УДК 343.98

КРИМИНАЛИСТИЧЕСКИЕ КЛАССИФИКАЦИИ ЦИФРОВОЙ ИНФОРМАЦИИ
Forensic Classification of Digital Information

Н. А. Иванов – доцент кафедры уголовного процесса и криминалистики Омской юридической академии, кандидат юридических наук

N. A. Ivanov – Associate Professor of the Criminal Procedure and Criminalistics Department of the Omsk Law Academy, Candidate of Law Sciences

Аннотация. *В работе предложено несколько классификационных схем цифровой информации, которая может быть использована в качестве источников доказательств в уголовном судопроизводстве. В прикладном плане предложенные классификации очень важны для разработки криминалистических средств, приемов, методов, методик обнаружения, фиксации, осмотра, изъятия, исследования цифровой информации, а также использования данной информации при выявлении и расследовании преступлений.*

Several classification schemes for digital information that could be used as sources of evidence in criminal proceedings are offered. In terms of application the proposed classification is very important for the development of forensic tools, means, methods, techniques for the detection, capture, inspection, seizure, investigation of digital information, as well as for the detection and investigation of crimes.

Ключевые слова: *уголовный процесс, расследование преступлений, криминалистическая классификация цифровой информации.*

Criminal procedure, investigation of crimes, criminalistics classification of digital information.

Криминалистика как наука и как отрасль практической деятельности способствует деятельности правоприменительных органов по установлению истины в судопроизводстве, отправлению правосудия и предупреждению преступлений. И при этом подавляющее число криминалистов вполне справедливо отмечало, что упорядочивание рекомендаций для целей эффективного выявления, раскрытия, расследования преступлений и судебного разбирательства уголовных дел производится в большинстве случаев через построение криминалистических классификаций, поскольку, помимо своего гносеологического значения как одного из средств познания, криминалистические классификации являются одним из средств повышения эффективности и результативности практической деятельности, разрабатываемых специально для борьбы с преступностью.

К проблеме криминалистической классификации компьютерной информации в своих работах неоднократно обращались многие ученые-криминалисты. Так, например, В. Б. Вехов предлагал с криминалистической точки зрения разделить компьютерную информацию на группы по следующим основаниям: 1) по юридическому положению – на недокументированную и документированную; 2) по категории доступности – на общедоступную компьютерную информацию общего пользования (с неограниченным доступом) и охраняемую законом компьютерную информацию, доступ к которой ограничивается в соответствии с законодательством Российской Федерации; 3) по форме представления – на электромагнитные сигналы как средство переноса компьютерной информации в пространстве и во времени с помощью электромагнитных ко-

лебаний (волн) и команды, файлы и программы для ЭВМ[1].

Н. А. Зигура, проанализировав ранее предложенные другими учеными классификации, предложила собственную, разделив компьютерную информацию на следующие классификационные группы: 1) по связи с событием преступления – в зависимости от того, являлась ли компьютерная информация орудием совершения преступления, объектом преступного посягательства, сохранила в себе следы совершения преступления или является иной информацией, которая устанавливает наличие или отсутствие обстоятельств, подлежащих доказыванию при производстве по уголовному делу, а также иных обстоятельств, имеющих значение для уголовного дела; 2) по источнику происхождения: в первую подгруппу она включила компьютерную информацию, созданную (внесенную) пользователем и которая является «результатом деятельности человека (записи делового или личного характера; данные, внесенные в различные программы для последующей обработки, например, создание баз данных)», а во вторую – компьютерную информацию, созданную аппаратными и программными средствами[2].

Крис Рид, один из ведущих американских ученых в области компьютерного права и использования компьютерной информации при расследовании различных видов противоправных действий, предложил разделить компьютерную информацию на шесть основных видов доказательств: исходные данные (raw data); базы данных (databases); коды, необходимые для расшифровки электронной информации (codes necessary to inteipret computer information); особенности алгоритма программирования или обработки данных; программное обеспечение коммерческого характера (commercial software); компьютерные системы (computer systems)[3].

Но компьютерная информация, как отмечалось ранее автором, является лишь частью общего объема цифровой информации[4]. Очевидно, что какие бы системы классификации цифровой информации ни были предложены, они всегда бывают довольно условными и, как это обычно бывает, не полностью отражают все характеристики данной группы источников сведений. В то же время полагаем, что предложенные классификационные системы в максимальной степени отражают те потребности предварительного расследования и судебного разбирательства уголовных дел, которые направлены на установление обстоятельств уголовного дела, подлежащих доказыванию, в соответствии со ст. 73 Уголовно-процессуального кодекса Российской Федерации.

Предложенные ранее разными авторами классификационные схемы компьютерной информации либо разделяют на неполные по содержанию группы, либо учитывают не все аспекты обнаружения, изъятия, фиксации и использования цифровой информации в криминалистическом обеспечении расследования различных видов преступлений.

Основное назначение предлагаемой автором криминалистической классификации цифровой информации заключается в том, что она в итоге позволит определить наиболее вероятные направления поиска этой группы источников сведений; разработать особые тактические приемы поиска, изъятия, хранения и т. п. цифровой информации; существенно увеличить эффективность предварительного расследования и судебного разбирательства уголовных дел на основе ее использования.

С учетом вышеизложенного, а также учитывая функциональное и информационное значение цифровой информации для целей криминалистического обеспечения расследования преступлений, источники ее появления или создания, место ее нахождения, целостность или фрагментарность и другие признаки, предлагаются следующие классификационные системы цифровой информации.

Классификация цифровой информации по виду (типу) машинных носителей, на которых

[1] См.: *Вехов В. Б.* Аспекты криминалистического исследования компьютерной информации и ее носителей // Вестник Муницип. ин-та права и экономики. Липецк, 2004. Вып. 1. С. 15–17.

[2] См.: *Зигура Н. А.* Компьютерная информация как вид доказательств в уголовном процессе России : дис. ... канд. юрид. наук. Челябинск, 2010. С. 91.

[3] См.: *Reed C.* Computer Law. N.-Y. : Blackstone, 1990. P. 123–126.

[4] См., напр.: *Иванов Н. А.* Цифровые доказательства: понятие и классификация // Криминалистика в системе правоприменения : материалы конф. М. : МАКС Пресс, 2008. С. 130–134 ; *Его же.* Криминалистическое компьютероведение, компьютерная криминалистика или цифровые доказательства // Роль кафедры криминалистики юридического факультета МГУ им. М. В. Ломоносова в развитии криминалистической науки и практики : в 2 т. М. : МАКС Пресс, 2010. Т. 2. С. 79–82.

она зафиксирована. В рамках данной классификации в первую очередь цифровая информация разбивается на ту, которая содержится на энергозависимых машинных носителях в моменты работы самих аппаратных средств цифровой техники, и на ту, которая содержится на энергонезависимых машинных носителях. Подобное разделение в значительной степени влияет на технологии ее изъятия.

Классификация цифровой информации по аппаратной привязке машинных носителей к средствам цифровой техники. В рамках данной классификационной схемы можно выделить четыре подгруппы: первая подгруппа – это информация, зафиксированная на машинных носителях, «жестко» встроенных в средства цифровой техники, к которым относятся оперативные запоминающие устройства (ОЗУ), постоянные запоминающие устройства (ПЗУ) и машинные носители, являющиеся неотъемлемой частью электронных плат аппаратной части средств цифровой техники; ко второй подгруппе мы относим информацию, зафиксированную на машинных носителях, устанавливаемых (встраиваемых) в средства цифровой техники, но которые могут быть легко демонтированы или заменены без какого-либо ущерба для целостности средств цифровой техники; в третью подгруппу входит информация, зафиксированная на переносимых машинных носителях, устанавливаемых в устройства записи/чтения машинной информации (накопители на гибких магнитных дисках, оптические машинные носители, флэш-карты и т. п.), а также на внешних накопителях на жестких магнитных дисках или твердотельных накопителях, подключаемых через внешние разъемы средств цифровой техники; в четвертую подгруппу включается информация, зафиксированная на машинных носителях большой емкости, входящих в состав локальных, территориальных или глобальных информационно-телекоммуникационных сетей, т. е. на носителях, к которым одновременно имеют доступ большое количество пользователей.

В рамках *классификации цифровой информации по месту ее нахождения* выделяются следующие группы: первая группа – это информация, находящаяся (зафиксированная) на переносимых машинных носителях и машинных носителях, встроенных в средства цифровой техники или подключаемых к ним, принадлежащих конкретному физическому или юридическому лицу, место нахождения которых перед их изъятием заранее установлено; во вторую группу включается информация на машинных носителях, доступная пользователям корпоративных информационно-телекоммуникационных сетей, находящаяся (зафиксированная) на машинных носителях, территориально расположенных на территории Российской Федерации; к третьей группе относится доступная пользователям локальных, территориальных, глобальных телекоммуникационных сетей информация, находящаяся (зафиксированная) на машинных носителях, территориально расположенных за пределами Российской Федерации.

В рамках *классификации цифровой информации по ее функциональному и информационному назначению* можно выделить пять основных групп: программы и программное обеспечение средств цифровой техники; электронные документы; базы данных; аудиовизуальные произведения; иная информация на машинных носителях. В последнюю группу включается информация, содержащаяся в системных и служебных файлах, log-файлах, фрагментах файлов и т. п.

Полагаем, что в рамках криминалистической классификации программ (программного обеспечения) средств цифровой техники можно выделить несколько основных подгрупп. В первую будут входить системное программное обеспечение, необходимое непосредственно для обеспечения работы средств цифровой техники (базовые системы ввода-вывода, операционные системы, программное обеспечение для обеспечения работы периферийной и телекоммуникационной техники), а также сервисное программное обеспечение (драйвера, утилиты, плагины и т. п.). Во вторую подгруппу будет отнесено прикладное программное обеспечение (ППО), предназначенное для решения или выполнения определенных конкретных задач, не связанных непосредственно с обеспечением работы средств цифровой техники. Третью и одну из самых больших по количеству и наименованию легальных прикладных программ подгруппу составляют образовательные, развлекательные и игровые программы, а также различные вспомогательные программы, например, органайзеры. В четвертую группу мы включаем программы, которые были специально созданы для совершения каких-либо противоправных действий, в том числе и так называемые «вредоносные программы».

Электронные документы можно разделить на несколько классификационных групп по различным основаниям. Первую и одну из самых больших групп составляют электронные документы, которые созданы в основном для последующей распечатки документной информации, которую внес пользователь в файл. Эти же файлы используются для осуществления официального и неофициального электронного документооборота. Во вторую группу, которую мы обозначим как электронные сообщения, включаются файлы, содержащие документную информацию в виде текста, звука, изображения и/или их сочетания, формируемые пользователем средств цифровой техники и предназначенные для передачи получателю с помощью различных почтовых сервисов (Mail.Ru, Яндекс.Почта, Gmail, Рамблер, Hotmail, Pochta.ru, Yahoo!), средств мобильной связи (голосовая почта, SMS, MMS). В третью группу мы включаем файлы систем мгновенного обмена сообщениями (Instant Messaging). Их отличие от электронной почты состоит в том, что обмен сообщениями идет в реальном времени (англ. instant – мгновенно). В современных программах сообщения появляются на мониторе собеседника уже после окончания редактирования и отправки сообщения. Широкий круг пользователей пользуется такими популярными системами мгновенного обмена сообщениями, как XMPP, Skype, ooVoo, AIM, ICQ, MSN, Yahoo!. В эту же группу включается и система Twitter, с помощью которой пользователи могут отправлять короткие текстовые заметки (до 140 символов).

Аудиовизуальные произведения, по сути, также являются электронными документами, но в связи с их особым функциональным назначением выделяются в отдельную группу, в которую мы включаем музыкальные и речевые аудиофайлы, аудиовизуальные файлы (фильмы, в т. ч. созданные путем мультипликации, с помощью видеокамер, рекламные ролики и т. п.).

В иную информацию, которая может содержаться (записана, зафиксирована) на машинных носителях, мы относим служебные и системные файлы, удаленные файлы, информацию, содержащуюся во фрагментах файлов, и информацию, записанную на машинных носителях их производителями.

Цифровую информацию по источнику ее происхождения можно разделить на информацию, целенаправленно созданную пользователем средств цифровой техники для ее передачи во времени и пространстве в целях общественного использования и хранения, и информацию, которая создается, фиксируется и отображается автоматически, вне зависимости от желания пользователя средствами цифровой техники, по правилам, установленным заказчиками, или разработчиками программного обеспечения, или производителями средств цифровой техники.

Цифровую информацию по возможности доступа к ней можно разделить на две основные группы. К первой группе относится информация на машинных носителях, доступ к которой собственником (владельцем) никоим образом не ограничивается, ко второй – информация, доступ к которой по тем или иным причинам ограничивается собственником (владельцем, посредником) с помощью специальных аппаратно-программных средств.

Целесообразность разделения цифровой информации по тем или иным классификационным признакам очевидна. Они описывают практически все возможные виды и свойства цифровой информации, что позволяет сотрудникам оперативно-следственных органов учесть каждый из ее видов, в отношении каждого применить те технологии, которые позволят в максимальной степени обеспечить их использование в качестве источников сведений для установления обстоятельств, определенных частью 1 ст. 73 УПК РФ.

В прикладном плане предложенные классификации очень важны для разработки криминалистических средств, приемов, методов, методик обнаружения, фиксации, осмотра, изъятия, исследования цифровой информации, а также использования данной информации при выявлении и расследовании преступлений и в судебном разбирательстве по уголовным делам.