О НЕКОТОРЫХ ИННОВАЦИЯХ ТАКТИКИ ОСМОТРА МЕСТА ПРОИСШЕСТВИЯ ПО ДЕЛАМ, СОПРЯЖЕННЫМ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНО-ЭЛЕКТРОННЫХ СРЕДСТВ

Дёмин К.Е.
Московский университет МВД России имени В.Я. Кикотя, г. Москва
email: diomin.costia@yandex.ru

Аннотация. В статье рассматриваются вопросы собирания доказательств с электронных носителей информации. Приводятся основные тактические приемы получения криминалистически значимой с указанных носителях, устанавливается их классификация в соответствии с решаемыми следственными задачами.

Ключевые слова: информационно-телекоммуникационная система; накопители на жестких магнитных дисках; компьютерные преступления; компьютерно-электронные средства, радиоэлектронное устройство; судебная компьютерно-техническая экспертиза; электронный документ.

Осмотр места происшествия (ОМП) по делам, сопряженным с использованием компьютерных средств технологий, как и в любых иных случаях относится к неотложным следственным действиям, состоящем в «… непосредственном восприятии, исследовании и фиксации объектов материальной обстановки, предметов и документов в целях обнаружения следов преступления, вещественных доказательств, выяснения обстановки происшествия и других обстоятельств, имеющих отношение к происшедшему событию [1, с. 429]». Принимая во внимание специфику следовой картины рассматриваемого вида преступлений, необходимо указать на то, что следы отображаются на «нетрадиционных» с точки зрения классической криминалистики носителях и не в «традиционном» виде, в них находит свое отражение «виртуальность» их существования в виде электронного сигнала. Так, для накопителя на жёстких магнитных дисках (НЖМД) или сменного носителя информации, например USB-флеш накопителя, они характеризуются в организации файловой системы, объеме занятой ими памяти, электронной структуры, частными характеристиками электронных носителей данных (ЭНД) и электронных документов (ЭД) на нем и т.д. Все указанные особенности должны отражаться в процессуальных документах (протокол ОМП). На наш взгляд, именно такая форма должна отражаться и учитываться при организации и процессуальном закреплении информации, содержащейся в электронной форме. В ходе проведения осмотра компьютерно-электронных средств (КЭС) основными объектами интереса следователя должны являться компьютерное или радиоэлектронное оборудование, ЭНД, в которых находятся ЭД, в ходе осмотра которых осматриваются папки, файлы, IP-адреса, базы данных КЭШ-памяти и т.д. Осмотр системного блока должен сопровождаться фиксацией в протоколе ОМП, в котором фиксируется содержание жесткого диска с детализацией выявленной информации. В процессе осмотра КЭС особое внимание обращается на имеющуюся следовую картину как будущего объекта как СКТЭ, так и иных видов судебных экспертиз, например, судебно-бухгалтерской, экономической, автотехнической и т.д. Не следует пренебрегать сбором традиционных следов (следов пальцев рук, различного рода микрочастиц, микроследов, микровеществ и т.п.), дальнейшее исследование которых позволит доказать факт нахождения оборудования у конкретного лица.

Как мы уже указывали раннее, «…недопустимо проводить какие-либо действия в процессе следственного осмотра КЭС, без наглядного и доступного комментария, без гарантий сохранности следовой картины криминального события, …объяснено должно быть любое нажатие на клавишу клавиатуры, передвижение

мыши. Это в дальнейшем позволит обезопасить добытые доказательства от негативной оценки их допустимости судом. Во всяком случае, понятые, не будучи специалистами в области компьютерных технологий (что зачастую и бывает), должны понимать, что делается и каков результат произведенных действий [2, с. 149-151]».

Порядок осмотра любых КЭС условно можно условно разделить на две стадии: на стадии статической стадии фиксируются данные о внешнем строении и физическом состоянии объекта, за которой следует динамическая стадия осмотра на которой собственно изучается и фиксируется информационное содержимое электронного аппарата, собственно на этой стадии и происходит поиск, обнаружение, фиксация и изъятие ЭД. Отметим, что осмотр ЭНД может идти параллельно с иными СД. Например, КЭС в виде сотовых телефонов, смартфонов, электронных ключей и магнитных карт для систем аутентификации и идентификации, в которых содержатся ЭД, имеющих доказательственное значение, могут находиться у сотрудников фирмы. Поэтому целесообразно первоначально провести обнаружение и приобщение к уголовному делу указанных предметов (например, в ходе выемки вышеперечисленных лиц или обыска помещения) и после этого приступать к непосредственному осмотру КЭС. Проведенное исследование показывает, что при проведении следственных действий изымались следующие электронные аппараты с электронными носителями данных (рис 1).

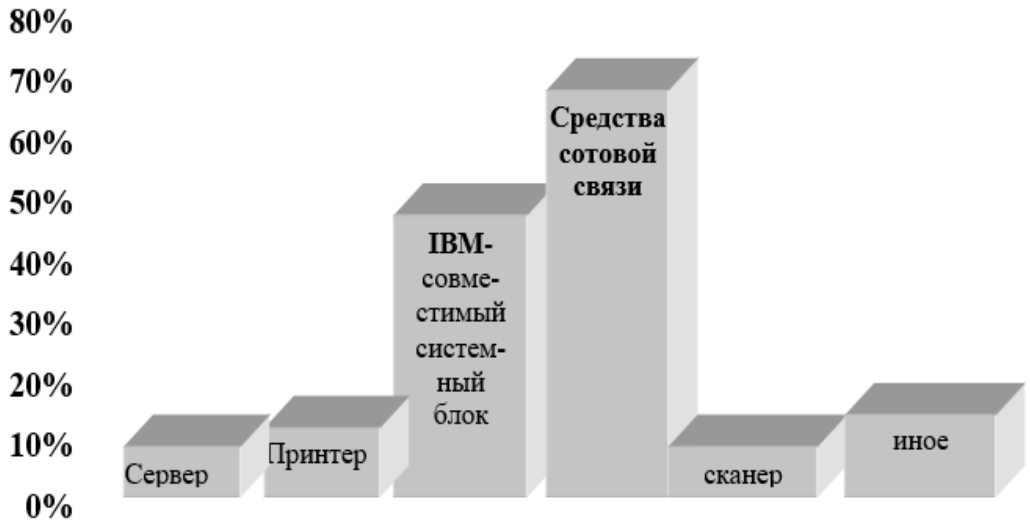

Рисунок 1. Средства электронной техники, изъятые в ходе расследования преступлений.

Изъятие информации из КЭС в строгом соответствии с процессуальными нормами и разработанными методиками - важнейшая задача оперативно-следственной группы [2, с. 149-151; 3, с. 72; 4, с. 140]. Тактические приемы на начальной стадии, должны содержать следующий комплекс оперативно-розыскных, следственных и организационно-технические мероприятий:

- предварительное изучение имеющихся оперативных материалов. Проведение спецоперации по выяснению полной технической реализации компьютерной сети, выяснение аппаратно-программной оснащенности учреждения и построения схемы связи;
- при необходимости реализация мероприятий по устранению возможных причин противодействия проведению ОРМ и СД;

- проведение осмотра (в соответствии со ст. 176, 177 УПК РФ) аппаратно-программного обеспечения с проведением исследования ЭД и ЭНД и выяснения функционального назначения КЭС, с составлением протокола осмотра;
- проведение выемки с целью обнаружения информационных массивов, и аппаратов используемых в качестве орудий совершения преступления, или для хранения криминалистически значимой информации;
- проведение опроса на месте проведения следственного действия с участием специалистов-экспертов, следующих лиц: операторов и программистов, административного состава, руководителей фирмы или учреждения;
- назначение и (возможно) проведение комплексной судебной компьютерных исследований. Изъятие образцов для экспертного исследования.

Целевой функцией при проведении указанных оперативно-следственных мероприятий является обнаружение, фиксация и изъятие доказательств совершенного преступления. В связи с этим необходимо сформулировать следующие требования, имеющие, в связи со спецификой объектов исследования – электронных документов и носителей информации, принципиальное значение:

- требование сохранности вещественных доказательств, в качестве каковых выступают как ЭНД, так и ЭД, которые должны храниться в неизменном виде;
- сохранения возможности проведения их повторных исследований;
- требование обеспечения возможности воспроизведения действий эксперта-криминалиста другими экспертами.

При производстве осмотра важно помнить о возможности нахождения встроенных команд по стиранию и уничтожению данных, поэтому очень важно, никого не допускать к компьютерам, произвести отключение от них всех устройств, которые могут каким-либо способом изменить в них информацию (модемы, сетевые кабели (если есть), клавиатура, мышь и т.п.).

После этого производятся следственные действия, в ходе которых следователем совместно со специалистом вырабатывается дальнейший ход мероприятия и необходимые при этом действия по изъятию компьютерной техники. Например, изъять компьютер целиком или произвести только изъятие информации, какой именно и в каком виде. Если изымается компьютер, особенно важно, если он выключен, то не включать его, а если включен, то выключить его с минимально возможными потерями информации. Поэтому особенно важно, чтобы специалист знал корректный способ выхода из различных операционных систем. Также было отмечено нами раннее, что необходимо использовать только легально приобретенными компьютерными программами, причем на место происшествия специалист выезжает, имея с собой обширный арсенал компьютерной техники, которая может ему пригодиться при копировании информации, ее восстановлении, декодировки и прочее. Как отмечалось нами раннее, необходимо указывать и возможные компьютерные или радиоэлектронные средства хранения электронных данных, уполномоченное лицо в соответствии со ст. 82 УПК РФ должно обеспечить сохранность изъятых аппаратных компонентов, в которых содержаться ЭД. Эти дополнения, также позволят тактически правильно и существенно повысить доказательственную силу ЭД в суде [5, с. 40-45].

Таким образом, любой ЭД, находящийся на ЭНД, при его обнаружении, фиксации и изъятии должен пройти следующие последовательные «… стадии:

- процессуально корректное установление аппаратного носителя, на и в котором находятся электронные массивы информации, установление формы и вида ЭД;
- процессуально корректное установление ЭД;
- фиксация ЭД с помощью сертифицированных методик и сертифицированного оборудования в том виде, в котором он был обнаружен;

- создание идентичной копии носителя с электронным массивом, в котором находится электронный документ;
- составление протокола осмотра ЭКС (предметов) с фиксацией носителя и электронного документа; если необходимо, трансформация электронного документа с помощью сертифицированных методик и оборудования в вид удобный для восприятия следователем или судом;
- исследование ЭД в условиях места происшествия или в экспертном учреждении с помощью сертифицированных методик и оборудования. Представление его в виде удобном для восприятия участниками уголовного или гражданского судопроизводства;
- оценка полученного ЭД в соответствии ст. 88 УПК Российской Федерации [4, с. 33-37]».

Таким образом, можно сделать вывод, о необходимости комплексного подхода при расследовании преступлений в сфере высоких технологий, сочетающего в себе тактику ОМП, основанную на методах классической криминалистики в сочетании с IT технологиями [7, с.51; 8, с. 73; 9, с.185], имеющего своей целью процессуальную корректность поиска, обнаружения, фиксации и исследования информационной следовой картины криминального события, получение доказательств, соответствующие требованиям ст.88 УПК.

Библиографический список

1. Криминалистика: Учебник / Отв. ред. Н.П. Яблоков. —3-е изд., перераб. и доп. // М.: Юристъ, 2005.
2. Васильев А.А., Дёмин К.Е. Криминалистические аспекты получения доказательственной информации с электронных носителей данных// Публичное и частное право. - 2011. – вып. III (XI) — С. 147-162.
3. Гердт К.М., Поляков В.В. Получение компьютерной информации : понятие, содержание и особенности производства оперативно-розыскного мероприятия//Проблемы правовой и технической защиты информации. — 2019. – № 7. — С. 71-75.
4. Сторожева Е.Е. Особенности следовой картины по компьютерным преступлениям // Проблемы правовой и технической защиты информации. — 2018. № 6. — С. 137-141.
5. Дёмин К.Е. , Васильев А.А. Методологические основы получения криминалистически значимой информации с мобильных платформ сотовой связи// Актуальные вопросы судебных экспертиз: материалы междунар. науч.-пр. конф. Иркутск, 14-15 апреля 2011г. — Иркутск ФГОУ ВПО «Восточно-сибирский институт МВД России» . – 2011. — С. 39-46.
6. Дёмин К.Е. О перспективах исследования электронных документов как объектов судебной экспертизы // Вестник академии экономической безопасности МВД России. — М.: Московский университет МВД РФ им.В.Я. Кикотя. – 2016 (4). — С. 33-37.
7. Васюков В.Ф. Использование криминалистически значимой и доказательственной информации об абонентах и абонентских соединениях при расследовании уголовных дел : монография / В.Ф. Васюков. – Орел: Орловский юридический институт МВД России имени В.В. Лукьянова, 2013. 120 с.
8. Беляев М.В., Демидова Т.В. Применение инновационных технологий при осмотре мест дорожно-транспортных происшествий // Вестник Академии экономической безопасности МВД России. – М.: Московский университет МВД РФ им.В.Я. Кикотя. – 2015 (2). – С. 72-77.
9. Хмыз А.И. Получение розыскной информации в ходе исследования электронных документов и их материальных отображений // Исторические,

философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. – Тамбов: Грамота, 2015. – № 12. – С. 184-189.

ON SOME INNOVATIONS IN THE TACTICS OF EXAMINING THE SCENE OF AN ACCIDENT IN CASES INVOLVING THE USE OF COMPUTER AND ELECTRONIC MEANS

Demin K.E.
Moscow University of the Ministry of the Interior of Russia named after V.Y. Kikotya, Moscow
email: diomin.costia@yandex.ru

Abstract. The article deals with the issues of collecting evidence from electronic media. The main tactical techniques for obtaining criminally significant information from these media are given, and their classification is established in accordance with the investigative tasks to be solved.

Keywords: information and telecommunication system; hard disk drives; computer crimes; computer-electronic means, radio-electronic device; forensic computer-technical expertise; electronic document.