МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное казенное образовательное учреждение
высшего образования
«Уфимский юридический институт Министерства внутренних дел
Российской Федерации»

Кафедра криминалистики

ДИПЛОМНАЯ РАБОТА

на тему **«ОСОБЕННОСТИ ОБНАРУЖЕНИЯ И ИЗЪЯТИЯ ДОКАЗАТЕЛЬСТВЕННОЙ ИНФОРМАЦИИ С ЭЛЕКТРОННЫХ НОСИТЕЛЕЙ, ЗНАЧЕНИЕ СУДЕБНОЙ КОМПЬЮТЕРНОЙ ЭКСПЕРТИЗЫ В РАССЛЕДОВАНИИ УГОЛОВНЫХ ДЕЛ (ПО МАТЕРИАЛАМ ТЕРРИТОРИАЛЬНОГО ОРГАНА ВНУТРЕННИХ ДЕЛ)»**

Выполнила
Семёнова Оксана Эдуардовна
обучающаяся по специальности
40.05.01 Правовое обеспечение
национальной безопасности
2017 года набора, 7101 учебной
группы

Руководитель
доцент кафедры криминалистики,
кандидат технических наук
Харисова Зарина Ирековна

К защите_____
рекомендуется / не рекомендуется
Начальник кафедры _____Э.Д. Нугаева
подпись
Дата защиты «___»_____2023 г. Оценка_____

ПЛАН

ВВЕДЕНИЕ

Актуальность темы работы заключается в широком применении информационных технологий (дале – ИТ) и технических средств с электронными носителями данных (далее – ЭНД) в различных сферах жизнедеятельности общества, что непосредственно повлияло на рост количества преступлений, совершаемых с их использованием. Повышенная общественная опасность данных деяний связана со сложностями их обнаружения в транснациональном киберпространстве, не имеющем государственных границ, что зачастую создает сложность в установлении лица, совершившего такое преступление.

Для повышения эффективности борьбы с указанными видами преступлений в уголовное законодательство на постоянной основе вносятся коррективы, добавляются отдельные положения и нормы. Так, например, были внесены значительные изменения, в частности, актуализации подверглись нормы, содержащиеся в главе 28 Уголовного кодекса Российской Федерации от 13 июня 1996 г. № 63-ФЗ[1]. Но для успешной борьбы с киберпреступлениями этих мер не всегда хватает. Действующее уголовное законодательство Российской Федерации на сегодняшний день не содержит охватывающей всю IT-преступность нормативно-закрепленной базы, а также механизмов для учета ответственности по рассматриваемым преступлениям в соответствии с их правомерной и реальной опасностью. Кроме того, в законодательстве в полной мере не определены и нормативно не закреплены понятия «преступление, совершаемое с использованием компьютерных технологий», «компьютерные технологии» и ряд других схожих понятий. В настоящее время по поводу определения, содержания, а также процессуального порядка получения, оценки

[1] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 24 мая 1996 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 5 июня 1996 г. // Собр. законодательства Рос. Федерации. – 1996. – № 25, ст. 2954.

и использования информации на ЭНД ведутся активные научные дискуссии. В число актуальных вопросов входит правовая неопределенность понятия электронного носителя информации как источника доказательственной информации. Недостатки правовой регламентации процессуального порядка получения доказательственной информации на электронных носителях зачастую отражаются на качестве расследования уголовных дел, эффективности сбора и оформления доказательств в виде информации на электронных носителях. Кроме того, противоречивость правоприменительной практики и недостаток научно обоснованных рекомендаций относительно порядка проверки и использования информации на ЭНД негативно сказываются на решении задач уголовного судопроизводства.

Теоритическая значимость определяется совокупностью перечисленных факторов, формирующих актуальные вопросы, связанные с необходимостью изучения особенностей совершения преступлений в сфере компьютерной информации и форм использования специальных знаний в их расследовании. Практическая значимость заключается в организации взаимодействия органов предварительного следствия со специалистами, способствующими раскрытию IT-преступлений, в том числе при обнаружении и изъятии доказательственной информации с ЭНД.

Стоит отметить, что преступления в сфере компьютерной информации имеют высокую степень латентности, которая достигает 90 %, при этом раскрываемость компьютерных преступлений составляет не более 5 %[1]. В связи с этим особое значение приобретает использование результатов различных судебных экспертиз при их выявлении и расследовании. Производство указанных экспертиз является составной частью деятельности по обеспечению безопасности, выявлению угроз и противодействию им.

Развитие науки и техники в области цифровой криминалистики в настоящее время не имеет соответствующего уровня экспертного

[1] Мазуров В. А. Компьютерные преступления. Классификация и способы противодействия: учебно-практическое пособие. М.: Палеотип, Логос, 2022. С. 167.

методического обеспечения, что осложняет расследование киберпреступлений и производство судебных экспертиз по ним. Кроме того, стремительное развитие информационных технологий, появление новых видов киберпреступности и изменение механизмов и методов их совершения требуют от специалистов, задействованных в раскрытии и расследовании такого рода преступлений, постоянного повышения квалификации.

Цель данной работы заключается в комплексном анализе особенностей применения специальных знаний при расследовании преступлений в сфере компьютерной информации, в частности, при назначении и производстве судебных компьютерных экспертиз (далее − СКЭ) ЭНД и использования их результатов при выявлении и расследовании преступлений.

Задачи работы:

– определение понятия и проведение классификации ЭНД;

– выделение особенностей проверки и оценки доказательственной информации на электронных носителях;

– определение правого положения электронных носителей информации в системе видов доказательств;

– анализ организации взаимодействия органов предварительного расследования со специалистами в сфере компьютерных технологий;

– рассмотрение предмета, объекта и задач судебных экспертиз, их назначение при расследовании IT-преступлений;

– выявление особенностей назначения и производства компьютерно-технических и иных видов экспертиз.

Для достижения цели работы и решения поставленных задач был использован универсальный диалектический метод познания, а также комплекс общенаучных и специальных методов, обеспечивающих объективность, всесторонность и полноту изучения предмета работы.

Объектом работы являются общественные отношения, складывающиеся в процессе обнаружения доказательственной информации, содержащейся на ЭНД, их изъятия и проведения судебных экспертиз ЭНД, а также

использования полученных результатов при выявлении и расследовании киберпреступлений.

Предметом работы являются генезис и современное состояние нормативного регулирования вопросов обнаружения, изъятия, проверки и оценки доказательственной информации на электронных носителях, ее использования в уголовно-процессуальном доказывании, а также практика реализации соответствующих нормативных предписаний, положений Конституции Российской Федерации, решений Конституционного Суда Российской Федерации, правоприменительной практики Верховного Суда Российской Федерации и нижестоящих судов, нормы уголовно-процессуального права России, литература в области уголовного процесса, криминалистики, а так же иная научно-техническая литература по теме исследования, материалы судебной практики и статистики.

Структура дипломной работы определяется целью и задачами и состоит из введения, двух глав, включающих шесть параграфов, заключения и списка использованной литературы.

ГЛАВА 1. ОСОБЕННОСТИ ОБНАРУЖЕНИЯ И ИЗЪЯТИЯ ДОКАЗАТЕЛЬСТВЕННОЙ ИНФОРМАЦИИ С ЭЛЕКТРОННЫХ НОСИТЕЛЕЙ

§ 1. Понятие и классификация электронных носителей информации

Достижения человечества в области информационных технологий способствовали развитию и модификации комплексных технических систем, обрабатывающих значительные массивы данных. Для ее получения, копирования, дистанционной передачи, а также для долгосрочного хранения в настоящее время используются множество типов и моделей ЭНД.

Повсеместное использование накопителей данных стало важным событием не только в информационной среде, но и при построении общественных отношений во всех сферах деятельности человека, а так же информационном обмене государственных институтов власти.

Тем не менее понятие «электронный носитель информации» на текущий момент никак не закреплено законодательно, но, отражено в ГОСТ Р 2.051-2013 Единая система конструкторской документации (далее – ЕСКД) «Электронные документы»[1], так в п. 3.1.9 термин «электронный носитель» определяется как материальный носитель, используемый для записи, хранения и воспроизведения информации, обрабатываемой с помощью средств вычислительной техники. Таким образом, электронный носитель – это любой материальный носитель, содержащий совокупность технических элементов, работающих посредством функционирования электронов в определенном информационном поле, использующийся в целях записи, хранения и воспроизведения информации, обрабатываемой с помощью различных средств вычислительной техники.

[1] ГОСТ 2.051-2013 Единая система конструкторской документации. Электронные документы. Общие положения : дата введения 1 июня 2014. – Москва: Стандартинформ, 2011 год.

Для полноценного понимания термина «электронный носитель» следует проанализировать его наиболее распространенные виды. Наиболее распространенной является классификация электронных носителей по признаку зависимости хранения данных на устройстве от источника питания (батареи). Рассматривая данный подход следует выделить, во-первых, энергозависимые носители, к которым можно отнести устройства, данные в которых остаются постоянными только благодаря использованию источника питания (батареи). К такого рода устройствам можно отнести:

1. Оперативное запоминающее устройство (далее − ОЗУ) электронных вычислительных машин (далее − ЭВМ). В момент запуска компьютера (при включении электропитания) в ОЗУ ЭВМ в определенном порядке загружаются файлы совместно с командами (программами) и данными, обеспечивающими для персонального компьютера (далее − ПК) возможность их обработки. Сведения о том, где и какая информация хранится или какими командами обрабатывается в ОЗУ ЭВМ в каждый конкретный момент доступны пользователю и при необходимости могут быть получены немедленно с помощью встроенных стандартных инструментов. Таким образом, ОЗУ ЭВМ фактически является носителем компьютерной информации. При этом нужно учитывать, что оно является энергозависимым, то есть данные стираются в момент отключения данного устройства от источника питания.

2. ОЗУ периферийных устройств. В процессе обработки информации компьютер ведет активный обмен информацией со своими периферийными устройствами, в том числе с устройствами ввода и вывода информации, которые, в свою очередь, имеют собственные оперативные запоминающие устройства, где временно хранятся массивы информации, предназначенные для обработки этими устройствами (например, лазерный принтер, где «в очереди» на печать присутствует несколько документов). Необходимо заметить, что создание оперативных запоминающих устройств является развивающейся тенденцией. Устройство ОЗУ периферийных устройств сходно с ОЗУ ЭВМ, но

поддается контролю и управлению и, следовательно, может рассматриваться как носитель компьютерной информации[1].

Одним из типов носителей являются энергонезависимые накопители, которые способны хранить данные при отсутствии электрического питания. Энергонезависимые носители, в свою очередь, можно разделить на следующие группы:

магнитные накопители;

оптические накопители;

магнитно-оптические накопители;

постоянно программируемое запоминающие устройство;

флеш-накопители.

Магнитные накопители, в свою очередь, подразделяются на три вида электронных носителей:

гибкий магнитный диск (дискета), которые в настоящее время практически не встречаются в практике;

накопитель на жестком магнитном диске (жесткий диск – HDD);

твердотельный накопитель (SSD);

flash-диск.

Жесткий диск (HDD), как правило, установлен внутри ПК. Для полноценной работы персонального компьютера и мобильных устройств необходим хотя бы один жесткий диск, при этом могут быть установлены и дополнительные накопители данных. Сведения о конкретном жестком диске могут быть получены путем использования встроенных в операционную систему (далее – ОС) программных средств, сторонних утилит, а также исходя из маркировки, нанесенной на диске.

В интересах расследования необходимы знания о таком свойстве жесткого диска (и других электронных носителей), как емкость. Емкость жесткого диска означает максимальный объем данных, которые могут на нем

[1] Телевицкая Ю. А. Понятие электронных носителей информации: проблемные аспекты интерпретации и толкования // Альманахъ молодых ученых: сборник научных статей. Том № 2 (4). Нижний Новгород: Нижегородская академия МВД России, 2021. С. 136.

храниться. Сведения о емкости зачастую могут быть полезны в тактическом плане. Например, свидетельствовать о намерениях пользователя по наполнению жесткого диска информацией определенного объема, а также о фактическом объеме компьютерной информации на носителе (последнее предполагает выбор следователем соответствующего электронного носителя, если принято решение об изъятии информации в ходе производства следственного действия).

Альтернативой жесткому диску является твердотельный накопитель (SSD) − компьютерное энергонезависимое запоминающее устройство на основе микросхем памяти. Другими словами, в них отсутствуют движущиеся механические части, и это является важной особенностью. Наиболее распространённый вид твердотельных накопителей использует для хранения информации флеш-память типа «NAND» (энергонезависимая флеш-память, которая может хранить данные, даже если она не подключена к источнику питания), однако существуют варианты, в которых накопитель создаётся на базе DRAM-памяти (тип компьютерной памяти, отличающийся использованием полупроводниковых материалов, состоящий из ячеек, созданных в виде емкости, где заряженная или разряженная ячейка хранит бит данных и, так как каждая ячейка такой памяти имеет свойство разряжаться – данный тип памяти снабжается аккумулятором). Помимо собственно микросхем памяти, подобный накопитель содержит управляющую микросхему − контроллер[1]. Твердотельный накопитель в разы быстрее жесткого диска, а также лучше защищен от падений, сотрясений, ударов и повседневного износа, что снижает вероятность потери данных. Благодаря своей скорости и надежности твердотельные накопители являются отличным вариантом для новых сборок ПК, серверов и сборщиков систем. Но HDD-диски в отличие от SSD-дисков обладают большим количеством циклов перезаписи и более высокой надежностью.

[1] Умнягина Ю. А. Электронные носители информации в уголовном судопроизводстве // Вестник Уральского юридического института МВД России. 2020. № 4(28). С. 52.

Оптические накопители обозначают категорию дисков, чтение с которых на компьютерных устройствах ведется с помощью оптического (лазерного) излучения. Оптические диски имеют различные модификации. Так, например, CD-диски имеют модификации CD-R, CD-ROM. DVD-диски имеют модификации DVD-R, DVD+R, DVD-DL, DVD+DL, DVD-RW, DVD+RW и др[1]. Здесь же необходимо отметить, что диски могут быть предназначены для однократной и многократной записи, а также предоставлять возможность односторонней и двухсторонней записи. Следователь должен иметь представление о модификациях дисков. Например, в ситуации, когда в ходе обыска обнаружены диски формата DVD-DL (с информацией на них), а на месте производства следственного действия отсутствует оптический дисковод, позволяющий осуществлять двухстороннюю запись, следователь может выдвинуть версию о местонахождении данного устройства в ином помещении.

Магнитно-оптические накопители сочетают в себе свойства оптических и магнитных дисков, которые изготавливаются с использованием ферромагнетиков. Магнитно-оптический диск взаимодействует с операционной системой так же как жесткий диск.

Постоянное программируемое запоминающее устройство ЭВМ состоит из интегрированных микросхем, содержащих общую программу управления, которая состоит из последовательно выполняемых рабочих программ – алгоритмов управления. Они не являются энергонезависимыми, данные не стираются в момент его отключения от источника питания. Данный элемент встроен в аппаратное устройство и фактически является носителем компьютерной информации.

Однако, в настоящее время, самыми распространенными электронными носителями информации являются флеш-накопители (flash-диск). Значительная емкость и компактные размеры позволяют легко переносить их, например, в кошельке или кармане. В зависимости от устройства носителя и его

[1] Россинская Е.Р. Проблемы использования специальных знаний в судебном исследовании компьютерных преступлений в условиях цифровизации // Вестник Университета имени О.Е. Кутафина. 2019. № 5 (57). С. 44.

применения выделяют USB-накопители и карты памяти SD (формат карт памяти, разработанный для использования в портативных устройствах). Также существуют и иные электронные носители информации.

Развитие информационно-телекоммуникационных технологий (далее − ИТТ) и их активное использование в повседневной жизни открыли новые возможности для обмена информационными ресурсами между пользователями. Вместе с тем появилась новая возможность для совершения преступлений путем использования данных технологий, в частности, осуществлением удаленного доступа к техническим средствам, что существенно облегчает организацию противоправных действий, и, следовательно, требует правового урегулирования и совершенствования законодательства в данной сфере для полноценного и всестороннего расследования преступлений, связанных с информационными технологиями.

Так, уместно изложить определение, данное В. С. Комиссаровым, который преступлениями в сфере компьютерной информации признает «умышленные общественно опасные деяния (действие или бездействие), причиняющие вред либо создающие угрозу причинения вреда общественным отношениям, регламентирующим безопасное производство, хранение, использование или распространение информации и информационных ресурсов либо их защиту»[1].

Общим объектом данных преступлений являются общественные отношения по обеспечению информационной безопасности. К числу непосредственных объектов преступных посягательств относятся: компьютерная информация, средства ее использования и хранения, отдельные файлы определенных информационно-телекоммуникационных сетей, а также ИТ, средства программной обработки и передачи данных, в том числе обеспечивающие защиту информации от неправомерного доступа.

[1] Комиссаров В. С., Крылова Н. Е., Тяжкова И. М. Уголовное право Российской Федерации: учебник. М.: Статут, 2016. С. 429.

Согласно ст. 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»: «информация − это сведения (сообщения, данные) независимо от формы их представления, а документированная информация − это зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель»[1].

Согласно примечанию к ст. 272 УК РФ [2], под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Так же следует рассмотреть классификацию электронных носителей информации, определяющую содержание уголовно-процессуального порядка собирания содержащейся на них доказательственной информации, которая производится по следующим основаниям:

по характеру связи с расследуемым событием: первичные (связанные непосредственно с событием преступления) и вторичные (полученные в ходе следственных и иных процессуальных действий);

по способу использования и получения доступа к содержащейся на электронных носителях информации: локальные (используемые путем непосредственного физического подключения к информационной системе или считывающему устройству) и сетевые (используемые путем опосредованного (дистанционного) соединения по каналам связи);

---

[1] Об информации, информационных технологиях и о защите информации: федер. закон Рос. Федерации от 27 июля 2006 г. № 149-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 8 июля 2006 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 14 июля 2006 г. // Собр. законодательств Рос. Федерации. – 2006. – № 31 (ч.1), ст. 3448.

[2] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 24 мая 1996 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 5 июня 1996 г. // Собр. законодательства Рос. Федерации. – 1996. – № 25, ст. 2954.

по возможности перемещения в пространстве: стационарные (конструктивно не предназначенные для перемещения информации из одной информационной системы в другую) и портативные (конструктивно предназначенные для перемещения информации между информационными системами);

по типу устройства хранения информации: внутренние (являющиеся неотъемлемым компонентом информационной системы, без которых невозможно ее функционирование) и внешние (являющиеся дополнительным (факультативным) компонентом информационной системы, изъятие которых не приведет к нарушению ее функциональности);

по сроку хранения информации: оперативного хранения (в течение срока определенного информационного процесса), временного хранения (в течение определенного временного интервала) и постоянного хранения (неограниченно);

по функциональной принадлежности: монофункциональные (для которых хранение информации является основной и единственной функцией) и полифункциональные (для которых хранение информации не является основной и единственной функцией);

по возможности автономной работы: энергозависимые (не способные выполнять функцию хранения информации без внешнего энергопотребления) и энергонезависимые (способные хранить информацию без внешнего энергопотребления).

В заключение настоящего параграфа следует отметить, что электронный носитель информации представляет собой техническое средство, конструктивно предназначенное для хранения информации в электронно-цифровой форме, доступной для обработки с использованием средств вычислительной техники, в связи с чем необходимо обладать специальными навыками и познаниями для их правильного обнаружения, фиксации и изъятия.

§ 2. Тактика следственных действий, направленных на обнаружение, фиксацию и изъятие электронных носителей

Для начала необходимо рассмотреть криминалистические особенности совершения преступлений с использованием электронных носителей и средств ИТ.

К таким действиям, как правило, относятся:

1. Хищения машинных носителей информации;

2. Использование различных средств наблюдения за ЭВМ, в том числе, визуальных, оптических и акустических;

3. Считывание и расшифровка различных электромагнитных излучений ПК и обеспечивающих их работу систем;

4. Запечетление и съем информации в процессе ее обработки;

5. Изготовление бумажных дубликатов входных и выходных документов, копирование распечаток;

6. Использование оптических и акустических средств наблюдения за лицами, имеющими отношение к необходимой злоумышленнику информации, с помощью которой производится фиксирование и записывание их разговоров;

7. Использование удаленного доступа с помощью сети «Интернет»;

8. Вступление в прямой контакт с лицами, имеющими отношение к необходимой злоумышленнику информации, получение от них необходимых сведений.

Такие действия, как правило характеризуются локальными следовыми картинами, которые далее определяются тем, что место совершения преступления и непосредственный объект преступного посягательства находятся недалеко друг от друга.

Также можно перечислить преступные действия, осуществляемые с использованием компьютерных и коммуникационных устройств. Реализация самого несанкционированного доступа используется с помощью таких способов, как подбор пароля или использование чужой учетной записи,

преодоления программ защиты данных, а также иные меры обхода защиты компьютерной информации.

Первоначальным следственным действием при расследовании преступлений, как правило, является осмотр. Так статья 176 уголовно-процессуального кодекса РФ (далее – УПК РФ) закрепляет такие виды, как: осмотр места происшествия, местности, жилища и иного помещения, предметов и документов[1]. Наибольший интерес представляет осмотр места происшествия (например, по местонахождению компьютеров организации, попавшей в поле зрения правоохранительных органов в связи с совершением преступления), а также осмотр предметов и документов (например, электронных носителей и информации, содержащейся на них).

Под осмотром места происшествия понимается безотлагательное следственное действие, направленное на установление, фиксацию и исследование обстановки места обнаружения электронного носителя информации, преимущественно электронно-цифровых следов и иных сведений, могущих иметь значение для возбуждения уголовного дела и его расследования.

Под осмотром электронных носителей информации понимается действие следователя в рамках осмотра места происшествия, а равно самостоятельное следственное действие по обнаружению, фиксации и изъятию преимущественно электронно-цифровых следов преступления и описанию общих и индивидуальных признаков электронного носителя информации. При этом статья 177 УПК РФ определяет, что осмотр следов преступления и иных обнаруженных предметов может быть произведен как в ходе осмотра места

[1] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 22 ноября 2001 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 5 декабря 2001 г. // Собр. законодательства Рос. Федерации. – 2001. – № 52 (ч. 1), ст. 4291.

происшествия (по общему правилу), так и после него, если для такого осмотра требуется продолжительное время или осмотр на месте затруднен[1].

Также важно отметить, что проведение осмотра места происшествия в жилище без согласия проживающих в нем лиц возможно на основании судебного решения в порядке, установленном ч. 5 ст. 165 УПК РФ, а в исключительных случаях – без судебного решения, но с последующим уведомлением судьи и прокурора в течение 24 часов после проведения осмотра.

В теории криминалистики предусмотрено, что важно не только правильное и всестороннее проведение следственного действия, но и подготовка к его проведению, то есть все то, что подразумевается как деятельность следователя до выезда на место происшествия. Своевременность прибытия на место происшествия и качество самого осмотра напрямую зависят от подготовки к осмотру до выезда на него. Содержание этой деятельности обусловлено вопросами, которые должен решить следователь на анализируемом этапе. Применительно к осмотру места происшествия, как способу получения доказательственной информации с электронных носителей, постановка целей не имеет какой-либо специфики. Речь здесь идет о целях, решаемых путем проведения осмотра места происшествия любого преступления, в частности получение исходных данных для построения криминалистических версий и проверка имеющихся криминалистических версий, получение и проверка имеющихся доказательств.

Однако определение круга задач применительно к осмотру места происшествия как способу получения доказательственной информации с электронных носителей будет иметь свою специфику. Поскольку задачи конкретизируют деятельность следователя, их формулировка должна учитывать сферу приложения его усилий. В этой связи задачи могут быть изложены следующим образом: обнаружение, фиксация и изъятие преимущественно электронно-цифровых следов преступления (например,

[1] Добровлянина, О. В. Некоторые аспекты о процессуальном изъятии (копировании) электронных носителей информации // Пермский юридический альманах. 2019. № 2. С. 641.

файлов, содержащих информацию о заключаемых договорах, по делам о мошенничествах в финансовой сфере и пр.) и данные следы могут быть оставлены в результате совершения компьютерных преступлений (ст. 272-274 УК РФ), а также иных преступных посягательств например мошенничеств, действий по доступу к системам мобильной связи и пользованию ее ресурсами и т.д.

Компьютеры, которые подключены к локальной сети или имеют выход в сеть Интернет, как правило, имеют два адреса: логический адрес сетевого уровня (IP-адрес), а так же физический адрес сетевой интерфейсной карты (MAC-адрес), которые фиксируются при отправлении пакетов за пределы пространства локации. Данное действие позволяет определять ЭВМ, с которой было совершено неправомерное посягательство, найти типичные и виртуальные следы.

На практике лица, которые обладают IT-навыками, осознавая свои неправомерные действия, с целью запутать органы расследования могут специально прописывать отличающийся от их собственного IP-адрес, как правило, это делается при помощи испольвания VPN-сервисов. В такой ситуации необходимо определить MAC-адрес сетевой карты, непосредственный уникальный номер, изменение или уничтожение которого практически невозможно.

Так, А. обвинялся в совершении нарушения тайны переписки и иных сообщений, неправомерном доступе к охраняемой законом компьютерной информации, что повлекло блокирование и модификацию компьютерной информации. Расследованием установлено, что А., находясь по месту своего жительства, посредством подключения к ЭВМ, находящейся в его квартире соединенной к системе ЭВМ – серверу оператора связи, зашел в социальную сеть «Вконтакте» по электронному адресу и автоматически оказался на персональной странице потерпевшей, так как логин и пароль доступа были автоматически сохранены в кэш (cash) ПК, принадлежащего А. Далее А. осуществил незаконный доступ к личной переписке, содержащейся на

персональной странице потерпевшей в социальной сети и изменил регистрационные данные и наименование персональной страницы, тем самым блокировал доступ потерпевшей к ее персональной странице пользователя. В ходе судебного разбирательства, уголовное дело в отношение А. прекращено. А. назначен штраф в размере 30 000 рублей[1].

Фиксация обстановки преступлений, в результате совершения которых были оставлены электронно-цифровые следы. Сведения об обстановке позволяют судить как об условиях использования лицом, совершившим преступление, электронных носителей информации, так и об условиях обнаружения и изъятия этих носителей правоохранительными органами. Это, в свою очередь, может иметь значение для придания информации на электронных носителях качества доказательств (например, обнаружение электронного носителя с нелицензионной бухгалтерской программой в помещении финансового подразделения проверяемой организации может свидетельствовать об относимости электронного носителя к уголовному делу). Постановка названных выше задач создает возможность достижения целей осмотра. Также перед началом осмотра следователь должен учитывать возможное наличие средств защиты от несанкционированного доступа. Для защиты информации от несанкционированного доступа применяются организационные, технические, программные и криптографические методы.

Подготовка к осмотру места происшествия предполагает знание следователем факта применения на месте осмотра (объекте осмотра):

организационных методов защиты информации (порядок осуществления пропускного режима в осматриваемом месте, типичные места хранения электронных носителей информации, возможность проникновения посторонних лиц в осматриваемое место и др.);

[1] Уголовное дело № 1-193***/2017 // Архив Ленинского районного суда г. Уфы. Оп. 4. 156 л.

технических методов защиты информации (фильтры, межсетевые экраны, электронные ключи для блокировки, устройства аутентификации и др.), в том числе возможности подключения сторонних носителей информации;

программных методов защиты информации (блокировка экрана и клавиатуры, использование средств парольной защиты BIOS (базовой системы ввода-вывода) и др.)[1].

Также, готовясь к осмотру, следователю необходимо собрать данные о наличии на месте предполагаемого осмотра объектов, оборудования, аппаратуры, устройств, которые важны для расследования уголовного дела и раскрытия преступления, способствовавшие совершению преступления и являющихся непосредственным предметом преступления или же его орудием.

Время осмотра места происшествия определяет конкретную дату, планируемое время начала и окончания следственного действия. При этом необходимо стремиться к тому, чтобы осмотр места происшествия по уголовным делам, где фигурирует компьютерная информация, был проведен на первоначальном этапе. В противном случае появляется возможность повреждения или уничтожения информации, содержащейся на электронных носителях.

Говоря о времени осмотра места происшествия следователь должен учитывать возможность привлечения необходимых участников к осмотру. Одним из таких участников выступает специалист. Его привлечение позволит осуществить данное следственное действие более полно, что, соответственно, повлияет на продолжительность осмотра. Кроме этого, в отдельных ситуациях участие специалиста обязательно. Участие специалистов вносит значительный вклад поскольку в противном случае восприятие следователем информационного содержания электронного носителя в ходе осмотра будет

[1] Удовиченко В. С. Особенности изъятия информации с электронных носителей в досудебном производстве // Алтайский юридический вестник. 2021. № 2(34). С. 133.

невозможным. Кроме того, могут быть внесены изменения в первоначальный образ данных на электронном носителе[1].

Согласно действующему законодательству специалист может оказать содействие следователю в обнаружении, закреплении и изъятии предметов и документов, применении технических средств в исследовании материалов уголовного дела, для постановки вопросов эксперту (ч. 1 ст. 58 УПК РФ). Одновременно специалист может принимать участие в обсуждении вопросов, касающихся назначения и производства судебной экспертизы (ч. 1, 3 и 4 ст. 57, ч. 1 ст. 197 УПК РФ). Кроме этого, он может помочь следователю в установлении механизма работы оборудования, определения места обнаруженного электронного носителя информации в компьютерной технике. Привлекая специалиста следователю необходимо убедиться в его компетентности. Компетентность специалиста – оценочный термин, поэтому его наполнение зависит от конкретной ситуации. Компетентность специалиста может быть установлена посредством анализа уровня его образования (например, наличие диплома о высшем образовании по специальностям, связанным с компьютерным программированием), периода работы в сфере оборота компьютерной информации, места работы на момент привлечения к производству следственного действия (как правило, целесообразно привлекать лиц, работающих в специализированных государственных учреждениях).

Профиль нужного специалиста определяется в зависимости от целей и задач осмотра с учетом первоначальных данных о характере преступления.

Здесь же следует отметить роль эксперта-криминалиста, который может оказать помощь в обнаружении и сборе традиционных доказательств (например, слабо видимых следов пальцев рук на клавиатуре, компьютерной мыши и т.д.). Так, например, по делам связанным с экономическими преступлениями, полезным будет приглашение бухгалтера со знанием

[1] Телевицкая Ю. А. Об актуальности исследования особенностей выемки электронных носителей информации // Наука и образование: актуальные вопросы, достижения и инновации: сборник статей V Международной научно-практической конференции. Пенза: Наука и Просвещение, 2022. С. 76.

особенностей экономических информационных систем, который может оказать содействие специалисту в обнаружении информации в специальных бухгалтерских программах.

В целях удостоверения факта, хода, содержания и результатов осмотра приглашаются понятые. При этом не рекомендуется их приглашение из числа работников организации, в которой проводится осмотр. Это продиктовано их возможной причастностью к совершению компьютерного преступления.

В качестве участников могут быть приглашены представители администрации осматриваемой организации. Таковыми могут быть руководитель организации или его заместитель, а также представитель службы безопасности или охраны организации.

Помимо этого, в практике может возникнуть ситуация, диктующая приглашение владельца электронного носителя информации. Например, если следователем принято решение о проведении осмотра мобильного телефона (или прогнозируется его наличие на месте происшествия) и до проведения осмотра были получены сведения о том, что в мобильном телефоне имеются коды блокировок, то для проведения следственного осмотра можно пригласить владельца мобильного телефона. Данному лицу будет предложено самостоятельно разблокировать свой телефон или заранее уточнить данные коды у владельца мобильного телефона, получив согласие на разблокирование телефона без его участия.

Также существенно влияет на проведение осмотра места происшествия выбранная тактика его проведения. В ходе осмотра могут использоваться различные тактические приемы. Так, осмотр помещения целесообразно осуществлять, применяя тактический прием «от центра к периферии». В качестве «центра» отправной точки осмотра места происшествия, будет выступать конкретный компьютер, а если речь идет об осмотре конкретного компьютера – то компьютерная информация, имеющая значение для уголовного дела. Дальнейшее движение должно быть направлено в сторону периферийных и иных устройств.

Осмотр сервера (серверной станции) может проводиться одновременно несколькими осмотровыми группами (параллельный осмотр). В этом случае организуется параллельное обследование входящих в локальную сеть рабочих станций. В помещениях с компьютерами допустим последовательный осмотр, т.е. осмотр осуществляется от одного компьютера к другому. Очередность осмотра устанавливается в зависимости от степени связанности компьютера (наличие кабеля связи, обеспечение условия прямой видимости для оборудования, оснащенного инфракрасным портом передачи информации) или удаленности его расположения от основного информационного узла (например, от сервера). Прибыв на место происшествия, следователь должен выполнить ряд незамедлительных действий:

1. Организовать блокировку доступа персонала, работающего в месте осмотра, ко всем компьютерам сети, серверу и иным средствам компьютерной техники (для недопущения изменения или повреждения информации во время осмотра);

2. Удалить всех посторонних (лиц, не участвующих в осмотре), по возможности разместив их в помещении, исключающем использование любых средств связи;

3. Выставить охрану у средств компьютерной техники и электрических распределительных щитов, пультов (при большом количестве мест разместить сотрудников, обеспечивающих охрану, в точках, позволяющих просматривать данные места);

4. При наличии локальной компьютерной сети, связывающей ПК, отсоединить удаленный доступ к системе извне, например, отключить шнур модема от телефонного кабеля; блокировать выход сервера во внешнюю (глобальную) сеть;

5. Установить, не запущена ли на компьютере программа уничтожения информации (при запуске данной программы с помощью специалиста предпринять действия по ее приостановлению или отмене, в том числе отключить ПК от питания).

Как уже было отмечено ранее, осмотр индивидуальных объектов (электронных носителей) может быть проведен как в рамках осмотра места происшествия, так и в границах самостоятельного следственного действия осмотра предметов.

Осмотр предметов, являющихся электронными носителями информации, необходим для того, чтобы зафиксировать внешние признаки данного носителя, а равно воспринять информацию в электронной форме с учетом того, что экспертами отмечается, что обнаружение информации нередко возможно без проведения экспертизы. В данном случае представляют интерес классические электронные носители (жесткий диск, компакт-диск и т.д.), а также отдельные современные объекты, содержащие данные носители (аппарат сотовой связи и пластиковая карта их осмотр продиктован необходимостью расследования преступлений, где орудием совершения преступлений или предметом посягательства являются данные объекты). При этом следует принимать во внимание возможность обнаружения типовых следов, названных ранее применительно к осмотру места происшествия.

Следовательно при осмотре электронных носителей информации необходимо не повредить сами электронные носители, а также информацию, содержащуюся на них, для этого может быть осуществлено резервное копирование данных.

При осмотре мобильного телефона следует фиксировать результаты его описания с применением терминов, которые определены нормативными актами или разработчиками средств связи, исключая бытовые выражения. Осмотр средства мобильной связи начинается с изучения упаковки. Упаковывают мобильный телефон обычно в коробку (бумажную, пластмассовую, металлическую), в бумажный конверт, в полиэтиленовый пакет и др. В протоколе осмотра указываются материал, из которого изготовлена упаковка, форма, размеры, цвет, наличие надписей, их содержание и расположение, способ нанесения, целостность, способ опечатывания упаковки.

Также при расследовании преступлений информация, используемая в доказывании, может быть получена при проведении обыска и выемки электронных носителей. Под обыском понимается проводимое следователем в установленном законом порядке самостоятельное следственное действие, направленное на отыскание, обнаружение и изъятие электронных носителей информации. Под выемкой понимается проводимое следователем в установленном законом порядке самостоятельное следственное действие, направленное на обнаружение и изъятие электронных носителей информации, могущих иметь значение для уголовного дела.

В отличие от выемки электронных носителей на практике именно обыск получил наибольшее распространение. Ведь выемка подразумевает под собой точное наличие сведений о нахождении искомого у подозреваемого, в то время, как обыск позволяет расширить круг поиска и получения необходимого для расследования уголовного дела.

Основу подготовки к данным следственным действиям составляет анализ следователем имеющихся материалов и сведений, полученных из проведенных ранее следственных действия (к примеру, осмотр и допрос). Исследование материалов уголовного дела позволяет следователю собрать сведения, полезные для производства обыска в тактическом плане.

Следовательно целесообразно изучить имеющиеся доказательства. Например, показания свидетеля могут содержать сведения о личности обыскиваемого лица, протокол осмотра места происшествия может содержать описание обстановки, в которой планируется проведение поисковых действий; иные документы могут содержать информацию о возможности нахождения в месте обыска определенных объектов (справка от организации-провайдера о подключении к телефону авторизации сервера с использованием устройства «модем» с телефонного номера подозреваемого может свидетельствовать о нахождении в месте проживания подозреваемого указанного устройства). Кроме этого, целесообразно изучить результаты оперативно-разыскной

деятельности. Данные материалы могут содержать сведения, характеризующие все элементы подготовки к производству обыска[1].

Принимая во внимание изложенное, целесообразно дополнить ч. 2 ст. 84 УПК РФ «Иные документы» новыми положениями, содержащими порядок приобщения к уголовному делу и хранения электронных носителей информации, которые по содержанию являются не вещественными доказательствами, а иными документами.

Так, исходя из вышеизложенного, можно сделать вывод:

1. Имеющиеся недостатки в уголовно-процессуальной регламентации работы с доказательствами на цифровом носителе сами по себе не являются основанием для введения в уголовно-процессуальный закон новой процессуальной формы цифровых доказательств, поскольку их получение возможно в рамках существующих процессуальных форм;

2. В отличие от электронного носителя информации - вещественного доказательства информация, содержащаяся в ином документе в электронной форме, не связана с конкретным материальным объектом-носителем и не обладает признаками, предусмотренными ст. 81 УПК РФ;

3. Существует необходимость процессуальной регламентации порядка приобщения к уголовному делу и хранения электронных носителей информации, содержащих доказательства в форме иных документов.

Так исходя из вышесказанного следует, что для объекивного и всестороннего расследования IT-преступлений необходимо тесное взаимодействие органов предварительного расследования со специалистами в сфере компьютерных технологий.

[1] Гребенюк О. А., Жидков Д. Н., Макарова Е. Н. Тактика обнаружения, изъятия и осмотра средств электронных носителей информации и их подготовки для назначения судебных экспертиз: учебно-практическое пособие. Санкт-Петербург: Санкт-Петербургский университет МВД России, 2020. С. 48.

§ 3. Организация взаимодействия органов предварительного расследования со специалистами в сфере компьютерных технологий

Деятельность по раскрытию, расследованию и предупреждению преступлений требует эффективного использования лицами, производящими расследование, специальных знаний специалистов и экспертов. В связи с этим вопросы организации взаимодействия между ними очень актуальны.

Преступления в сфере компьютерных технологий отличаются большой латентностью и в некоторых случаях невозможностью установления лиц, их совершивших. По мнению Н. Н. Федотова «успех в раскрытии компьютерных преступлений зависит от грамотной работы следователя и специалиста»[1].

Чтобы эффективно использовать специальные знания в сфере компьютерных технологий следователь должен четко представлять реальные возможности использования знаний привлекаемых специалистов, владеть информацией о такого рода специалистах и иметь возможность установить с ними контакт.

Следователь должен выяснить вид техники, тип операционной системы и т.п., привлечь эксперта или специалиста, обладающего специальными знаниями в области компьютерных технологий соответствующего профиля в зависимости от сложившейся следственной ситуации, определить цели, задачи производства определенного следственного действия, подготовить необходимое компьютерное оборудование, программное обеспечение.

Организация взаимодействия следователя с экспертами и специалистами в ходе выявления, раскрытия и расследования преступлений в сфере компьютерных технологий, имеет определенные проблемы в связи с трудностями межведомственного взаимодействия.

Взаимодействие следователя с экспертно-криминалистическими подразделениями других ведомств, независимыми экспертными учреждениями,

---

[1] Федотов Н. Н. Форензика – компьютерная криминалистика. М.: Юридический Мир, 2017. С. 109.

когда отсутствует собственное экспертно-криминалистическое подразделение или специалист соответствующего профиля в штате носит формализованный характер, что вызывает определенные сложности на практике.

Экспертная-криминалистическая деятельность регламентируется Федеральным законом «О государственной судебно-экспертной деятельности в Российской Федерации»[1] и ведомственными нормативными актами (приказы МВД России, МЧС России, Министерства юстиции России и др.), например, приказом МВД России от 29 июня 2005 г. № 511 «Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации» и пр.

В ходе проведения следственных действий следователь не может выполнить самостоятельно те или иные мероприятия, связанные с обнаружением, поиском, фиксацией либо изъятием следов с объектов компьютерной техники, либо с помощью ее применения. Отмеченное обстоятельство не позволяет применять обширный круг способностей специалиста и эксперта на каждой стадии приготовления к следственному действию[2]. Эксперт или специалист при подготовке к следственному действию может оказать содействие следователю:

1. В выборе круга действий, в пределах которых будет проводиться следственное действие (осмотр места происшествия, проверка показаний на месте, обыск и т.д.);

2. Определении тактики проведения следственного действия (осмотр места происшествия, следственный эксперимент, обыск и т.д.);

3. Подборе технических средств, необходимых для проведения следственного действия (обыск, выемка, проверка показаний на месте и т.д.);

---

[1] О государственной судебно-экспертной деятельности в Российской Федерации: федер. закон Рос. Федерации от 31 мая 2001 г. № 73-ФЗ принят Гос. Думой Федер. Собр. Рос. Федерации 5 апреля 2001 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 16 мая 2001 г. // Собр. законодательств Рос. Федерации. – 2001. – № 23, ст. 2291.

[2] Баев О. Я. Криминалистика: учебное пособие. М.: Юстиция, 2017. С. 258.

4. В выборе способа установления, изъятия и фиксации следов преступления (осмотр места происшествия, проверка показаний на месте и т.д.);

5. В поиске предметов, заменяющих специально предназначенные и необходимые для качественного проведения следственного действия (следственный эксперимент, проверка показаний на месте);

6. В установлении границ в пределах объекта, подлежащего поиску, обнаружению и изъятию (выемка, обыск, осмотр места происшествия), и т.д.

На практике следователи в основном используют процессуальный порядок проведения следственных действий во время работы со специалистом, экспертом, игнорируя непроцессуальную [1].

К непроцессуальной форме взаимодействия следователя и специалиста, в том числе при расследовании преступлений в сфере компьютерных технологий, относятся следующие виды:

осуществление предварительного исследования объекта;

консультативная помощь между специалистом и экспертом;

использование криминалистических учетов;

исполнение поручения технического характера;

принятие участия в оперативно-розыскных мероприятиях;

выработка совместных мероприятий в целях эффективного использования определенных методов и средств борьбы с преступностью;

анализ уголовных дел в целях планирования и принятия мер по устранению ранее выявленных недостатков;

оказание содействия при совместных выездах в составе следственно-оперативных групп на место совершения резонансного преступления[2].

---

[1] Гавло В. К., Поляков В. В. Некоторые особенности расследования преступлений, связанных с неправомерным доступом к компьютерной информации // Известия Алтайского государственного университета. 2016. № 2. С. 47.

[2] Потапов С. А. Совершенствование расследования и раскрытия преступлений в сфере компьютерной информации // Социально-экономические явления и процессы. 2016. № 10. С. 95.

На основе вышеизложенного можно сделать вывод, что недостатками взаимодействия следователя и специалиста, в том числе при расследовании преступлений в сфере компьютерных технологий, являются неупорядоченность действий, регулируемых нормами процессуального законодательства и конкретными ведомственными нормативными актами, слабая техническая обеспеченность территориальных органов внутренних дел, низкий уровень профессиональной подготовки сотрудников, безразличие субъектов взаимодействия, согласованность законодательной базы, норм взаимодействия и прочие минусы в координационной работе субъектов, недостаточная оценка эффективности взаимодействия, неосведомленность и не знание эмоционально-психологических аспектов взаимодействия и т.п.[1].

Для устранения перечисленных недостатков взаимодействия следователя и эксперта (специалиста) необходимо законодательное урегулирование взаимодействия, улучшение качества технической оснащенности экспертных учреждений, дополнительная профессиональная подготовка субъектов взаимодействия и т.д.

Таким образом, учитывая сложность и многогранность использования специальных знаний в области компьютерных технологий при проведении любых следственных действий, следователю нужно индивидуально подбирать специалиста для каждого отдельного действия и не забывать удостовериться в его компетентности. При проверке компетенции следует обращать внимание не только на наличие у привлекаемого технического специалиста диплома о высшем специальном образовании, но и на его специализацию, опыт и другие факты, на основании которых можно судить о его квалификации. Так же необходимо понимать цели и задачи судебных экспертиз и грамотно использовать их результаты при выявлении и расслеовании преступлений.

[1] Криминалистика: учебник для бакалавров. 2-е изд., испр. и доп. / Л. Я. Драпкина. М.,: Издательство Юрайт, 2023. С. 243-244.

ГЛАВА 2. СУДЕБНЫЕ ЭКСПЕРТИЗЫ И ИСПОЛЬЗОВАНИЕ ИХ РЕЗУЛЬТАТОВ ПРИ ВЫЯВЛЕНИИ И РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

§ 1. Предмет, объекты и задачи судебных экспертиз, их назначение при расследовании преступлений

Особенностью преступлений с использованием электронных носителей является то, что для их успешного раскрытия и расследования необходимо знание их специфики. Так, например, при расследовании уголовного дела кроме традиционных экспертиз также требуется проведение таких экспертиз, как: компьютерно-техническая, информационно-технологическая и информационно-техническая. Объединяет эти виды судебных экспертиз компьютерная информация, исследуемая, однако, с разных сторон – технологической либо технической. Различаются они и по непосредственным объектам исследования.

Объектом информационно-технологической экспертизы является установленный порядок обработки информации, осуществляемый по заданным алгоритмам, или информационная технология, основанная на применении современной информационно-вычислительной техники, средств связи и телекоммуникаций, составляющих основу информатизации общества [1].

Непосредственным предметом информационно-технологической экспертизы могут быть:

проектная документация на разработку и эксплуатацию компьютерных систем и сетей, отражающая процессы сбора, обработки, накопления, хранения, поиска и распространения информации;

---

[1] Табункина Т.А. Проблемы получения уголовно-процессуальных доказательств в современных условий информатизации общества на досудебных стадиях расследования по уголовному делу // Государство и право в изменяющимся мире: правовая система в условиях информатизации общества. Материалы IV научно-практической конференции с международным участием. 2019. С. 273.

документированная информация (документ), то есть зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать (отдельные документы и массивы документов в информационных системах), в том числе конфиденциальная информация;

материалы сертификации информационных систем, технологий и средств их обеспечения и лицензирования деятельности по формированию и использованию информационных ресурсов;

приказы и распоряжения администрации, инструкции, протоколы, договоры, положения, уставы и методики по эксплуатации компьютерных систем и сетей, отражающие порядок формирования информационных массивов и доступа к ним (важнейшими из этих предметов исследования могут быть должностные инструкции сотрудников соответствующих информационных подразделений);

схемы движения информации от источников к потребителю с указанием пунктов ее сбора, контроля, накопления, обработки и использования;

табель распределения выходных данных (перечень пользователей с указанием периодичности, объема и сроков поступления информации), а также другие документы, позволяющие наиболее полно раскрыть сущность информационной технологии данной компьютерной системы или сети (они обычно прилагаются к техническому заданию на их разработку);

входные и выходные документы, установленные для данной автоматизированной информационной системы;

словари, тезаурусы и классификаторы;

иные эксплуатационные и сопроводительные документы (особое значение для расследования компьютерных преступлений имеют журналы и другие виды учета работы операторов, регистрации сбойных ситуаций и обращений в компьютерную систему или сеть)[1].

[1] Гавло В. К., Поляков В. В. Некоторые особенности расследования преступлений, связанных с неправомерным доступом к компьютерной информации // Известия Алтайского государственного университета. 2016. № 2. С. 49.

Несомненно, что все указанные документы должны быть изъяты своевременно и с соблюдением установленных законом норм.

Информационно-технологическая экспертиза назначается в тех случаях, когда для возникающих в ходе расследования вопросов требуются специальные познания в технологии информационных процессов.

Возможности этой экспертизы достаточно широки. С ее помощью можно определить: соответствие существующего технологического процесса компьютерной обработки информации проектной и эксплуатационной документации на конкретную информационную систему либо сеть, конкретные отклонения от установленной информационной технологии, а также непосредственных исполнителей, допустивших нарушение установленной информационной технологии, надежность организационно-технологических мер защиты компьютерной информации, вредные последствия, наступившие из-за неправомерного нарушения установленной технологии компьютерной обработки информации, обстоятельства, способствовавшие преступному нарушению технологии электронной обработки информации.

При изучении заключения экспертизы, следователь должен выявить:

отношения сбора, хранения, переработки и отправки информации;

какие нарушения произведены от обычного процесса;

кто имеет право или кто управлял действием в конкретный период;

имеются ли меры защиты компьютерной безопасности, установленные производителем;

что влечет нарушение вышеуказанных правил;

какие действия необходимо совершать для недопущения нарушений.

Предметом информационно-технической экспертизы является установленный порядок работы технических средств и поддержание информационной безопасности при помощи различных систем и инструментов, к которым относятся: технические ресурсы обработки данных, электронные

носители информации (различные накопители на жестких дисках и т.д.) и программные ресурсы, информационные базы данных[1].

Таким образом, можно сделать вывод о том, что при назначении информационно-технической экспертизы в процессе расследования преступлений в сфере компьютерной информации, встает вопрос о специфике назначения исследования в области технической части компьютерных систем и сетей.

К основным задачам информационно-технической экспертизы относятся восстановление испорченных информационных данных, единичных файлов на персональном устройстве или месте хранения, поиск проблем, повлиявших на нарушение первоначальной системы, поиск возможного вируса, используемого злоумышленником для получения доступа к информационной системе или локальной сети, установление программных средств, обеспечивающих защиту компьютерного средства от незаконного проникновения в систему.

Рассматривая результат данной экспертизы, следователь должен выяснить, установлено ли материально-техническое состояние компьютерного устройства, способность выполнения определенных действий, свойства неразрешенных переменных данных, записанных на дополнительные источники информации, способность установки и работы дополнительного программного обеспечения без разрешенного доступа пользователя, антивирусные и прочие программные устройства, предназначенные для защиты компьютера от вредоносных программ, процесс заражения компьютера вредоносным вирусом, описание вируса, заразившего компьютерную программу, место проникновения и способ установки вируса, вред причиненный компьютерным вирусом.

[1] Гребенюк О. А., Жидков Д. Н., Макарова Е. Н. Тактика обнаружения, изъятия и осмотра средств электронных носителей информации и их подготовки для назначения судебных экспертиз: учебно-практическое пособие. Санкт-Петербург: Санкт-Петербургский университет МВД России, 2020. С. 50.

Данные вопросы не носят обязательный и исчерпывающий характер. В зависимости от конкретной ситуации могут быть заданы новые и конкретные вопросы по каждому делу.

Встречаются и другие виды информационно-технической экспертизы:

экспертиза электронно-цифровой подписи;

экспертиза процесса разработки и использования программного обеспечения;

компьютерно-сетевая экспертиза,

экспертиза обстоятельств создания и использования файлов и баз данных и др[1].

На основе проведенного анализа можно сделать ряд выводов. Специфика преступлений в сфере компьютерной информации обуславливает необходимость проведения по уголовным делам данной категории информационно-технологической и информационно-технической экспертиз. Объектом информационно-технологической экспертизы является установленный порядок обработки информации, осуществляемый по заданным алгоритмам или информационная технология, основанная на применении современной информационно-вычислительной техники, средств связи и телекоммуникаций, составляющих основу информатизации общества. Непосредственными предметами информационно-технологической экспертизы могут быть различного рода документы: проектная документация, документированная информация, материалы сертификации информационных систем и т.п.

Объектом информационно-технической экспертизы является техническое обеспечение информационной безопасности компьютерных систем и сетей. Предметами информационно-технической экспертизы являются инструменты, с помощью которых осуществляется доступ к информационным технологиям: технические средства обработки информации, машинные носители

[1] Козлов В. Е. Теория и практика борьбы с компьютерной преступностью. М.: Телеком. 2016. С. 406.

информации и машинограммы, создаваемые средствами вычислительной техники, программные средства и базы данных.

Круг вопросов, задаваемых по данным видам преступлений не является исчерпывающим и, исходя из ситуации, может изменяться в зависимости от расследуемого преступления.

Результаты экспертного исследования, совместно с другими документами, являющимися доказательствами, полученными в ходе предварительного следствия (протоколы обыска, осмотра места происшествия, протоколы осмотра предметов и документов, показания свидетелей и др.) оцениваются следователем на предмет их достоверности, объективности и достаточности для доказывания действий лица (лиц), совершивших преступления в сфере компьютерной информации. В противном случае уголовное дело в отношение обвиняемого(ых) может быть прекращено в связи с недоказанностью преступления в сфере компьютерной информации. Так, по делу Ю. обвинялась в совершении преступлений предусмотренных: ст.ст. 158, 163, 159, 183, ч. 2 ст. 272 УК РФ[1]. В виду не достаточности доказательств, собранных в ходе предварительного следствия, в ходе рассмотрения дела в суде государственный обвинитель отказался от поддержания обвинения в отношение Ю. по ч. 2 ст. 272 УК РФ, что свидетельствует о не достаточности доказательств вины Ю. по предъявленному обвинению.

Можно сделать вывод, что определение предмета судебной экспертизы в общем виде конкретизируется через определение предметов судебных экспертиз различных родов и видов. Так, предметом судебной компьютерно-технической экспертизы являются факты и обстоятельства, устанавливаемые на основе исследования закономерностей разработки и эксплуатации компьютерных средств, обеспечивающих реализацию информационных процессов, что зафиксированы в материалах уголовного, гражданского дела или дела об административном правонарушении.

[1] Уголовное дело № 1-183***/2018 // Архив Белебеевского городского суда РБ. Оп. 1. 214 л.

Экспертные задачи неразрывно связаны с вопросами, выносимыми на разрешение судебной экспертизы. Общие и типичные задачи предоставляют собой научное обобщение всевозможных вопросов по данному роду или виду экспертиз. Конкретные задачи судебной экспертизы реализуются путем постановки определенных вопросов эксперту в зависимости от имеющихся объектов и материалов гражданского или уголовного дела, дела об административном правонарушении, однако у компьютерно-технических экспертиз имеются свои особенности, которые необходимо рассмотреть более детально.

§ 2. Особенности назначения и производства компьютерно-технических экспертиз

Компьютерно-техническая экспертиза является самостоятельным родом судебных экспертиз, которая проводится в «целях определения статуса объекта как компьютерного средства, выявления и изучения его следовой картины в расследуемом преступлении, получения доступа к информации на носителях данных с последующим всесторонним ее исследованием»[1].

Согласно Приказу Министерства юстиции Российской Федерации от 27 декабря 2012 г. № 237 «Об утверждении Перечня родов (видов) судебных экспертиз, выполняемых в федеральных бюджетных судебно-экспертных учреждениях Минюста России, и Перечня экспертных специальностей, по которым представляется право самостоятельного производства судебных экспертиз в федеральных бюджетных судебно-экспертных учреждениях Минюста России», в рамках компьютерно-технической экспертизы происходит исследование информационных компьютерных средств. Исходя из такого определения можно сделать вывод о том, что круг вопросов, решаемых компьютерно-технической экспертизой не является исчерпывающим. В

[1] Потапов С. А. Совершенствование расследования и раскрытия преступлений в сфере компьютерной информации // Социально-экономические явления и процессы. 2016. № 10. С. 94.

современной научной среде круг вопросов, относящихся к компьютерно-технической экспертизе, значительно шире.

В состав компьютерно-технической экспертизы входят четыре типа экспертиз:

1. Аппаратно-компьютерная;

2. Программно-компьютерная;

3. Информационно-компьютерная (экспертиза данных);

4. Компьютерно-сетевая[1].

Выделение подобного числа и разновидностей экспертиз обуславливается качественными признаками предметов, предоставляемых на экспертизу и проблемами, решаемыми в рамках экспертизы.

Статьей 195 УПК РФ установлен порядок назначения судебной экспертизы, согласно которому следователь, признав необходимым назначение судебной экспертизы, выносит об этом постановление.

Судебная экспертиза производится государственными судебными экспертами и иными экспертами из числа лиц, обладающих специальными знаниями. Перед направлением экспертизы следователь обязан ознакомить с постановлением о назначении подозреваемого, обвиняемого, его защитника, потерпевшего, а также его представителя и разъяснить им права, все это фиксируется в протоколе ознакомления, которое предусмотрено уголовно-процессуальным законодательством.

Требованиями к экспертному заключению являются полнота (обозначение абсолютно всех свойств; исследование всех вопросов эксперту; использование всех возможных методик, обеспечивающих полноту всего исследования), объективность (объективность подхода к поставленным задачам), всесторонность (изучение объекта исследования со всех позиций), достоверность, допустимость (возможность использования результатов заключения в суде как доказательства).

---

[1] Васюков В. Ф. Особенности назначения судебных компьютерных экспертиз при расследовании преступлений в сфере информационно-коммуникационных технологий // Судебная экспертиза. 2016. № 2(46). С. 139.

Вышеперечисленный список требований к экспертному заключению определяет конкретные требования к экспертной методике проведения той или иной экспертизы. Экспертная методика должна отвечать всем требованиям, установленным законодательством относительно всестороннего исследования объекта и обеспечивать достоверность экспертного заключения, отвечать требованиям законности, быть безопасной, эффективной и полезной для расследования конкретного вида преступления[1].

Следователь вправе присутствовать при производстве судебной экспертизы, получать разъяснения эксперта по поводу проводимых им действий. Факт присутствия следователя при производстве экспертизы фиксируется в заключении эксперта.

После проведения экспертизы, эксперт согласно ст. 204 УПК РФ самостоятельно составляет заключение. В целом, с точки зрения процессуального законодательства, назначение компьютерно-технической экспертизы не отличается от назначения других видов экспертиз. В некоторых случаях лица подготовленные ответить на вышеуказанные вопросы не обладают знаниями процессуального права (если это не сотрудники ведомственных экспертных подразделений).

Рассмотрим подробнее вопросы, которые ставятся перед экспертом при осуществлении различных судебных компьютерно-технических экспертиз.

Так, аппаратно-компьютерная экспертиза направлена на решение вопросов, связанных с исследованием технической (аппаратной) части компьютерных средств, как правило, эти вопросы носят диагностический характер. В ходе судебной аппаратно-компьютерной экспертизы проводится исследование компьютеров, как стационарных так и переносных, локальных сетей, отдаленных приборов, сетевых аппаратных устройств, сотовых телефонов, комплектующие любого типа, используемые в компьютере, различных записывающих приборов и устройств памяти.

---

[1] Пропастин С. В. Назначение компьютерной экспертизы по делам об интернет-преступлениях // Уголовный процесс. 2016. № 6 (138). С. 39.

Эксперту в процессе выполнения аппаратно-компьюторной экспертизы необходимо ответить, например, на следующие вопросы:

1. Относится ли представленное устройство к компьютерному средству?

2. К какому типу оно относится?

3. Каковы тактико-технические характеристики устройства?

4. Для каких целей служит представленное устройство?

5. Какова роль данного аппаратного средства в компьютерной системе?

6. Возможно ли использовать данное устройство для решения определенной задачи?

7. Какие начальные характеристики аппаратного устройства?

8. Каким образом были внесены функциональные изменения на представленное устройство?

9. Функционирует ли представленное аппаратное средство?

10. Имеются ли отклонения от типовых характеристик прибора?

11. Имеются ли царапины, следы уничтожения или дефекты повреждения на устройстве?

12. В каком режиме должно функционировать представленное средство?

13. Является ли выявленная неисправность заводским браком либо следствием нарушения эксплуатации?

14. Является ли представленное аппаратное средство носителем информации?

15. Какое запоминающее устройство предназначено для работы с данным накопителем информации?

16. Каковы параметры (форм-фактор, емкость, среднее время доступа к данным, скорость передачи данных и др.) носителя информации?

17. Доступен ли для чтения представленный носитель информации?

18. Каковы причины отсутствия доступа к носителю информации?

Программно-компьютерная экспертиза ориентирована на решение вопросов, связанных с исследованием программного обеспечения. В ходе программно-компьютерной экспертизы изучению подвергаются операционная

система, утилиты всех видов, программы разработки и отладки, системная информация, основные приложения общего назначения и т.д.

Компьютерно-сетевая экспертиза является одним из видов компьютерных экспертиз, ее проведение направлено на выявление неправомерных действий при помощи устройства непосредственно в сетевой работе пользователя[1].

Компьютерно-сетевая экспертиза используется для определения типа носителя (устройства), характеристики представленного носителя (устройства), технического состояния, установления механических или иных повреждений, обнаружения скрытых файлов, возможности копирования информации с устройства, параметров и возможностей установленных программ[2].

На практике перед экспертами при назначении компьютерно-сетевой экспертизы ставятся, например, следующие вопросы:

1. Имеются ли признаки работы данного устройства в сети Интернет?

2. Через какое устройство был осуществлен выход в локальную сеть?

3. Имеется ли информация относительно средств платежей при помощи данного устройства?

4. Была ли осуществлена отправка, какой либо информации непосредственно через локальную сеть или сеть Интернет?

Основным видом компьютерно-технических экспертиз, позволяющим создать достаточное количество доказательственной базы при помощи диагностических и идентификационных вопросов, является информационно-компьютерная экспертиза. На нее возложены задачи, связанные с поиском, обнаружением, оценкой информации, содержащейся в компьютерной системе.

---

[1] Елфимов П. В. Особенности проведения и назначения комплексных судебных экспертиз // Вестник Уральского юридического института МВД России. 2017. № 2. С. 47.

[2] Демин К. Е. О дидактических основах и стандартизации судебной компьютерно-технической экспертизы, проводимой в государственных экспертных органах Российской Федерации // Теория и практика фундаментальных и прикладных исследований в сфере судебно-экспертной деятельности и ДНК-регистрации населения Российской Федерации: Всероссийская научно-практическая конференция с международным участием. 2021. С. 52.

Для проведения эффективной оценки перед экспертами ставятся следующие вопросы:

1. В каком формате имеются информационные данные?

2. Какими характеристиками обладает данная информация?

3. Какими сведениями обладает информация?

4. К какому типу принадлежат выявленные данные – текстовые, графические, электронная таблица, мультимедиа и др.?

5. Как образом осуществлен доступ к данным на носителе информации?

6. Какие характеристики параметров имеет система для защиты данных?

7. Имеются ли следы незаконного проникновения в систему?

8. В каком формате сохранены защищаемые данные[1]?

Проанализировав материалы уголовных дел, можно сделать вывод о том, что расследование по делам связанным с компьютерной информацией является весьма сложным, отчасти это связано с тем, что проведение тех или иных следственных действий следователем самостоятельно имеет определенную сложность, так как последние не обладают специальными знаниями. Не все государственные экспертные учреждения имеют специалистов, обладающих допуском для проведения компьютерно-технических экспертиз в данной области. Имеются проблемы и при назначении компьютерно-технических экспертиз, в связи с тем, что следователь зачастую указывает вопросы, явно выходящие за пределы компетенции эксперта.

Судебная компьютерно-техническая экспертиза производится государственными судебными экспертами и иными специалистами из числа лиц, обладающих специальными знаниями в области компьютерных технологий.

В целом, с точки зрения процессуального законодательства, назначение компьютерно-технической экспертизы не отличается от назначения других видов судебных экспертиз. Однако, привлекаемые сведущие лица обычно не

[1] Васюков В. Ф. Особенности назначения судебных компьютерных экспертиз при расследовании преступлений в сфере информационно-коммуникационных технологий // Судебная экспертиза. 2016. № 2(46). С. 141.

обладают правовыми знаниями, что нередко выступает источником процессуальных нарушений. В связи с этим, следователю необходимо заострить внимание на подробном разъяснении прав и обязанностей экспертам.

Но не только компьютерно-технические экспертизы помогают в раскрытие IT-преступлений и выявление следовой картины преступления, но и ряд иных судебных экспертиз, рассмотрим их в дальнейшем.

§ 3. Особенности назначения и производства иных видов экспертиз

В связи со сложностью уголовных дел в сфере компьютерной информации часто возникает необходимость производства комплексных судебных экспертиз. Комплексная экспертиза − это вид экспертизы, в которой принимают участие несколько экспертов различных специальностей.

Производство комплексных экспертиз приобретает особую актуальность и объясняется тем, что возрастает «профессионализм» преступников, их более тщательная подготовка к совершению преступления, но самое главное − это эффективность такой экспертизы, которая связана с большой возможностью совокупного применения знаний из различных отраслей науки и техники [1].

Для проведения экспертных исследований в сфере компьютерной информации, носящих комплексный характер, приглашаются высококвалифицированные специалисты в области информатики, вычислительной техники и программирования, а также традиционных видов криминалистической экспертизы, экономической, финансовой, бухгалтерской и товароведческой экспертиз.

Например, идентификационная задача может быть решена с помощью комплексной компьютерно-технической и судебно-автороведческой экспертизы, позволяющей проверить, не написана ли данная компьютерная программа конкретным лицом.

---

[1] Елфимов П. В. Особенности проведения и назначения комплексных судебных экспертиз // Вестник Уральского юридического института МВД России. 2017. № 2. С. 50.

В особенно непростых ситуациях, где необходимо привлечь судебного бухгалтера к информации, которая невозможна для доступа или закрыта, то необходимо назначить комплексную судебно-бухгалтерскую и компьютерно-техническую экспертизу. Изначально необходимо произвести компьютерно-техническую экспертизу для доступа к необходимой информации, затем производится судебно-бухгалтерская экспертиза для последующего исследования информационных данных обнаруженной компьютерно-технической экспертизой.

Объектом комплексных компьютерно-технических и судебно-бухгалтерских экспертиз являются сведения о хозяйственных операциях, находящиеся в компьютерах и их сетях, зафиксированные на носителях информации и обладающие свойствами, изучение и оценка которых требует привлечения интегративных знаний специалистов в области компьютерной техники и в области судебной бухгалтерии, авторские и модифицированные типовые программы, обрабатывающие информацию о хозяйственных операциях, правила работы которых специалист-бухгалтер не может понять без помощи программистов, зашифрованная соответствующая информация, процедуры расшифровки которой имеют значение не только для установления ее функционального значения, но и для оценки ее содержания, отдельные фрагменты данных, установить относимость которых к бухгалтерской информации возможно только совместными усилиями экспертов двух специалистов.

Следует отметить, что эксперт компьютерно-технической экспертизы не решает самостоятельные задачи и в большинстве случаев участвует в формировании только промежуточных выводов, в качестве предмета оценки здесь выступает только информация о хозяйственных операциях. Каждый из экспертов вправе подписывать только часть экспертного заключения, отражающего результата его работы.

В ходе комплексной судебно-бухгалтерской экспертизы и экспертизы программного обеспечения, устанавливают:

1. Возможность несанкционированного скрытого доступа к программному обеспечению с целью внесения изменений, влияющих на результаты расчетов и отчетность, механизм совершения таких изменений, их характер и последствия;

2. Кто из работников учреждения, обслуживающих и эксплуатирующих эти средства, имеет указанные выше возможности;

3. Размер причиненного материального ущерба;

4. Какие нарушения правил, регламентирующих ведение бухгалтерского учета и отчетности, могли способствовать образованию ущерба;

5. Какая операционная система использована в конкретном компьютере;

6. Не вносились ли в программу данного системного продукта какие-либо коррективы, изменяющие выполнение операций (какие именно);

7. Возможно ли получение доступа к конфиденциальной финансовой информации, имеющейся в данной сети, и каким образом может быть осуществлен этот доступ.

На сегодняшний день остаются неурегулированными, нечетко прописанными в инструкциях такие аспекты, как порядок направления объектов экспертизы в судебно-экспертные учреждения различных ведомств и критерии отбора ведущего из них, порядок заявления ходатайств со стороны ведущего судебно-экспертного учреждения и его действий в случае отказа в удовлетворении ходатайств и др.

Вопрос организации проведения комплексной судебной экспертизы непосредственно связано с законодательной регламентацией в целом. Так, проведение комплексной судебной экспертизы закреплено в ст. 201 УПК РФ, где указано, что в заключении экспертов, участвующих в производстве комплексной судебной экспертизы, указывается, какие исследования и в каком объеме провел каждый эксперт, какие факты он установил и к каким выводам пришел. Каждый эксперт, участвовавший в производстве комплексной судебной экспертизы, подписывает ту часть заключения, которая содержит описание проведенных им исследований, и несет за нее ответственность.

При этом законодательно не регламентированы условия и порядок организации и производства комплексной судебной экспертизы, назначения ее возможных субъектов, их статус, функции, а также порядок формулирования экспертами общего заключения.

Комплексная экспертиза − это экспертиза, в производстве которой участвуют несколько экспертов различных специальностей или узких специализаций (профилей).

Эффективность использования комплексной судебной экспертизы в значительной мере определяется степенью разрешенности ряда общих проблем, стоящих перед ней в целом проблема разработки общей методики решения задач комплексной судебной экспертизы, требующая совместной разработки экспертами разных специальностей комплексных методик, общих алгоритмов их действий в процессе совместной работы по производству комплексной экспертизы, неурегулированность порядка направления объектов экспертизы в судебно-экспертные учреждения различных ведомств и критерии отбора ведущего из них, неурегулированность порядка заявления ходатайств со стороны ведущего судебно-экспертного учреждения и его действий в случае отказа в удовлетворении ходатайств и др., нерегламентированность условий и порядка организации и производства комплексной судебной экспертизы, назначения ее возможных субъектов, их статус, функции, а также порядок формулирования экспертами общего заключения[1].

Перечисленные организационно-правовые проблемы комплексных судебных экспертиз должны быть разрешены в рамках УПК РФ, ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации», ведомственных актов.

Итак, можно сделать вывод, что порядок назначения и производства судебной экспертизы определен в гл. 27 УПК РФ. Однако назначение судебной экспертизы не является самостоятельным следственным действием, а является

[1] Антонов О. Ю. Анализ цифровой информации как одна из задач криминалистического исследования компьютерных средств и систем // Вестник криминалистики. 2020. № 2(74). С. 19.

лишь первоначальным этапом проводимой в рамках уголовного дела судебной экспертизы, за которым следует проведение экспертом исследования, формулирование выводов по поставленным перед ним вопросам, составление заключения. Назначение судебной экспертизы оформляется постановлением следователя, принявшего соответствующее решение (ст. 195 УПК РФ). Итогом же проведения судебной экспертизы является заключение эксперта, которое УПК РФ определяет как представленные в письменном виде содержание исследования и выводы по вопросам, поставленным перед экспертом лицом, ведущим производство по уголовному делу.

ЗАКЛЮЧЕНИЕ

На основании вышеизложенного можно сделать вывод, что преступления в сфере компьютерной информации – это умышленные общественно опасные деяния, совершаемые намерено или по неосторожности, которые причиняют вред защищаемым общественным отношениям либо создают угрозу причинения вреда.

Способы совершения преступлений в сфере компьютерной информации представлены двумя основными группами:

1. Преступные действия, осуществляемые без использования технических устройств, при проникновении в информационные системы или воздействия на них извне;

2. Преступные действия, осуществляемые с пользованием компьютерных устройств и или иных технических средств, в которых доступ осуществляется путем подбора логина и пароля, поиска пробелов в программе, и иных мер обхода защиты компьютерной информации.

Наиболее простым способом незаконного доступа к компьютерной информации является использование беспроводного соединения, чужого регистрационного адреса в сети Интернет либо чужого телефонного номера, использование услуг провайдера, которые не фиксируют данные абонентов сети, а также анонимных прокси-серверов и пр.

Широкое применение информационных технологий и технических средств с ЭНД в различных сферах повседневной жизни общества существенно повлияло на рост количества преступлений, совершаемых с их использованием. Повышенная общественная опасность данных деяний связана со сложностями, возникающими при их раскрытии и при установлении лица, совершившего такое преступление, а также в виктимологическом поведении пострадавших. Способ нарушения правил эксплуатации ЭВМ и защищенного использования ЭНД бывает активным (самовольное выполнение непредусмотренных операций при компьютерной обработке информации) или пассивным (невыполнение

предписанных действий) и связан с технологией обработки информации на компьютере.

Формами использования специальных знаний при расследовании IT-преступлений являются консультативная, справочная, сопроводительная и собственно процессуальная деятельность специалистов в области компьютерных технологий.

Следственными действиями, в которых возможно участие специалиста при расследовании IT-преступлений, являются осмотр места происшествия, осмотр предметов, обыск, допрос и выемка ЭНД.

При производстве осмотра места происшествия вниманию специалиста и следователя подвергаются компьютерно-технические средства, файловая система ПК, данные системного и прикладного ПО, а также ЭНД.

Специалист принимает активное участие в подготовке специальных технических и программных средств для производства обыска и выемки по делам об IT-преступлениях, определяет наиболее оптимальное время их производства и т.п. В ходе обыска следователь или специалист проводит поиск ЭНД и анализ сетевых источников и ресурсов, исследует каждое аппаратное средство ЭВМ и выявляет следы неправомерного использования компьютерных технологий.

Непроцессуальной формой взаимодействия следователя и специалиста, в том числе при расследовании IT-преступлений, являются такие виды как воссоздание первоначального объекта исследования, консультативная помощь эксперта или их группы, использование базы данных, исполнение поручений технического характера, содействие в участии ОРМ, разработка совместных организационных мер по эффективному использованию экспертно-криминалистических методов и средств в борьбе с преступностью, коллективное исследование материалов уголовных дел для эффективного принятия мер при работе с вещественными доказательствами.

Для преодоления недостатков взаимодействия следователя и специалиста соответственно необходимы:

актуализация действующего законодательства;

четкое правовое регулирование взаимодействия лиц;

улучшение материально-технической оснащенности подразделений;

дополнительная профессиональная подготовка субъектов взаимодействия;

С целью повышения качества производства следственных действий при расследовании IT-преступлений, в целях полной и своевременной раскрываемости данных преступлений, необходимо обязательное наличие в штате правоохранительных органов специалистов в области информационных технологий.

Специфика IT-преступлений обуславливает необходимость проведения по уголовным делам данной категории различных экспертиз. Так, объектом информационно-технологической экспертизы является установленный порядок обработки информации, осуществляемый по заданным алгоритмам или информационная технология, основанная на применении современной информационно-вычислительной техники, средств связи и телекоммуникаций, составляющих основу информатизации общества. Непосредственными предметами информационно-технологической экспертизы могут быть различного рода документы: проектная документация, документированная информация, материалы сертификации информационных систем и т.п.

Объектом информационно-технической экспертизы является техническое обеспечение информационной безопасности компьютерных систем и сетей. Предметом информационно-технической экспертизы являются инструменты, с помощью которых осуществляется доступ к информационным технологиям: (технические средства обработки информации, машинные носители информации, программные средства и базы данных).

Вопросы, задаваемые эксперту не ограничиваются одним и теми же распространенными вопросами и могут изменяться в зависимости в том числе и

от расследуемого события и выяснения обстоятельств информационно-технологического или информационно-технического характера.

Компьютерно-техническая экспертиза является такой экспертизой, которую можно отнести к классу инженерно-технических экспертиз, с помощью которой происходит комплексное исследование технической части компьютерных средств, программного обеспечения, объектов сетевых информационных технологий, информации, содержащейся в компьютерной системе.

В составе компьютерно-технической экспертизы выделяют четыре вида экспертиз: аппаратно-компьютерную, программно-компьютерную, информационно-компьютерную, компьютерно-сетевую.

Судебная компьютерная-техническая экспертиза производится государственными судебными экспертами и иными экспертами из числа лиц, обладающих специальными знаниями.

В целом, с точки зрения процессуального законодательства назначение компьютерно-технической экспертизы ЭНД не отличается от назначения других видов экспертиз. В ее производстве участвуют несколько экспертов различных специальностей или узких специализаций (профилей). Однако привлекаемые сведущие лица обычно не обладают правовыми знаниями и нередко выступают источником процессуальных нарушений.

Необходимость совершенствования нормативного регулирования процессуальных положений, регламентирующих использование вещественных доказательств в процессе производства по уголовным делам, создаёт предпосылки для последовательного уточнения тех особенностей, которыми обладают вещественные доказательства. Представляется, что любые нормативные изменения, связанные с нормами о доказательствах и доказывании должны строиться только на качественном научном материале. Только в этом случае можно избежать противоречивости положений УПК РФ, создающей сложности в правоприменении.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

I. Нормативные правовые акты и официальные документы

1. Конституция Российской Федерации: принята всенародным голосованием 12 декабря 1993 г. с учетом поправок, внесенных Законом Рос. Федерации о поправках к Конституции Рос. Федерации от 21 июля 2014 г. № 11-ФКЗ // Собр. законодательства Рос. Федерации. – 2014. – № 31, ст. 4398.

2. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 24 мая 1996 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 5 июня 1996 г. // Собр. законодательства Рос. Федерации. – 1996. – № 25, ст. 2954.

3. О государственной судебно-экспертной деятельности в Российской Федерации: федер. закон Рос. Федерации от 31 мая 2001 г. № 73-ФЗ принят Гос. Думой Федер. Собр. Рос. Федерации 5 апреля 2001 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 16 мая 2001 г. // Собр. законодательств Рос. Федерации. – 2001. – № 23, ст. 2291.

4. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 22 ноября 2001 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 5 декабря 2001 г. // Собр. законодательства Рос. Федерации. – 2001. – № 52 (ч. 1), ст. 4291.

5. Об информации, информационных технологиях и о защите информации: федер. закон Рос. Федерации от 27 июля 2006 г. № 149-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 8 июля 2006 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 14 июля 2006 г. // Собр. законодательств Рос. Федерации. – 2006. – № 31 (ч.1), ст. 3448.

6. Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации: приказ Министерства внутренних дел Российской Федерации

от 29 июня 2005 № 511 // Бюллетень нормативных актов федеральных органов исполнительной власти. – № 35. – 2005.

7. Об утверждении Перечня родов (видов) судебных экспертиз, выполняемых в федеральных бюджетных судебно-экспертных учреждениях Минюста России, и перечня экспертных специальностей, по которым представляется право самостоятельного производства судебных экспертиз в федеральных бюджетных судебно-экспертных учреждениях Минюста России: приказ Министерства юстиции Российской Федерации от 27 декабря 2012 № 237 // Рос. газета. – № 24. – 2013.

8. ГОСТ 2.051-2013 Единая система конструкторской документации. Электронные документы. Общие положения : дата введения 1 июня 2014. – Москва : Стандартинформ, 2011 год.

II. Учебная, научная литература и иные материалы

1. Антонов О. Ю. Анализ цифровой информации как одна из задач криминалистического исследования компьютерных средств и систем // Вестник криминалистики. 2020. № 2(74). С. 17–23.

2. Баев О. Я. Криминалистика: учебное пособие. М.: Юстиция, 2017. С. 258–259.

3. Васюков В. Ф. Особенности назначения судебных компьютерных экспертиз при расследовании преступлений в сфере информационно-коммуникационных технологий // Судебная экспертиза. 2016. № 2(46). С. 138–142.

4. Гавло В. К., Поляков В. В. Некоторые особенности расследования преступлений, связанных с неправомерным доступом к компьютерной информации // Известия Алтайского государственного университета. 2016. № 2. С. 47–51.

5. Гребенюк О. А., Жидков Д. Н., Макарова Е. Н. Тактика обнаружения, изъятия и осмотра средств электронных носителей информации и их

подготовки для назначения судебных экспертиз: учебно-практическое пособие. Санкт-Петербург: Санкт-Петербургский университет МВД России, 2020. С. 48–50.

6. Демин К. Е. О дидактических основах и стандартизации судебной компьютерно-технической экспертизы, проводимой в государственных экспертных органах Российской Федерации // Теория и практика фундаментальных и прикладных исследований в сфере судебно-экспертной деятельности и ДНК-регистрации населения Российской Федерации: Всероссийская научно-практическая конференция с международным участием. 2021. С. 50–53.

7. Добровлянина, О. В. Некоторые аспекты о процессуальном изъятии (копировании) электронных носителей информации // Пермский юридический альманах. 2019. № 2. С. 641–649.

8. Елфимов П. В. Особенности проведения и назначения комплексных судебных экспертиз // Вестник Уральского юридического института МВД России. 2017. № 2. С. 46–51.

9. Киреева, А. А. Электронный документ: эволюция понятия и носителя информации // Документ в современном обществе: факторы и тенденции развития информационной среды. Екатеринбург: Издательство Уральского университета. 2019. С. 78–81.

10. Козлов В. Е. Теория и практика борьбы с компьютерной преступностью. М.: Телеком. 2016. С. 405–406.

11. Комиссаров В. С., Крылова Н. Е., Тяжкова И. М. Уголовное право Российской Федерации: учебник. М.: Статут, 2016. С. 429-430.

12. Криминалистика. Полный курс: учебник / А.Г. Филиппов [и др.]. М.: Юрайт, 2017. С. 293-294.

13. Криминалистика: учебник для бакалавров. 2-е изд., испр. и доп. / Л. Я. Драпкина. М.,: Издательство Юрайт, 2023. С. 243-244.

14. Мазуров В. А. Компьютерные преступления. Классификация и способы противодействия: учебно-практическое пособие. М.: Палеотип, Логос, 2022. С. 167-168.

15. Потапов С. А. Совершенствование расследования и раскрытия преступлений в сфере компьютерной информации // Социально-экономические явления и процессы. 2016. № 10. С. 94–98.

16. Пропастин С. В. Назначение компьютерной экспертизы по делам об интернет-преступлениях // Уголовный процесс. 2016. № 6 (138). С. 37–41.

17. Россинская Е.Р. Проблемы использования специальных знаний в судебном исследовании компьютерных преступлений в условиях цифровизации // Вестник Университета имени О.Е. Кутафина. 2019. № 5 (57). С. 44-45.

18. Табункина Т.А. Проблемы получения уголовно-процессуальных доказательств в современных условий информатизации общества на досудебных стадиях расследования по уголовному делу // Государство и право в изменяющимся мире: правовая система в условиях информатизации общества. Материалы IV научно-практической конференции с международным участием. 2019. С. 272–276.

19. Телевицкая Ю. А. Об актуальности исследования особенностей выемки электронных носителей информации // Наука и образование: актуальные вопросы, достижения и инновации: сборник статей V Международной научно-практической конференции. Пенза: Наука и Просвещение, 2022. С. 74–76.

20. Телевицкая Ю. А. Понятие электронных носителей информации: проблемные аспекты интерпретации и толкования // Альманахъ молодых ученых: сборник научных статей. Том № 2 (4). Нижний Новгород: Нижегородская академия МВД России, 2021. С. 136–145.

21. Удовиченко В. С. Особенности изъятия информации с электронных носителей в досудебном производстве // Алтайский юридический вестник. 2021. № 2(34). С. 133–138.

22. Умнягина Ю. А. Электронные носители информации в уголовном судопроизводстве // Вестник Уральского юридического института МВД России. 2020. № 4(28). С. 52–55.

23. Федотов Н. Н. Форензика – компьютерная криминалистика. М.: Юридический Мир, 2017. С. 109-110.

III. Эмпирические материалы

1. Уголовное дело № 1-183***/2018 // Архив Белебеевского городского суда РБ. Оп. 1. 214 л.

2. Уголовное дело № 1-338***/2017 // Архив Советского районного суда г. Уфы. Оп 10. 178 л.

3. Уголовное дело № 1-193***/2017 // Архив Ленинского районного суда г. Уфы. Оп. 4. 156 л.

Материал вычитан, цифры, факты, цитаты сверены с первоисточником. Материал не содержит сведений, составляющих государственную и служебную тайну.

О. Э. Семёнова