В. Б. Вехов

«ЭЛЕКТРОННАЯ КРИМИНАЛИСТИКА»: ПОНЯТИЕ И СИСТЕМА

Анализ юридической литературы, материалов следственной и судебной практики свидетельствует о том, что электронные следы – электронные носители и содержащаяся в их памяти криминалистически значимая компьютерная информация стали все чаще использоваться в качестве доказательств по уголовным делам о преступлениях различных видов [1, с. 8]. В связи с массовым использованием в уголовном судопроизводстве материальных носителей рассматриваемой категории и содержащейся в их памяти информации УПК РФ был дополнен нормами, регламентирующими порядок работы с ними [2, с. 22–23].

Вместе с тем в настоящее время невозможно представить фотографию и видеозапись без средств цифровой фото- и видеосъемки, документоведение – без компьютерных средств обработки и исследования документов, габитоскопию – без компьютерных средств создания субъективных портретов и восстановления прижизненного облика лица по его костным останкам черепа, дактилоскопию – без средств автоматизированной обработки и идентификации следов пальцев рук, оружиеведение – без компьютерных средств исследования и идентификации следов выстрела на гильзах и пулях, криминалистическую регистрацию – без автоматизированных информационно-поисковых и аналитических систем, исследование электронных доказательств – без соответствующего программно-технического инструментария.

В целях ускорения развития криминалистики как науки на основе инновационных компьютерных технологий, по нашему мнению, целесообразно приступить к формированию в рамках криминалистической техники нового направления – системы научных положений и разрабатываемых на их основе автоматизированных методик расследования отдельных видов преступлений, а также приемов, методов и рекомендаций по их использованию в деятельности органов предварительного расследования. Под автоматизированной методикой расследования отдельных видов преступлений полагаем возможным понимать технико-криминалистическое средство, которое представляет собой информационную систему, базирующуюся на типовой компьютерной модели преступлений, выделяемых в отдельную группу по каким-либо криминалистическим основаниям [3, с. 8–11].

К сожалению, как правильно отмечает Е. Р. Россинская, закономерности возникновения, движения и видоизменения потоков криминалистически значимой компьютерной информации, за исключением рассмотрения этих вопросов в рамках методики расследования преступлений в сфере компьютерной информации, криминалистикой изучаются пока недостаточно. Литература на эту тему носит неупорядоченный фрагментарный характер. Возможности получения и использования подобной информации в криминалистических целях большинству сотрудников органов предварительного расследования и судьям неизвестны, и думается, что для исследования компьютерных средств, систем, сетей и обрабатываемой с их помощью информации необходим особый комплекс специальных знаний. В связи с чем предлагается новая частная теория, которая должна объединять криминалистическое исследование компьютерных средств и систем; рассмотрение в криминалистической тактике особенностей алгоритма и технологии производства следственных действий, направленных на получение криминалистически значимой компьютерной информации, и служить базой для разработки новых и совершенствования имеющихся методик расследования компьютерных преступлений [4, с. 110].

Изложим свою точку зрения относительно названия, системы и содержания элементов предлагаемой теории.

Криминалистическое исследование компьютерной информации, средств ее обработки и защиты определим как систему научных положений и разрабатываемых на их основе технических средств, приемов, методик и рекомендаций по собиранию, исследованию и использованию компьютерной информации, средств ее обработки и защиты в целях раскрытия, расследования и предупреждения преступлений. Подразделим ее на следующие направления:

1. Криминалистическое учение о компьютерной информации.

2. Криминалистическое исследование компьютерных устройств, информационных систем и информационно-телекоммуникационных сетей.

3. Криминалистическое использование компьютерной информации, средств ее обработки и защиты.

Криминалистическое учение о компьютерной информации – это подраздел криминалистического исследования компьютерной информации, средств ее обработки и защиты, который занимается изучением закономерностей возникновения и сокрытия электронных следов и разработкой на этой основе технических средств, приемов и методов по их обнаружению, фиксации, изъятию и исследованию в целях раскрытия, расследования и предупреждения преступлений. В его систему должны входить:

1) криминалистическое исследование документированной компьютерной информации (электронных документов, их отдельных реквизитов, в том числе динамичной и статичной электронной подписи, а также электронно-цифровых ключей);

2) криминалистическое исследование вредоносных компьютерных программ (информационно-программного оружия и следов его применения).

Криминалистическое исследование компьютерных устройств, информационных систем и информационно-телекоммуникационных сетей является вторым подразделом. Он представляет собой систему научных положений и разрабатываемых на их основе технических средств, приемов и методов по исследованию компьютерных устройств, информационных систем и информационно-телекоммуникационных сетей как материальных носителей криминалистически значимой компьютерной информации в целях раскрытия, расследования и предупреждения преступлений. В его структуре целесообразно выделить криминалистические исследования следующих видов носителей электронных следов:

1) машинных носителей информации;

2) интегральных микросхем и микроконтроллеров;

3) пластиковых карт и других комбинированных документов, имеющих электронные реквизиты;

4) компьютеров – электронных вычислительных машин (ЭВМ);

5) информационных систем;

6) информационно-телекоммуникационных сетей.

Криминалистическое использование компьютерной информации, средств ее обработки и защиты – третий подраздел. Определим его как систему научных положений и разрабатываемых на их основе специальных программно-технических средств, а также приемов, методов и рекомендаций по использованию компьютерных технологий и средств защиты информации для раскрытия, расследования и предупреждения преступлений. Основные направления его развития состоят в применении в целях борьбы с преступностью:

1) общедоступных, а также специальных компьютерных программ и устройств, информационных систем и информационно-телекоммуникационных сетей, например: автоматизированных методик расследования преступлений отдельных видов; информационных систем и сетей, обеспечивающих ведение и использование разыскных, криминалистических и экспертно-криминалистических учетов; производство криминалистических экспертиз и исследований;

2) программно-технических средств защиты информации, циркули-

рующей в сфере уголовного судопроизводства, документов, огнестрельного оружия, боеприпасов и чужого имущества;

3) компьютерной информации, в том числе электронных документов, как доказательств по уголовным делам – электронных доказательств.

Как отмечалось ранее [5, с. 10–19], природа информации, носителями которой выступают объекты следообразования, различна. Следообразующий объект выступает носителем непосредственной, первичной информации, выражающейся в совокупности присущих ему индивидуальных и устойчивых свойств и признаков. Следовоспринимающий объект – это носитель отраженной, производной от первого объекта информации, возникшей вследствие их контакта. В результате устанавливается причинно-следственная связь между ними на основе связи с расследуемым событием.

Но следовоспринимающий объект несет информацию не только об отражаемом объекте. Он является также носителем информации о механизме следообразования, то есть о действиях с отражаемым объектом или самого отражаемого объекта. Эта информация передается от системы к системе при помощи каких-либо материальных носителей в виде сигнала, который является отображением сообщения и средством переноса информации в пространстве и во времени.

Сигнал может иметь самую различную физическую природу, в том числе электромагнитную. Он включает в себя содержание информации и форму информации. Отображение определенных свойств объекта или события составляет содержание сигнала. Материальная его основа как средство отображения, хранения и перемещения служит его формой.

Следы, образующиеся при использовании преступником в качестве средства и (или) предмета преступления компьютерной информации, есть отдельная составная часть системы материально фиксированных следов. Они являются объектом поиска, фиксации, изъятия, предварительного и судебно-экспертного исследования по уголовным делам о преступлениях различных видов, а также источником собираемой и используемой в уголовном судопроизводстве доказательственной информации.

В соответствии с примечанием 1 к ст. 272 Уголовного кодекса Российской Федерации (далее – УК РФ) под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Общие криминалистические признаки компьютерной информации целесообразно определить следующим образом:

1) является одной из объективных форм существования информации – электронной формой;

2) всегда опосредована через материальный – электронный носитель, вне которого физически не может существовать;

3) доступ к компьютерной информации могут одновременно иметь несколько лиц;

4) достаточно просто и быстро преобразуется из неэлектронных форм в электронную и обратно, например, при сканировании документа с бумажного носителя и последующей распечатки на бумаге его электронного образа;

5) копируется на различные виды электронных носителей и пересылается на любые расстояния, ограниченные только радиусом действия современных средств электросвязи;

6) обнаруживаются, копируются, исследуются и используются в целях уголовного судопроизводства только с помощью специальных научно-технических средств – средств поиска, сбора, хранения, обработки, передачи и предоставления компьютерной информации.

Компьютерную информацию представляется возможным классифицировать по следующим криминалистическим основаниям.

1. По юридическому положению: недокументированная и документированная. Первая – это данные, управляющие команды и сигналы, образующиеся и (или) используемые в процессе обработки информации и не обладающие признаками документа, например, логин и пароль доступа к сети Интернет или ее ресурсу, сетевой адрес, доменное имя, ключ электронной подписи. Вторая – это зафиксированная на электронном носителе путем документирования информация с электронными реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель.

2. По режиму уголовно-правовой охраны: информация общего пользования и охраняемая законом.

3. По форме представления: файл, сетевой адрес, информационная система, база данных, программа для ЭВМ (компьютерная программа), доменное имя, электронное сообщение, электронная подпись, электронный документ, электронный журнал, электронные денежные средства, сайт, страница сайта.

4. По возможности использования в качестве информационного оружия. К этой категории относится вредоносная компьютерная программа – компьютерная программа либо иная компьютерная информация, которая предназначена для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств ее защиты (ч. 1 ст. 273 УК РФ). Как упоминалось ранее,

она является разновидностью информационного оружия – информационно-программным оружием, которое основано на применении разрушающего программного воздействия на аппаратное, программно-математическое обеспечение, компьютерную информацию, в том числе на средства ее защиты, информационные системы и информационно-телекоммуникационные сети [6]. Фактически вредоносные компьютерные программы представляют собой программные автоматы – самодействующие в электронной среде виртуальные устройства, производящие работу по заданной преступником программе без его непосредственного участия. Они являются как предметом отдельного, предусмотренного ст. 273 УК РФ, так и средством совершения других преступлений.

Выделим следующие общие криминалистические признаки вредоносной компьютерной программы:

1) программа способна уничтожать, блокировать, модифицировать либо копировать компьютерную информацию или нейтрализовать средства защиты компьютерной информации;

2) программа не предполагает предварительного уведомления обладателя или пользователя компьютерной информации, компьютерного устройства, информационной системы или информационно-телекоммуникационной сети о характере своих действий;

3) программа не запрашивает согласия (санкции) у обладателя или пользователя компьютерной информации, компьютерного устройства, информационной системы или информационно-телекоммуникационной сети на реализацию своего назначения – алгоритма работы.

Отсутствие у компьютерной программы хотя бы одного из этих признаков делает ее невредоносной.

Литература

1. Вехов В. Б. Криминалистическое учение о компьютерной информации и средствах ее обработки: дис. … д-ра юрид. наук. Волгоград, 2008.

2. Вехов В. Б. Работа с электронными доказательствами в условиях изменившегося уголовно-процессуального законодательства // Российский следователь. 2013. № 10.

3. Вехов В. Б. Автоматизированные методики расследования преступлений как новое направление в криминалистической технике // Известия Тульского государственного университета. Экономические и юридические науки. Вып. 3. Ч. II. Юридические науки. Тула, 2016.

4. Россинская Е. Р. К вопросу о частной теории информационно-компьютерного обеспечения криминалистической деятельности // Известия

ТулГУ. Экономические и юридические науки. Вып. 3. Ч. II. Юридические науки. Тула, 2016.

5. Вехов В. Б. Электронные следы в системе криминалистики / В. Б. Вехов, Б. П. Смагоринский, С. А. Ковалев // Судебная экспертиза. Вып. 2 (46) 2016. Волгоград, 2016.

6. Вехов В. Б. Вредоносные компьютерные программы как предмет и средство совершения преступления // Расследование преступлений: проблемы и пути их решения: сб. науч.-практ. тр. М., 2015. № 2.

К. В. Гончаров

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ОПТИМИЗАЦИИ ИСПОЛЬЗОВАНИЯ РЕЗУЛЬТАТОВ ОПЕРАТИВНО-РАЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ В РАССЛЕДОВАНИИ ЗЛОУПОТРЕБЛЕНИЙ ПОЛНОМОЧИЯМИ ЛИЦАМИ, НАДЕЛЕННЫМИ УПРАВЛЕНЧЕСКИМИ ФУНКЦИЯМИ В КОММЕРЧЕСКИХ И ИНЫХ ОРГАНИЗАЦИЯХ

Сложный, серийный и завуалированный характер злоупотребления полномочиями субъектами управленческой деятельности обеспечивает объективную потребность к обращению к потенциалу оперативно-разыскной деятельности [1, с. 57–60; 2, с. 17–20]. Результаты оперативно-разыскной деятельности, как показывает следственно-судебная практика по делам данной категории преступлений, выступают не только одним из типичных элементов содержания такого повода для возбуждения уголовного дела, как сообщения о преступлении, полученного из иных источников, но и активно реализуются в процессе всего предварительного расследования [3, с. 61–64].

Напомним, что в соответствии с п. 36.1 ст. 5 УПК РФ под результатами оперативно-разыскной деятельности понимаются «сведения, полученные в соответствии с федеральным законом об оперативно-разыскной деятельности, о признаках подготавливаемого, совершаемого или совершенного преступления, лицах, подготавливающих, совершающих или совершивших преступление и скрывшихся от органов дознания, следствия или суда».

Процесс представления и использования в расследовании результатов оперативно-разыскной деятельности регулируется оперативно-разыскным и уголовно-процессуальным законодательством. В соответствии со ст. 11 Федерального закона «Об оперативно-розыскной деятельности»