная категория следов приобретает ещё большее значение.

Из статистики, представленной на официальном сайте МВД РФ, следует, что из всех преступлений (2 024 337 преступлений), совершенных в 2019 году,

преступления, совершенные с использованием компьютерных и телекоммуникационных технологий, составляют 14,5% (294 409 преступлений)[1]. Учитывая, что удельный вес таких преступлений с каждым годом лишь увеличивается, исследования в этой области представляют особую важность. Таким образом, изучению данного вида виртуальных следов необходимо уделить особое внимание, сформировать на основе их изучения методические рекомендации, а выделение их в отдельную категорию в классификации является обоснованным.

В качестве классификации можно предложить деление виртуальных следов в зависимости от обстоятельств, подлежащих доказыванию по уголовному делу и предусмотренных ст. 73 УПК РФ. Так, к примеру, с помощью виртуальных следов можно установить обстоятельства, характеризующие личность лица, совершившего преступление, сведения, относящиеся к событию преступления, такие как время, способ совершения преступления и т.д.

Необходимость выделения виртуальных следов по данному критерию объясняется тем, что данные обстоятельства подлежат обязательному установлению, и знание путей получения этой информации при помощи виртуальных следов может облегчить эту задачу. В связи с этим выделение типов файлов, которые могут содержать информацию, подлежащую установлению, разработка способов их обнаружения, фиксации, изъятия и исследования может обеспечить повышение эффективности расследования преступлений.

Значительное влияние на процесс работы с виртуальными следами оказывает структура и содержание информации, которая в них представлена, взаимосвязь этих двух элементов. В контексте данной категории классификации под структурой понимается формат файла, в котором содержится информация, а под содержанием – сама информация, которая раскрывается в ходе проведения исследований электронных носителей информации, расследования преступления. В связи с этим обоснованным является выделение отдельной классификации по данному критерию, а также является необходимым выявление взаимосвязи этих двух элементов, что позволит определить пути применения полученной в ходе расследования преступлений информации. Среди этой категории следов можно выделить следы, в которых содержится:

1) информация о создании, изменении и удалении файлов;

2) информация об активности в информационно-телекоммуникационных сетях;

3) информация, содержащаяся в текстовых файлах;

4) информация, содержащаяся в видео-файлах;

5) информация, содержащаяся в аудио-файлах;

6) информация, содержащаяся в графических файлах.

Текстовые, графические, видео- и аудио-файлы позволяют установить обстоятельства, имеющие значение для уголовного дела. Так, например, из графических и видео-файлов можно установить внешность лица, совершившего

[1] Краткая характеристика состояния преступности в Российской Федерации за январь - декабрь 2019 года // МВД РФ. URL: https://мвд.рф/reports/item/19412450/.

преступление, получить информацию времени и месте совершения преступления.

Текстовые файлы могут содержать информацию о событии преступления, о личности лица, совершившего преступление, о потерпевших. Аудио-файлы позволяют получить фонограмму голоса, иные сведения, имеющие значение для расследования уголовного дела. Научные разработки в области исследования данных файлов является перспективным. В настоящее время существуют исследования, посвященные изучению особенностей использования данных файлов при расследовании преступлений. Вопросы использования аудио- и видео-файлов рассмотрены в научных статьях Г.В. Оленина [12, с. 23], А. Хаитжанова, А.С. Глазкова [13, с. 221–224] и др. К примеру, вопросы использования графических и текстовых файлов рассмотрены в научной статье А.Г. Себякина [14, с. 262–270]. Помимо информации, содержащейся в этих файлах, значение имеют сведения об их создании, удалении и изменении, поскольку это может свидетельствовать о попытках фальсификации или сокрытия информации.

С появлением всевозможных социальных сетей и мессенджеров исследование указанных выше файлов стало ещё более актуально, так как зачастую лица, готовящие, совершающие или совершившие преступления координируют свои действия, используя информационно-телекоммуникационную сеть «Интернет». Данная практика особенно распространена при совершении преступлений, связанных с незаконным оборотом наркотических средств с их дистанционной продажей, при которых места закладок сообщаются при помощи отправки текстовых, графических и аудио-файлов через мессенджеры. Для примера можно привести приговор Правобережного районного суда г. Магнитогорска Челябинской области по делу № 1-562/2019 от 27 ноября 2019 г.,[2] в котором указан протокол осмотра изъятого телефона. В ходе осмотра телефона в приложении централизованной службы мгновенного обмена сообщениями сети «Интернет» были обнаружены фотографии участков местности с указанием адреса и конкретного места закладок.

Помимо работы с файлами в сети интернет, актуальным вопросом является выявление активности в информационно-телекоммуникационной сети «Интернет». Данное направление исследования связано с существованием регистрирующих файлов (log-файлов), которые содержат в себе информацию о соединениях пользователей сети с отдельными ресурсами. Log-файлы были предметом изучения в работах А.Г. Волеводз [15, с. 4–12], А.Б. Смушкина. Так, например, А.Г. Волеводз, обращая внимание на важность log-файлов для хода расследования преступления, указывает, что они могут содержать большое количество информации, как о пользователе, так и об отправляемых сообщениях.

Предложенные в статье критерии для классификации виртуальных следов, на наш взгляд, представляют значение для уточнения имеющихся методик работы с виртуальными следами. Их детальное исследование позволит приме-

[2] Дело № 1-562/2019 : Приговор Правобережного районного суда г. Магнитогорска Челябинской области от 27 нояб. 2019 г. // Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/KGJE6rt5mT1x/.

нять оптимальные методики работы с виртуальными следами на практике, что позволит значительно повысить эффективность расследования преступлений, при совершении которых используются компьютерные технологии.

Список использованной литературы

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. – Москва : Юрлитинформ, 2002. – 314 с.
3. Козлов В.Е. Теория и практика борьбы с компьютерной преступностью / В.Е. Козлов. – Москва : 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 // Сибирский юридический вестник. – 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, 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-на-Дону, 2017. – С. 40–46.
9. Гамбарова Е.А. Проблемы и перспективы применения социальных медиа и мессенджеров в расследовании преступлений / Е.А. Гамбарова // Юридический вестник Самарского университета. – 2016. – Т. 2, № 1. – С. 145–150.
10. Введенская О.Ю. Особенности следообразования при совершении преступлений посредством сети Интернет / О.Ю. Введенская // Юридическая наука и правоохранительная практика. – 2015. – № 4 (34). – С. 209–216.
11. Овчинникова О.В. Собирание электронных доказательств, размещенных в сети Интернет / О.В. Овчинникова // Правопорядок: история, теория, практика. – 2016. – № 4 (11). – С. 67–70.
12. Оленин Г.В. Экспертиза цифровой аудио- и видеозаписи. Применение в следственной практике устройств цифровой фиксации аудио- и видеоинформации / Г.В. Оленин // Эксперт-криминалист. – 2009. – № 2. – С. 21–23.
13. Хаитжанов А. Аудиозапись (фонограмма) как доказательство в уголовном процессе / А. Хаитжанов, А.С. Глазков // Надежность и качество : труды Междунар. симпозиума : в 2 т. – Пенза, 2011. – Т. 1. – С. 221–224.
14. Себякин А.Г. Возможности использования контекстного поиска информации на компьютерных носителях в целях выявления, расследования и профилактики преступлений / А.Г. Себякин. – DOI 10.17150/2500-

4255.2019.13(2).262-270 // Всероссийский криминологический журнал. – 2019. – Т. 13, № 2. – С. 262–270.

15. Волеводз А.Г. Следы преступлений, совершенных в компьютерных сетях / А.Г. Волеводз // Российский следователь. – 2002. – № 1. – С. 4–12.

References

1. Meshcheryakov V.A. *Prestupleniya v sfere komp'yuternoi informatsii: osnovy teorii i praktiki rassledovaniya* [Crimes in the field of computer information: the basics of the theory and practice of investigation]. Voronezh State University, 2002. 407 p.

2. Volevodz A.G. *Protivodejstvie komp'juternym prestuplenijam: pravovye osnovy mezhdunarodnogo sotrudnichestva* [Counteraction to Computer Crimes: Legal Foundation of International Cooperation]. Moscow, Jurlitinform Publ., 2002. 314 p.

3. Kozlov V.E. *Teoriya i praktika bor'by s komp'yuternoi prestupnost'yu* [Theory and Practice of Cybercrimes' Fighting]. Moscow, Goryachaya Liniya – Telekom Publ., 2002. 336 p.

4. Semenov A.Yu. Some aspects of identification, removal and investigation of traces arising from the commission of crimes in the field of computer information. *Sibirskii yuridicheskii vestnik = Siberian Legal Bulletin*, 2004, no. 1, pp. 53–55. (In Russian).

5. Krasnova L. B. *Komp'yuternye ob'ekty v ugolovnom protsesse i kriminalistike. Avtoref. Kand. Diss.* [Computer objects in criminal procedure and criminalistics. Cand. Diss. Thesis]. Voronezh, 2005. 24 p.

6. Leontev V.P. *Bol'shaya entsiklopediya komp'yutera i Interneta* [Great Encyclopedia of Computer and Internet]. Moscow, Prosveshchenie Publ., 2006. 1121 p.

7. Smushkin A.B. Virtual Traces in Criminalistics. *Zakonnost' = Legality*, 2012, no. 8 (934), pp. 43–48. (In Russian).

8. Vekhov V.B. Electronic Criminalistics: Concept and System. *Kriminalistika: aktual'nye voprosy teorii i praktiki. Materialy mezhdunarodnoi nauchno-prakticheskoi konferentsii* [Criminalistics: Topical Issues of Theory and Practice. Materials of International Research Conference]. Rostov-on-Don, 2017, pp. 40–46. (In Russian).

9. Gambarova E.A. Problems and Prospects of the Use of Social Media and Messengers in the Investigation of Crimes. *Yuridicheskii vestnik Samarskogo universiteta = Juridical Journal of Samara University*, 2016, vol. 2, no. 1, pp. 145–150. (In Russian).

10. Wedenskaya O.Yu. Characteristics of Leaving Traces While Committing Internet Crimes. *Yuridicheskaya nauka i pravookhranitel'naya praktika = Legal Science and Law Enforcement Practice*, 2015, no. 4 (34), pp. 209–216. (In Russian).

11. Ovchinnikova O.V. Gathering of Electronic Evidence, Placed in the Internet. *Pravoporyadok: istoriya, teoriya, praktika = The Rule of Law: History, Theory, Practice*, 2016, no. 4 (11), pp. 67–70. (In Russian).

12. Olenin G.V. Expertise of digital audio and video recording. Application in investigative practice of devices for digital recording of audio and video information. *Ekspert-kriminalist = Expert-Criminalist*, 2009, no. 2, pp. 21–23. (In Russian).

13. Khaitzhanov A., Glazkov A.S. Audio recording (phonogram) as evidence in criminal proceedings. *Nadezhnost' i kachestvo. Trudy Mezhdunarodnogo simpoziuma* [Security and Quality. Proceedings of International Symposium]. Penza, 2011, vol. 1, pp. 221–224. (In Russian).

14. Sebyakin A.G. The Possibilities of Using Contextual Information Search on Computer Media to Identify, Investigate and Prevent Crimes. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2019, vol. 13, no. 2, pp. 262–270. DOI: 10.17150/2500-4255.2019.13(2).262-270. (In Russian).

15. Volevodz A.G. Traces of crimes committed in computer networks. *Rossiiskii sledovatel' = Russian Examining Magistrate*, 2002, no. 1, pp. 4–12. (In Russian).

Информация об авторе

Льянов Муса Микаилович – аспирант, кафедра уголовного права и процесса, Институт государства и права, Тюменский государственный университет; следователь-стажер, Следственное управление УМВД России по г. Тюмени, г. Тюмень, Российская Федерация, e-mail: musa-lyanov@mail.ru.

Information about the author

Lyanov, Musa M. – Ph.D. Student, Department of Criminal Law and Procedure, Institute of State and Law, Tyumen State University; Trainee Investigator, Investigative Department, Russian Ministry of Internal Affairs in the City of Tyumen, Tyumen, Russian Federation, e-mail: musa-lyanov@mail.ru.