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 **«КРИМИНАЛИСТИЧЕСКОЕ ИССЛЕДОВАНИЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ И ТЕХНИКИ В ЦЕЛЯХ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ (ПО МАТЕРИАЛАМ ТЕРРИТОРИАЛЬНОГО ОРГАНА ВНУТРЕННИХ ДЕЛ)»**

Выполнил
Асфандиярова Динара Дамировна
обучающийся по специальности
40.05.01 Правовое обеспечение
национальной безопасности
2018 года набора, 811 учебного взвода

Руководитель
преподаватель кафедры,
Ермолаева Любовь Николаевна

К защите _____
рекомендуется / не рекомендуется
Начальник кафедры _____ Э.Д. Нугаева
подпись
Дата защиты «___» _____ 2023 г. Оценка _____

ПЛАН

Введение……. 3

Глава 1. Общая характеристика криминалистического исследования компьютерной информации и техники в целях раскрытия и расследования преступлений..……. 5

§ 1. Понятие, цели криминалистического исследования компьютерной информации в целях раскрытия и расследования преступлений…….…… 5

§ 2. Предмет и объекты криминалистического исследования компьютерной информации в целях раскрытия и расследования преступлений …… 14

Глава 2. Особенности криминалистического исследования компьютерной информации и техники в целях раскрытия и расследования преступлений……..……. 21

§ 1. Криминалистические инструменты исследования компьютерной информации в целях раскрытия и расследования преступлений……. 21

§ 2. Проблемы, связанные с криминалистическим исследованием компьютерной информации в целях раскрытия и расследования преступлений……. 31

Заключение…… 40

Список использованной литературы…….. 46

Приложение 1 ……... 51

Приложение 2 ...……..... 52

ВВЕДЕНИЕ

Актуальность темы дипломной работы. Криминалистическое исследование компьютерной информации – достаточно новое явление в криминалистической технике. Появилось оно, в первую очередь, благодаря высокому уровню цифровизации общества. Все больше и больше общественных процессов перетекает в цифровую среду.

Важно понимать, что и уголовный мир не отстает от технологического прогресса, поэтому криминалистическая техника тоже должна подстраиваться под эти изменения. Криминалисты, как практики, так и ученые изучая компьютерную информацию смогут эффективнее профилактировать и раскрывать преступления совершенные с использованием высоких технологий.

На данный момент криминалистическое исследование компьютерной информации проводится в отношении почти всех категорий преступлений. Особенно это актуально для преступлений в сфере компьютерной информации, терроризма и экстремизма, экономических преступлений, распространения порнографической продукции, нарушений авторских и смежных прав, изготовление поддельной печатной продукции.

Объектом дипломной работы являются общественные отношения, возникающие в процессе криминалистического исследования компьютерной информации и техники в целях раскрытия и расследования преступлений.

Предметом дипломной работы являются применимые к объекту исследования: нормы и нормативные предписания российского законодательства; материалы судебной практики; доктринальные источники по теме исследования.

Степень научной разработанности дипломной работы. Про криминалистическое исследование компьютерной информации и техники в целях раскрытия и расследования преступлений написано достаточно большое количество научных трудов: научных статей, учебников, монографий.

В частности, такие авторы как Д.А. Камышов, Н.Н. Кулешова, Е.И. Христофорова, С.Ю. Скобелин, В.Н. Омелин, П.С. Пастухов и другие посвятили свои научные труды указанной теме.

Цель дипломной работы заключается в комплексном анализе криминалистического исследования компьютерной информации и техники в целях раскрытия и расследования преступлений.

Исходя из цели работы, можно выделить следующие задачи:

- определить понятие, цели криминалистического исследования компьютерной информации в целях раскрытия и расследования преступлений;

- рассмотреть предмет и объекты криминалистического исследования компьютерной информации в целях раскрытия и расследования преступлений;

- проанализировать порядок криминалистического исследования компьютерной информации в целях раскрытия и расследования преступлений;

- исследовать проблемы, связанные с криминалистическим исследованием компьютерной информации в целях раскрытия и расследования преступлений. Структура работы предполагает следующее её деление: введение, две главы, четыре параграфа, заключение, список использованной литературы, приложения.

ГЛАВА 1. ОБЩАЯ ХАРАКТЕРИСТИКА КРИМИНАЛИСТИЧЕСКОГО ИССЛЕДОВАНИЯ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ И ТЕХНИКИ В ЦЕЛЯХ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ

§ 1. Понятие, цели криминалистического исследования компьютерной информации в целях раскрытия и расследования преступлений

С каждым годом общество все больше и больше связывает свою жизнь с цифровым миром. Несомненно, это влияет и на преступный мир. Перед человечеством остро встал вопрос более глубокой проработки криминалистической теории и практики борьбы с преступлениями совершенными с использованием высоких технологий. В то же время можно заметить, что имеется некоторое отставание законодателя в данном вопросе.

Как отмечается в Стратегии развития отрасли информационных технологий в Российской Федерации, «масштаб влияния отрасли информационных технологий на государство значительно превосходит сугубо отраслевые эффекты.

Развитие информационных технологий является одним из важнейших факторов, способствующих решению ключевых экономических, социальных задач государственной политики»[1].

В то же время, в работе криминалиста очень важно следовать современным тенденциям.

Как потерпевшие, так и преступники используют в своей повседневной жизни разнообразные электронные устройства (телефоны, планшеты, компьютеры, электронные часы, GPS и так далее). Данные устройства в частности успешно используются в приготовлении, совершении преступлений, сокрытии следов преступления.

---

[1] Об утверждении Стратегии развития отрасли информационных технологий в Российской Федерации на 2014 – 2020 годы и на перспективу до 2025 года: распоряжение Правительства РФ от 01 ноября 2013 № 2036-р (ред. от 18 октября 2018) // Официальный интернет-портал правовой информации. URL:http://www.pravo.gov.ru/ (дата обращения: 02.02.2023).

Таким образом, преступники совершают так называемые «бесконтактные» преступления, то есть преступления с удаленным доступом, что исключает оставление трасологических следов. Однако, как и при совершении любого вида преступления, лицо его совершающее оставляют следы, в данном случае это будут цифровые следы, от которых зачастую сложнее избавиться.

Все вышеперечисленное ставит новые вопросы перед криминалистами. В частности, необходимо постоянно совершенствовать механизм сбора доказательственной компьютерной информации, также необходимо решить вопрос как такой вид информации изымать, фиксировать и исследовать[1]. Нужно учитывать специфику компьютерной информации и уже исходя из этого выстраивать систему взаимодействия.

Ценность компьютерной информации заключается в том, что с её помощью можно более эффективно выполнять функции по выявлению, раскрытию и расследованию преступлений, идентификации неопознанных трупов и многое другое.

Сам процесс получения и использования компьютерной информации в качестве доказательства осуществляется в большей степени в рамках проведения оперативно-розыскной деятельности. Определение понятия «оперативно-розыскная деятельность» содержится в Федеральном законе от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности».

Согласно ст. 1 указанного Федерального закона, оперативно-розыскная деятельность – «вид деятельности, осуществляемой гласно и негласно оперативными подразделениями государственных органов, уполномоченных на то настоящим Федеральным законом (далее - органы, осуществляющие оперативно-розыскную деятельность), в пределах их полномочий посредством проведения оперативно-розыскных мероприятий в целях защиты жизни, здоровья, прав и свобод человека

[1] Скобелин С. Ю. Использование цифровых технологий при доказывании преступной деятельности // Российский следователь. 2019. № 3. С. 26-28.

и гражданина, собственности, обеспечения безопасности общества и государства от преступных посягательств»[1].

Согласно ст. 6 ФЗ «Об оперативно-розыскной деятельности», при осуществлении оперативно-розыскной деятельности проводится в частности такое оперативно-розыскные мероприятие как получение компьютерной информации.

На данный момент определение оперативно-розыскного мероприятия не закреплено в российском законодательстве. В связи с этим необходимо обратиться к доктринальным источникам, которые содержат достаточно большое количество вариаций определения данного понятия.

Чаще всего под оперативно-розыскными мероприятиями понимаются «предусмотренные законом и подзаконными нормативными актами разведывательно-поисковые действия, проводимые уполномоченным субъектом преимущественно негласными средствами и методами при наличии определенных оснований и в соответствии с установленным порядком, направленные на получение, фиксацию и проверку сведений, предметов и документов как источников таких данных, значимых для выявления, предупреждения, пресечения и раскрытия преступлений, а также для решения иных задач оперативно-розыскной деятельности»[2].

В законе отсутствует определение криминалистического исследования компьютерной информации. В целом криминалистическое исследование – это раздел криминалистической техники, в рамках которого изучается каким образом криминалистически значимая информация возникает, влияет на объекты, как движется. Исходя из указанного выше определения, помня о специфике компьютерной информации, как объекта исследования, можно

---

[1] Об оперативно-розыскной деятельности: федер. закон Рос. Федерации от 12 августа 1995 № 144-ФЗ (ред. от 28.12.2022) // Официальный интернет-портал правовой информации. URL:http://www.pravo.gov.ru/ (дата обращения: 07.01.2023).

[2] Омелин В. Н. Оперативно-розыскные мероприятия и оперативно-розыскные действия: критерии разграничения // Закон и право. 2018. № 11. С. 132-134.

сформировать следующее определение криминалистического исследования компьютерной информации.

Криминалистическое исследование компьютерной информации – это система научных положений, на основе которых разрабатываются отдельные приемы, методы и рекомендации по использованию компьютерных технологий и информации, содержащейся в них для раскрытия, расследования и предупреждения преступлений.

Криминалистическое исследование данных объектов проводится в рамках следующих следственных действий: осмотр, обыск, выемка. Следственные действия – это предусмотренные и строго регламентированные уголовно-процессуальным законом, обеспеченные силой государственного принуждения действия уполномоченных лиц, цель которых сбор и проверка доказательств по уголовному делу. К примеру, в ходе обыска по уголовному делу № 0001, проводимого по адресу местопроживания подозреваемого К, был обнаружен мобильный телефон, принадлежащий последнему. Данный объект до фиксации его изъятия в протоколе следственного действия был подвергнут исследованию. Результат исследования показал, что на устройство установлено мобильное приложение «ВКонтакте» с личной страницей подозреваемого, находящейся в свободном доступе для всех пользователей указанной социальной сети, где был размещен материал порнографического характера[1] Это позволило непосредственно на месте и в ходе производства следственного действия определить доказательственное значение обнаруженного объекта. Так, по уголовному делу № 0002, возбужденному в отношении неустановленного лица по признакам преступления, предусмотренного ст. 159.6 Уголовного кодекса Российской Федерации, криминалистическое исследование персонального компьютера потерпевшей и информации, содержащейся на нем, проводилось в ходе осмотра места происшествия[2].

[1] Уголовное дело № 0001 // Арх. ОМВД РФ по Уфимскому району РБ. Оп. 1. 101 л.
[2] Уголовное дело № 0002 // Арх. ОМВД РФ по Уфимскому району РБ. Оп. 1. 134 л.

В модельном законе «Об оперативно-розыскной деятельности» от 16 ноября 2006 г. № 27-6, принятый Межпарламентской Ассамблеей государств-участников СНГ закреплено следующее понятие мониторинга информационно-телекоммуникационных сетей и систем – «это получение сведений, необходимых для решения конкретных задач оперативно-розыскной деятельности, и их фиксация путем наблюдения с применением специальных технических средств за характеристиками электромагнитных и других физических полей, возникающих при обработке информации в информационных системах и базах данных и ее передаче по сетям электрической связи, компьютерным сетям и иным телекоммуникационным системам»[1].

Часто при выявлении того или иного понятия, в нашем случае это понятие словосочетания «получение компьютерной информации» необходимо вычленить отдельные признаки данного явления. К последним можно отнести следующее[2]:

1. В рамках поиска компьютерной информации необходимо использовать специальные способы доступа к информационным технологиям. Это необходимо делать путем использования специального оборудования, обеспечивающего скрытность доступа к указанным технологиям, включая дистанционный доступ.

2. В рамках поиска компьютерной информации осуществляется мониторинг ряда информационных ресурсов, содержащих сведения, полезные для решения задач оперативно-розыскной деятельности.

Таким образом, получение компьютерной информации – это получение специально уполномоченным на то органом хранящейся у операторов связи или Интернет-провайдеров следующих видов информации:

---

[1] Модельный закон «Об оперативно-розыскной деятельности». Принят на двадцать седьмом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ (постановление №27-6 от 16 ноября 2006 года) // Информационная система «КОНТИНЕНТ». URL:http://continent-online.com/Document/?doc_id= 30161811 (дата обращения: 07.01.2023).

[2] Налбандян Р. Г. Получение компьютерной информации как новая категория оперативно-розыскного законодательства // Проблемы экономики и юридической практики. 2018. № 1. С. 137-144.

1. информация о взаимодействии пользователя с компьютерной информацией, будь то получение, передача, обработка этой информации; Информация может быть представлена в разных формах: аудио, текстовая, видео, фото.

2. непосредственно содержащаяся в аудио, видео, фото, тексте;

3. о взаимодействии пользователя с компьютерной информацией, поступающая путем использования сети «Интернет», а также информация о самом пользователе;

4. непосредственно содержащаяся в сети «Интернет», к которой имеет доступ пользователь.

Компьютерная криминалистика по своему содержанию включает[1]:

1. поиск компьютерных данных и их восстановлении в случае удаления;

2. обработка данных и вычленение информации, представляющей особое криминалистическое значение. Формирование электронных доказательств;

3. анализ полученных данных и их использование в целях раскрытие и расследование преступлений.

При помощи компьютерной информации можно решить множество криминалистических задач: получить доказательства, выявить расположение преступника с его соучастниками и возможными свидетелями. В рамках компьютерной криминалистики можно знакомиться с личными переписками, изучить журнал браузеров, прослушать телефонные разговоры, то есть проводить все следственные и иные процессуальные действия направленные на изучение цифровых следов.

Несомненно, для совершения указанных действий есть ряд ограничений. В противном случае такие действия считались бы незаконными и противоречащими Конституции РФ.

Таким образом, можно выделить цель компьютерной криминалистики. Глобальной целью является поиск, фиксация, обработка

[1] Пастухов П. С. О необходимости развития компьютерной криминалистики // Пермский юридический альманах. 2018. № 1. С. 450-460.

и анализ компьютерной информации, которая в последующем будет использоваться как доказательство в суде.

Можно сказать, что выделение компьютерной криминалистики вполне обоснованно. В то же время важно оценить сформированность данного нового направления криминалистического исследования. В науке это происходит путем выявления следующих критериев:

1. Существуют специфические задачи, которые не решаются при использовании других видов криминалистического исследования.

В целом можно выделить одну главную задачу криминалистического исследования компьютерной информации – оптимизация деятельности правоохранительных органов в борьбе с преступностью путем использования современных технологий.

Указанную задачу можно разделить на несколько элементов[1]:

1) исследование закономерностей между компьютерной информацией и преступлением;

2) разработка и совершенствование средств и специальных способов поиска, фиксации, изъятия, исследования и использования компьютерной информации;

3) разработка и совершенствование тактических приемов, необходимых для поиска компьютерной информации;

4) исследование и внедрение зарубежного опыта в области изучения компьютерной криминалистики;

5) разработка и внедрение новейших компьютерных разработок в практическую деятельность в области компьютерной криминалистики.

2. Существует особая специфика объектов исследования, при условии их распространенности.

[1] Смушкин А. Б. Цели, задачи и функции электронной цифровой криминалистики // Криминалистика: вчера, сегодня, завтра. 2020. № 1 (13). С. 103-107.

В случае исследования компьютерной информации имеется специфичный объект исследования – информация, находящаяся в цифровой среде, закрепленная на каком-либо электронном носителе.

Для взаимодействия с данным объектом необходимы особые навыки и умения, также необходимо знание законодательства. Например, Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 № 149-ФЗ, Федеральный закон «О персональных данных» от 27 июля 2006 № 152-ФЗ.

3. Выработана методологическая и методическая разработанность данного направления.

Несмотря на то, что данное направление появилось относительно недавно, уже есть некоторые методологические и методические правила и рекомендации.

Важным также является изучение функций компьютерной криминалистики. Под функцией в целом понимается деятельность, роль объекта в рамках некоторой системы, роль, значение (назначение, предназначение) чего-либо.

Следует выделить две ключевые функции компьютерной криминалистики:

1. Познавательная.

Данная функция направлена на изучение носителей компьютерной информации, способов фиксации информации на компьютере. Изучается каким образом, технические средства участвовали в совершении преступления, какие следы были оставлены преступником[1].

В основном данная функция направлена на поиск и изучение новых знаний. При этом исследуется не просто любая информация, а именно криминалистически значимая компьютерная информация.

2. Конструктивная.

[1] Смушкин А. Б. Цели, задачи и функции электронной цифровой криминалистики // Криминалистика: вчера, сегодня, завтра. 2020. № 1 (13). С. 103-107.

В рамках названной функции создаются и совершенствуются новые технические средства, как-либо помогающие в поиске, фикции, исследовании компьютерной информации.

Она охватывает создание новых средств, приемов, методов и рекомендаций, также направленных на поиск, фиксацию, исследование компьютерной информации. Все вышеперечисленное помогает преобразовать полученную компьютерную информацию в полноценное доказательство по делу. Конструктивная функция направлена на совершенствование технических средств, необходимых для успешной работы правоохранительных органов.

3. Прогностическая.

Прогностическая функция направлена на анализ потенциальных угроз для человечества, изучается, каким образом современные технологии могут повлиять на человечество и к каким рискам это может привести. На основе составленного прогноза создаются новые или совершенствуются старые технические средства, способы и методы поиска, фиксации и анализа компьютерной информации.

Нередко получение компьютерной информации путают с другими оперативно-розыскными мероприятиями, например, такими как: контроль почтовых отправлений, телеграфных и иных сообщений, снятие информации с технических каналов связи. Для того, чтобы качественно провести грань между различными оперативно-розыскными мероприятиями[1] необходимо проанализировать название конкретного ОРМ и выявить, какие действия совершаются во время таких мероприятий.

Для начала стоит заметить, что получение компьютерной информации посредством оперативно-розыскного мероприятия направлено именно на обнаружение на техническом средстве (компьютере) непосредственно или в сети «Интернет» компьютерной информации.

В данном случае не предполагается, что эта информация кому-то передается, как например, при прослушивании телефонных переговоров

[1] Далее – «ОРМ».

(прослушивание телефонных переговоров как оперативно-розыскное мероприятие). В последнем ОРМ важен сам факт, что в конкретную единицу времени информация передавалась по телефону.

Если анализировать такое оперативно-розыскное мероприятие как снятие информации с каналов связи и контроль почтовых отправлений, то в данном случае также важен именно факт передачи информации от одного человека другому. При получение компьютерной информации, информация не передается, а хранится[1].

Таким образом, даже несмотря на то, что во всех трех случаях используется техническое средство, отличие все же имеется.

В то же время, следует заметить, что появление компьютерной криминалистики абсолютно оправдано и логично. При все больше возрастающей популярности компьютерных технологий, наличии специфических объектов для изучения, необходимости применять специальные средства и знания для изучения компьютерной информации, важность выделения криминалистического исследования компьютерной информации не может ставиться под сомнения.

§ 2. Предмет и объекты криминалистического исследования компьютерной информации в целях раскрытия и расследования преступлений

Объектом исследования является то, что непосредственно изучается в рамках определенного направления.

В целом объектом криминалистического исследования компьютерной информации в целях раскрытия и расследования преступлений является непосредственно компьютерная информация.

Определение компьютерной информации закреплено в примечании 1 ст. 272 Уголовного кодекса Российской Федерации (далее УК РФ). Так, «под

[1] Алексанин А. С. О понятии и содержании оперативно-розыскного мероприятия «получение компьютерной информации» // Правовое государство: теория и практика. 2018. № 1 (51). С. 153-159.

компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи»[1].

Общее понятия информации содержится также в некоторых других законах. Так, например, в п. 1 ст. 2 ФЗ №149 «Об информации, информационных технологиях и о защите информации» указывается, что «информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления».

Данное определение не дает достаточной конкретизации, более того нам необходима привязка к цифровому, электронному характеру информации. В п. 11.1 ст. 2 указанного закона также содержится следующее понятие: «Электронный документ – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах»[2].

В УК РФ компьютерная информация предстает в виде электрических сигналов. В ФЗ № 149 от 27.07.2006 «Об информации, информационных технологиях и о защите информации» указывается, что компьютерная информация – это сведения, представленные в электронной форме. Понятие данное в УК РФ более точно отображает физическую сторону информации. Однако эти определения дополняют друг друга и понятие компьютерной информации становится более проработанным и понятным.

При определении понятия информация нередко обращаются к федеральному закону РФ «О государственной тайне».

---

[1] Уголовный кодекс Российской Федерации от 13 июня 1996 № 63-ФЗ (ред. от 29 декабря 2022 №586-ФЗ) // Официальный интернет-портал правовой информации. URL:http://www.pravo.gov.ru/ (дата обращения: 02.02.2023).

[2] Об информации, информационных технологиях и о защите информации: федер. закон от 27 июля 2006 № 149-ФЗ (ред. от 29 декабря 2022 №604-ФЗ) // Официальный интернет-портал правовой информации. URL:http://www.pravo.gov.ru/ (дата обращения: 02.02.2023).

В ст. 2 рассматриваемого закона дается следующее определение носителей сведений, составляющих государственную тайну: «...материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов»[1].

Таким образом, компьютерная информация – это искусственно созданный объект (созданный человеком). При этом такая информация не может существовать без специальных приспособлений (электронно-вычислительной техники и электронных средств связи).

В целом компьютерная информация состоит всего из двух основных элементов: носитель информации (то, на чем компьютерная информация хранится); сама компьютерная информация (её содержание).

Важно подчеркнуть, что компьютерная информация, содержится в форме, пригодной для обработки электронной вычислительной машиной.

Как отмечалось ранее компьютерная информация считывается с компьютерной техники. Чаще всего встречается классификация компьютерной техники в зависимости от функционального назначения[2]:

I. аппаратные средства.

Это технические средства, используемые для обработки данных. В числе аппаратных средств можно назвать:

1. Компьютер / ЭВМ. Компьютер занимается автоматической обработкой различной поступающей информации.

Компьютеры в свою очередь классифицируются на: а) супер – ЭВМ; б) большие ЭВМ; в) мини - ЭВМ, микро - ЭВМ, персональные ЭВМ.

Все они отличаются по сложности выполняемых задач, объёму обрабатываемой информации и числу пользователей. То есть, например,

---

[1] О государственной тайне: закон Рос. Федерации от 21 июля 1993 № 5485-1 (ред. от 05 декабря 2022 №498-ФЗ) // Официальный интернет-портал правовой информации. URL:http://www.pravo.gov.ru/ (дата обращения: 02.02.2023).

[2] Волеводз А. Г. Компьютерная информация как объект криминалистического следоведения // Криминалистическая техника: Учебник / Отв. ред. И. М. Балашов, рук. колл. С. В. Маликов. М.: Юрлитинформ, 2008. С. 336-381.

обычный гражданин в повседневной жизни пользуется третьим видом ЭВМ. Исследование такого компьютера поможет при расследовании не сложных преступлений.

Второй и первый вариант исследуется при совершении более сложных преступлений. В данном случае такими ЭВМ пользуется не один человек, а несколько, поэтому необходимо также определить, кто именно совершил преступление.

2. Периферийное оборудование.

Под периферийным оборудованием подразумевается оборудование зависящее от ЭВМ. Оно скорее осуществляет передачу определенных заданных данных и команд.

Можно перечислить следующие виды такого оборудования: принтер, модем (это устройство для связи между компьютерами), факс-модем (сочетает в себе функции модема и обмена другими факс-модемами).

3. Физические носители магнитной информации.

Это устройства, предназначенные для хранения информации, используемой при работе с компьютером. В качестве примера можно привести винчестер (накопитель на жестком диске).

II. Программные средства.

Программные средства можно понимать по-разному. В первом случае это определенный набор программ, которые обеспечивают функционирование компьютера, помогают выполнять определенные команды с целью получения заданного результата.

Во втором случае это материалы, зафиксированные на физическом носителе полученные в ходе их разработок, и порождаемые ими аудиовизуальные отображения.

К программным средствам можно отнести:

1. Программное обеспечение.

Это совокупность программ, отвечающих за управление компьютером и обработку информации. Программное обеспечение используется для организации вычислительного процесса, автоматизации процессов.

К программному обеспечению относится: а) системные программы (например, операционные системы); б) прикладные программы (например, редакторы, антивирусы); в) системы программирования (например, C++, Python).

2. Машинная информация.

То есть это информация, зафиксированная и хранящаяся на машинном носителе. Важно заметить, что компьютерная криминалистика при исследовании компьютерной информации изучает не саму компьютерную технику, а файлы, хранящиеся в ней.

Из всего вышеперечисленного следует выделить объекты, в отношении которых эксперты чаще всего проводят исследования, это: компьютер / ЭВМ, накопитель на жестком диске, диски, дискеты, флеш-накопители.

Признаки компьютерной информации[1]:

1. компьютерная информация содержится на материальном носителе в виде кода, из чего следует, что она не доступна для человеческого восприятия. Человек не может взаимодействовать с такой информацией без использования специального оборудования;

2. компьютерная информация хранится на материальном носителе, но при этом не всегда она привязана только к одному носителю. Особенно это актуально, если мы говорим про информацию, хранящуюся в сети «Интернет»;

3. компьютерная информация может быть отделена от материального носителя без изменений;

[1] Мицкевич А. Ф., Суслопаров А. В. Понятие компьютерной информации по российскому и зарубежному уголовному праву // Пробелы в российском законодательстве. Юридический журнал. 2010. № 2. С. 206-209.

4. компьютерная информация может быстро создаваться, меняться, передаваться;

5. при изъятии информации с материального носителя она сохраняется в первоисточнике;

6. компьютерная информация в некоторых случаях доступна для широкого круга пользователей.

Объект исследования следует отличать от предмета исследования.

Если под объектом исследования подразумевается то, что непосредственно изучается в рамках конкретного направления, то предметом исследования является особая проблема, отдельные стороны объекта, его свойства и особенности, взаимосвязи. Так, в предмет криминалистического исследования компьютерной информации входит:

1. Исследование процесса обработки и способов фиксации компьютерной информации.

2. Разработка и совершенствование криминалистической тактики и техники в указанной области. Создание новых способов и приемов поиска, фиксации и изъятия компьютерной информации.

Компьютерная информация также не однородна по своей природе. Существует множество классификаций.

1. Классификация в зависимости от материального носителя, содержащего компьютерную информацию:

а) жесткий магнитный диск. Данное устройство может находиться как непосредственно внутри компьютера, так и отдельно от него;

б) оперативное запоминающее устройство (ОЗУ-RAM) и постоянное запоминающее устройство (ПЗУ-ROM). Данные объекты отвечают за сохранение информации;

в) гибкие магнитные диски или дискеты (например, накопитель). Данный объект предназначен для считывания и фиксирования компьютерной информации;

г) накопители на магнитных лентах (стримеры). Данный объект необходим для записи и воспроизведения компьютерной информации. Стримеры, например, также используются для архивирования информации.

д) оптические и магнитооптические диски. Это, например, накопитель на компакт-дисках (CD-ROM), магнитооптические дисководы, ZIP-устройства и другие.

2. Классификация в зависимости от функционального назначения: а) текстовая; б) графическая; в) мультимедиа; г) информация в форматах баз данных; д) программные средства.

3. Классификация в зависимости от правового статуса: а) документ (обладает рекизатами); б) информация, не имеющая документированной формы.

Не редким является поиск информации о преступлении и преступнике в информационно-телекоммуникационной сети.

Под информационно-телекоммуникационной сетью понимается «технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники. Для целей уголовного законодательства понятия электронных и информационно-телекоммуникационных сетей не разграничиваются. При этом следует иметь в виду, что сеть «Интернет» является одним из их видов»[1].

Таким образом, можно опять-таки сделать вывод, что имеется ряд проблем с проработкой понятийного аппарата. Необходимо дать более подробное понятие компьютерной информации, так как действующее понятие не охватывает все многогранность объекта.

[1] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»: постановление Пленума Верховного Суда РФ от 15 декабря 2022 № 37 // Официальный сайт Верховного суда Российской Федерации. URL: https://vsrf.ru/documents/own/31913/ (дата обращения: 02.02.2023).

ГЛАВА 2. ОСОБЕННОСТИ КРИМИНАЛИСТИЧЕСКОГО ИССЛЕДОВАНИЯ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ И ТЕХНИКИ В ЦЕЛЯХ РАСКРЫТИЯ ИРАССЛЕДОВАНИЯ ПРЕДСТУПЛЕНИЙ

§ 1. Криминалистические инстументы исследования компьютерной информации в целях раскрытия и расследования преступлений

Криминалистическое исследование компьютерной информации должно проводиться исключительно специально обученными на то людьми, то есть специалистами и экспертами.

Выделяют две основные процессуальные формы проведения криминалистического исследования компьютерной информации:

1. С участием специалиста.

Специалист привлекается для осуществления действий, связанных с поиском, исследованием (по поручению следователя), фиксацией и изъятием компьютерной информации.

Специалист привлекается для: поиска компьютерной информации; изучение текущего состояния компьютерной информации, ее изменений; решение вопроса о необходимости проведения экспертизы с участием эксперта.

Специалист обладает специальными знаниями в указанной области, однако, если возникает риск утраты или изменения исследуемой информации, то уже привлекается эксперт. Также эксперт привлекается в целом при решении более сложных криминалистических задач[1].

На специалиста в сфере компьютерной криминалистики возлагаются следующие функции[2]: сбор данных; дублирование и сохранение данных; восстановление данных; поиск документов; преобразование мультимедиа;

---

[1] Яблоков Н. П. Криминалистика: Учебник, 3-е изд., перераб. и доп. М.: Юрайт, 2023 г., С. 239.

[2] Пастухов П. С. О необходимости развития компьютерной криминалистики // Пермский юридический альманах. 2018. № 1. С. 450-460.

выступление в качестве экспертов свидетелей в суде; исследование компьютерных данных и так далее.

2. С участием эксперта.

Эксперт проводит компьютерно-техническую экспертизу, которая назначается как в отношении компьютерной информации, так и в отношении компьютерного оборудования (ПРИЛОЖЕНИЕ 1).

Можно выделить следующие виды судебных экспертиз, назначаемых при изучении компьютерной информации:

1) судебная аппаратно-компьютерная экспертиза (исследование самих материальных носителей информации);

2) судебная программно-компьютерная экспертиза (исследование программного обеспечения компьютерной системы);

3) судебная информационно-компьютерная экспертиза (данный вид экспертизы направлен на поиск, обнаружение, анализ и оценку информации, подготовленной пользователем или созданной программами);

4) судебная компьютерно-сетевая экспертиза (анализ сетевого трафика и отслеживание пакет данных, передаваемых через сеть для обнаружения вторжений и вредоносных программ).

Эксперт – это специалист, дающий заключение при рассмотрении какого-либо вопроса. Они обладают специальными знаниями в своей работе пользуются специфической профессиональной лексикой. В то же время эксперт должен уметь доступным для понимания языком объяснить сложные технические процессы. Он должен объяснить, каким образом можно обнаружить компьютерную информацию, где конкретно её искать, что она из себя представляет, а также какое именно отношение она имеет к преступлению.

При исследовании цифровых следов устанавливается: 1) какие сайты в сети «Интернет» посетил пользователь; 2) какие файлы пользователь создавал и редактировал на компьютере; 3) когда файл в последний раз открывался; 4) производились ли пользователем попытки удалить файл; 5) были ли попытки

сфабриковать доказательства; 6) имелись ли электронные копии документов, которые были удалены из печати; 7) были ли файлы переданы кому-либо путем использования электронных средств.

«Государственная судебно-экспертная деятельность основывается на принципах законности, соблюдения прав и свобод человека и гражданина, прав юридического лица, а также независимости эксперта, объективности, всесторонности и полноты исследований, проводимых с использованием современных достижений науки и техники»[1].

При проведении экспертизы эксперт должен руководствоваться основополагающими принципами, применяемыми при исследовании компьютерной информации. К ним в частности можно отнести[2]:

1. Надежное фиксирование информации, недопущение изменения информации.

2. Для исследования компьютерной информации необходимо произвести изъятие материального носителя, на котором находится данная компьютерная информация. В случае, если изъятие невозможно, в исключительных случаях исследование может производиться на месте.

3. При проведении экспертизы обязательно должно участвовать лицо, имеющее специальные познания в области компьютерных технологий.

4. Обязательное ведение протокола. Это обеспечительная мера, направленная на соблюдение прав всех участвующих лиц, а также способствует приобретению исследуемому объекту статуса доказательства.

Важно отметить, что данные принципы актуальны не только в работе эксперта, но и в работе специалиста.

---

[1] О государственной судебно-экспертной деятельности в Российской Федерации: федер. закон Рос. Федерации от 31 мая 2001 № 73-ФЗ // Официальный интернет-портал правовой информации. URL:http://www.pravo.gov.ru/ (дата обращения: 05.02.2023).

[2] Россинская Е. Р., Шамаев Г. П. Новый раздел криминалистики: криминалистическое исследование компьютерных средств и систем // Baikal Research Journal. 2015. Т. 6. № 1. С. 317-325.

В связи со сложностью объектов исследования при назначении конкретной экспертизы следователю рекомендуется предварительно согласовать вопросы с экспертом.

В постановлении о назначении судебно-компьютерной экспертизы, порядок вынесения и содержание которого предусматривается ст. 195 Уголовно-процессуального кодекса РФ[1], перед экспертами могут быть поставлены следующие вопросы при исследовании компьютерной информации[2]:

1. Совершались ли какое-нибудь манипуляции (передача, изменение) с компьютерной информацией? Если да, то когда и каким образом? Был ли осуществлен доступ с одного компьютера или с нескольких? Если доступ был с одного компьютера, то можно ли выявить с какого?

2. Имеется ли возможность каким-либо образом корректировать, видоизменять исследуемую информацию? Имеются ли уничтоженные или измененные файлы? Какая есть информация о файле (наименование, дата формирования, объем)? Когда в последний раз вносились изменения (дата и характер изменений)?

3. Какие средства применялись при работе с компьютерной информацией? К какому типу они относятся?

4. К какому типу относится исследуемая компьютерная информация (текст, фото, видео, аудио)?

5. Была ли информация создана на исследуемом компьютере или имеется иной первоисточник?

6. Есть ли доступ в «Интернет»?

7. Имеются ли какие-либо системы защиты на исследуемом компьютере?

8. Можно ли идентифицировать пользователей, пользующихся исследуемой компьютерной информацией?

---

[1] Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001г. № 174-ФЗ (с посл. изм. и доп. от 17 февраля 2023г. № 30-ФЗ) // Официальный интернет-портал правовой информации. URL:http://pravo.gov.ru/ (дата обращения: 07.01.2023).

[2] Яблоков Н.П. Криминалистика: Учебник, 3-е изд. М.: Юрайт, 2023. С. 187.

Данный перечень вопросов не исчерпывающий.

Можно выделить два основных метода экспертных исследований: математические методы и научно-технические методы.

Это, например, анализ, моделирование, метод экспертных оценок и так далее.

Перед проведением экспертизы необходимо проверить компетенцию самого эксперта. Узнать, какая необходима в конкретном случае экспертиза. Иногда возникает необходимость пригласить нескольких экспертов. Это связано с обладанием узких знаний в конкретной области, следовательно, необходимо тщательно анализировать какие программные и технические средства были использованы при взаимодействии с определенными файлами и ссылками.

Экспертиза не всегда проходит абсолютно гладко. Часто возникает множество дополнительных препятствий. В некоторых случаях может возникнуть потребность изучить компьютерные систем в процессе их функционирования. Этот способ примнется чаще при необходимости выявления ошибок в работе, выявлении слабых мест в защите.

В данном случае часто применяется методика экспертного эксперимента, исследование информации непосредственно на месте происшествия.

При проведении компьютерной экспертизы важно соблюдать ряд условий. Важнейшим из них можно назвать обеспечение сохранности полученной компьютерной информации. В данном случае необходимо уделить особое внимание способу фиксации такой информации. В практике фиксация осуществляется путем создания копии полученной информации.

Для обеспечения надлежащей сохранности компьютерной информации применяются всевозможные продвинутые программы блокираторов записи, такие как: Disklock, HDSEntry. Данные программы применяются при невозможности создания точной копии.

Стоит помнить, что компьютерная информация достаточно уязвима и нередко подвергается воздействию посторонних факторов.

Таким образом, подтверждать факт необходимости обеспечения сохранности полученной компьютерной информации не имеет смысла. В случае утраты такой информации или носителя, на котором находилась компьютерная информация, необходимо ставить вопрос о том, произошло ли это случайно или по чьей-либо вине, были ли допущены ошибки экспертом.

При надлежащей фиксации информации можно полноценно оценить работу эксперта, проанализировать сделанные им выводы, определить значимость этих выводов в качестве доказательства по делу.

В случае необходимости эксперту могут быть поставлены дополнительные вопросы.

После проведения экспертизы необходимо проверить качество составленного заключения. В частности, важно оценить насколько полно использовались предоставленные эксперту материалы. Основная сложность заключается в том, что исследуемая информация предоставляется в очень большом объеме, что определяет некоторые сложности исследования. В то же время, не вся информация имеет отношение к вопросам, поставленным перед экспертом.

Таким образов, ещё раз стоит подчеркнуть важность совместной работы следователя и эксперта. Следователь предварительно очерчивает круг вопросов, которые необходимо рассмотреть в рамках исследования. Эксперт просматривает все предоставленную ему информацию, однако в дальнейшем изучает только тот объем и только те файлы, которые дадут ответ на следственные вопросы. В этом случае эксперт должен указать, почему он ограничился изучением только определенных объектов из всех представленных ему.

В экспертном заключении должны указывать средства и методы, применимые при исследовании компьютерной информации в ходе проведения экспертизы. Однако не обязательно указывать подробный перечень этих средств и методов, так как в таком случае заключение будет перегружено не особо важной для дела информацией.

Что более важно, так это то, что эксперт должен в целом продемонстрировать весь процесс работы, логическую последовательность и результаты. Важно отметить, что эксперт при формировании заключения использует специальную терминологию, в то же время важно предоставлять информацию как можно более понятной для обывателей.

Эксперт в своей деятельности не всегда использует последние разработки в сфере компьютерной криминалистики. Это в первую очередь связано с высокой стоимостью соответствующего оборудования. В то же время экспертизы все равно характеризуется высокой степенью точности результатов.

Можно выделить следующие основные ошибки, которые наиболее часто допускаются при назначении и производстве компьютерной экспертизы:

1. Постановка перед экспертом задачи оценить содержание компьютерной информации.

Работа эксперта заключается скорее в поиске информации, установлении фактов. Он не обладает знаниями в области юриспруденции и криминалистики, то есть не может качественно оценить содержание полученной компьютерной информации. Указанной работой занимается скорее следователь. Эксперт в свою очередь должен работать совместно со следователем, выполнять поиск по заданным последним параметрам (ключевым словам).

Нередко привлекаются также и специалисты наряду с экспертами. Это необходимо в том случае, если в рамках исследования встречается информация, для понимания которой требуются специальные познания (это например, экономика, бухгалтерия).

2. От эксперта требуют дать правовую оценку.

Эта ошибка напрямую связана с предыдущей. В таком случае эксперт будет выходить за пределы своих полномочий, а экспертное заключение лишится статуса доказательства. На практике техника исследуется с использование следующей высокотехнологичной криминалистической техники:

1. Аппаратно-программный комплекс «Мобильный Эксперт Криминалист» (рисунок 1-3) или «UFED».

Данное техническое средство направлено на восстановление удаленных данных. Это поможет определить, какие подготовительные действия были совершены, какие были попытки сокрытия следов преступления[1].

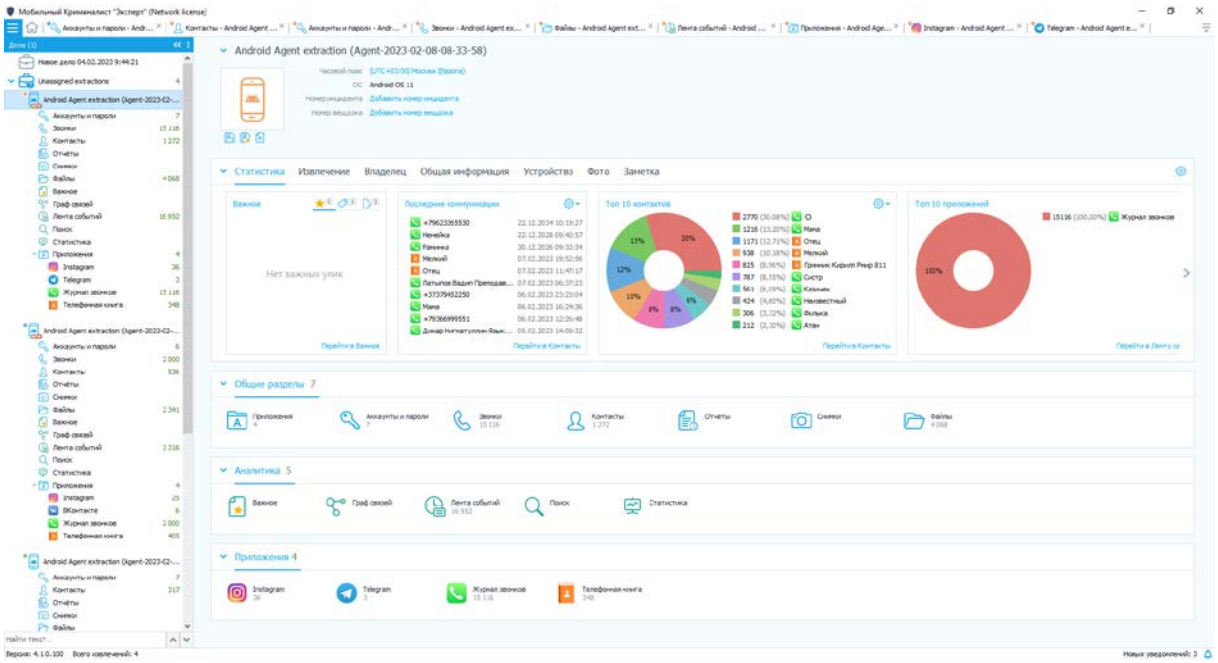

рис. 2.1. Результат извлечения информации с мобильного устройства «Xioami redmi note 8 pro»

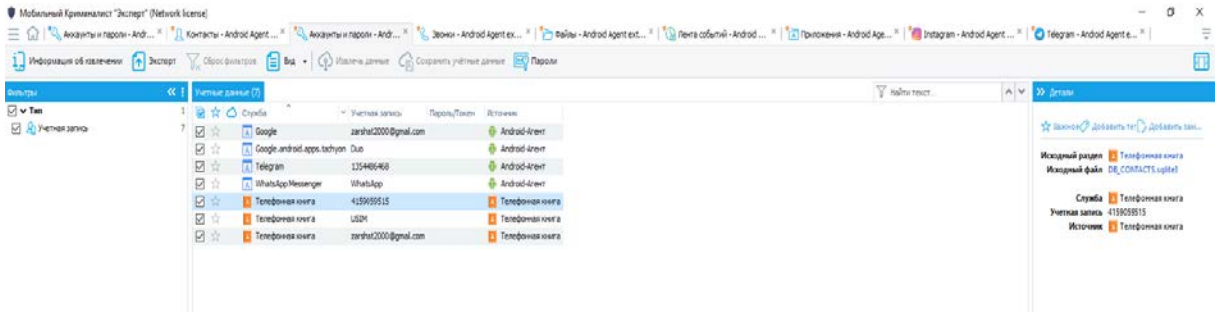

рис. 2.2. Учетные данные паролей с мобильного устройства «Xioami redmi note 8 pro»

[1] Скобелин С. Ю. Использование цифровых технологий при доказывании преступной деятельности // Российский следователь. 2019. № 3. С. 26-28.

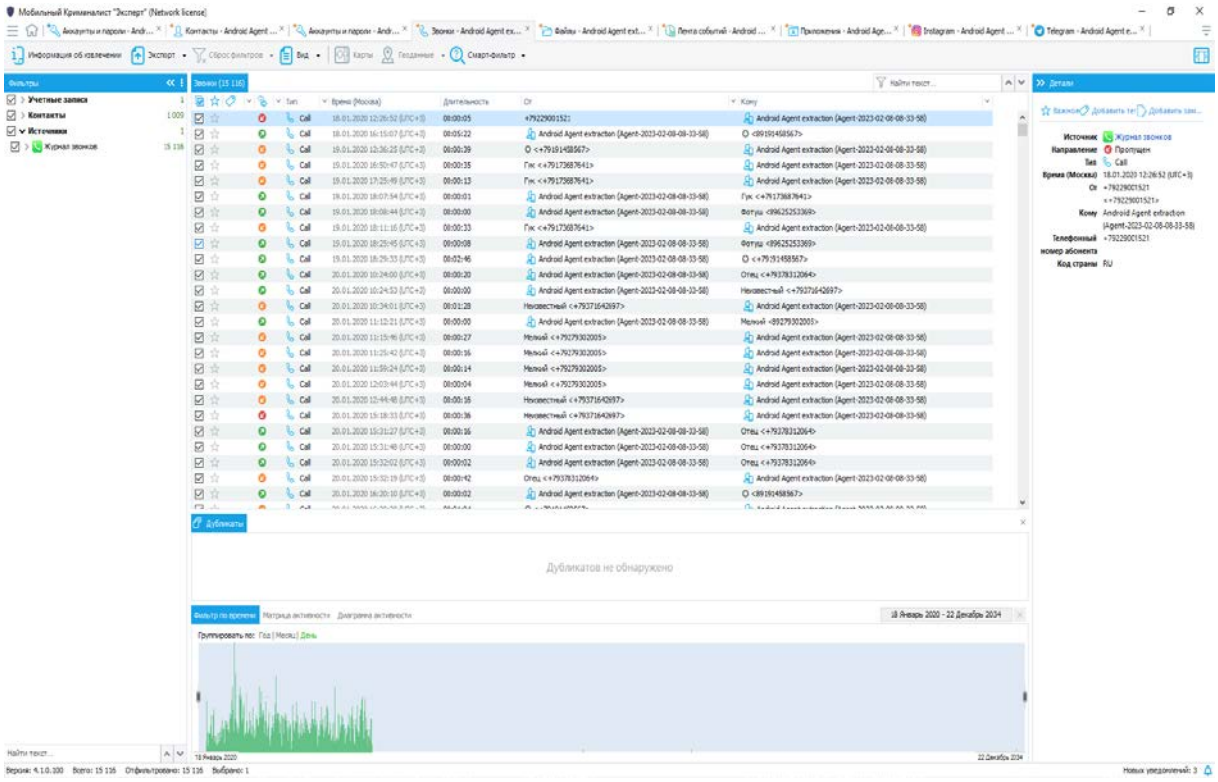

рис. 2.3. Учетные данные звонков с мобильного устройства «Xioami redmi note 8 pro»

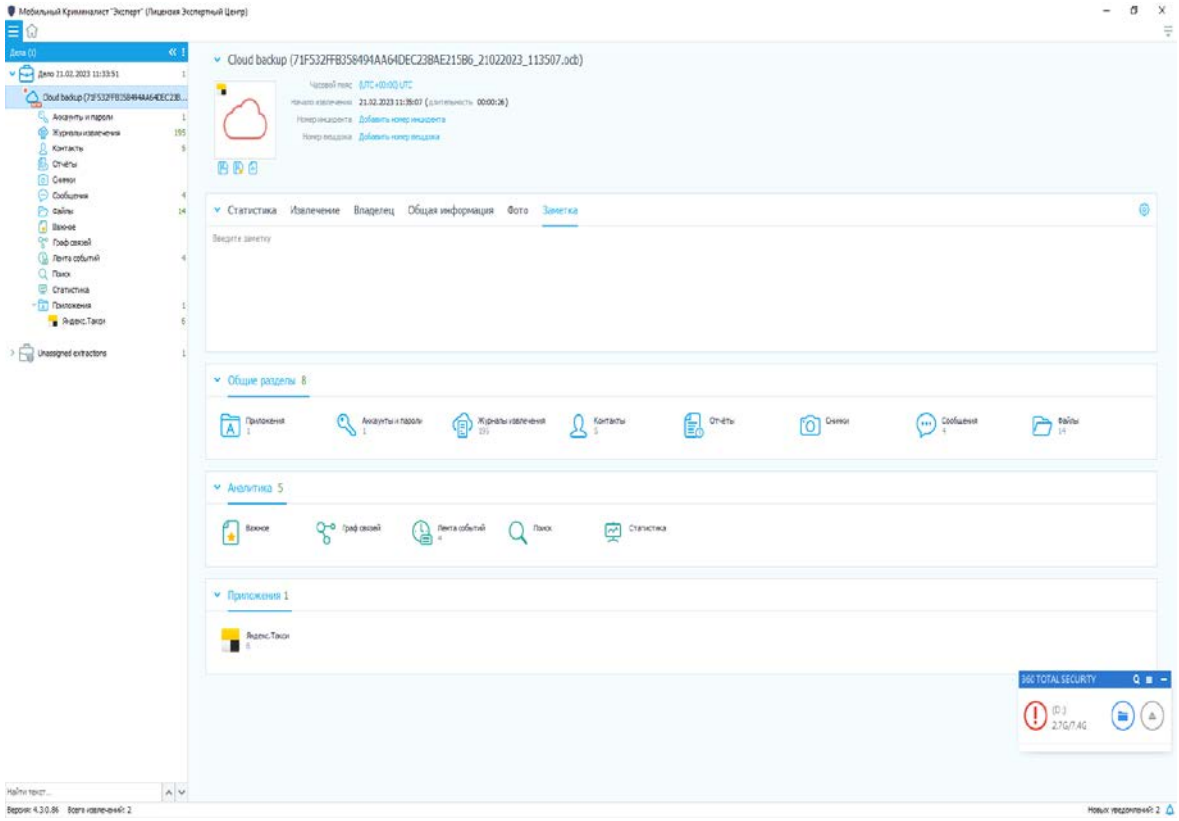

рис. 2.4. Общая информация данных, извлечённые с мобильного приложения «Yandex Taxi»

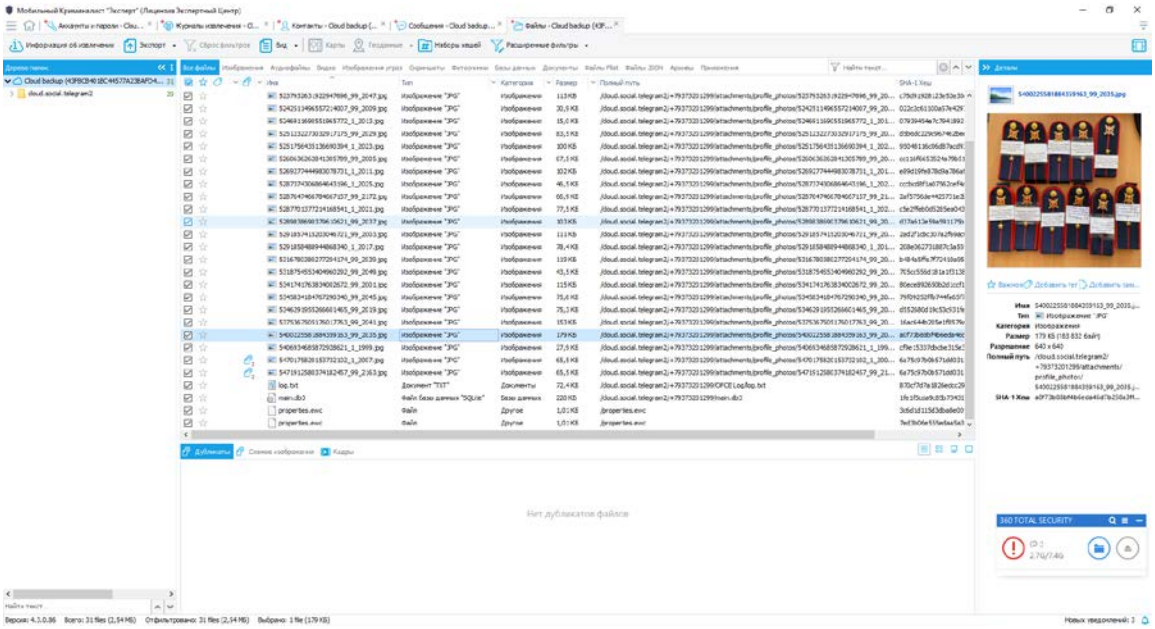

рис. 2.5. Данные изображений, извлечённых с мобильного приложения «Telegram»

2. XRY Logical.

Это более совершенный зарубежный аналог «Мобильного криминалиста». Данная программа дает возможность быстро извлекать, получать и восстанавливать данные прямо на месте преступления. Он также позволяет преодолевать системы безопасности и шифрования на заблокированных устройствах.

3. Встроенный приемный и передающий модуль GPS или ГЛОНАСС.

Устройство предоставляет возможность определить местонахождение пользователя в конкретную единицу времени. Также данное устройство сохраняет информацию о месте и времени соединения с роутером.

4. Медиафайлы.

На многих телефонах есть возможность узнать конкретное место, где было сделано фото или видео. Также можно использовать электронные транспортные карты, которые также указывают на время и местонахождение конкретного лица в заданную единицу времени. Получить данную информацию следователь может либо через оператора связи, либо непосредственно из электронного устройства, изъятого у лица.

5. Комплекс «ЛИС-М».

Данный комплекс позволяет найти конкретного пользователя, а также осуществляет поиск общих знакомых подозреваемого.

6. EnCase Forensic.

Эта программа проводит анализ информации и в итоге подготавливает отчеты о полученных результатах.

Таким образом, можно сделать вывод, что сам процесс криминалистического исследования компьютерной информации в РФ более-менее выверен. Имеется четкое понимание за какую область отвечает специалист, эксперт и следователь.

Специфичным является только круг вопросов, который ставятся перед экспертом для проведения исследования и в последующем дачи заключения, а также использование определенных средств и техники для проведения исследования.

К экспертам и специалистам предъявляются скорее общие требования с учетом особенностей сбора и фиксации компьютерной информации.

§ 2. Проблемы, связанные с криминалистическим исследованием компьютерной информации в целях раскрытия и расследования преступлений

Учитывая вышесказанное, нельзя не согласиться с актуальностью и необходимостью исследования компьютерной информации в целях раскрытия и расследования преступлений.

К такому же мнению пришел законодатель. Можно выделить две основные меры, которые необходимо соблюдать при решении вопроса об эффективном противодействии преступности в области высоких технологий:

1. Организационные меры.

Это меры, направленные на организацию и корректировку процесса работы, в том числе подразумевающее создание отдельных подразделений, техническое оснащение этих подразделений, повышение квалификации сотрудников.

В ходе выполнения выпускной квалификационной работы был проведен опрос среди экспертов (в количестве 10 человек) экспертно-криминалистического центра (далее - ЭКЦ) МВД по Республике Башкортостан (ПРИЛОЖЕНИЕ 2). Перед экспертами были поставлены следующие вопросы: 1) Какие типичные ошибки допускают следователи при назначении судебных экспертиз, объектами которых являются компьютерная информация и техника? 2) Какие существуют иные причины, препятствующие своевременному и полному проведению назначенных экспертиз, объектами которых являются компьютерная информация и техника? Результат опроса показал следующие причины, затрудняющие проведение вышеперечисленных экспертиз:

1) Неверное наименование экспертизы – 10 экспертов.

В соответствии с приказом МВД России №511 от 29.06.2005 г. «Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации» в системе органов Внутренних дел Российской Федерации есть только «Судебная компьютерная экспертиза» (в ЭКЦ МВД России не проводятся программно-технические, компьютерно-технические, программно-аналитические судебные экспертизы). В связи с этим, вопросы, связанные с работоспособностью, с техническими характеристиками, механизмами воздействия в ЭКЦ не решаются, исследуется только информация на различных носителях (жесткие диски, карты памяти, флеш-накопители, мобильные телефоны);

2) «Шаблонность» вопросов, которые ставят перед экспертом без учета конкретной ситуации – 8 экспертов. Сроки производства судебных компьютерных экспертиз часто увеличиваются в связи с тем, что инициаторы исследования до назначения экспертиз не консультируются с экспертами по правильной формулировке вопросов. В связи с этим часто выносятся вопросы, выходящие за пределы компетенции экспертов, или вопросы, решение которых занимает продолжительное время и при этом не имеет отношение к сути уголовного дела;

3) Избыточность объектов с постановкой вопросов, по каждому из них вне зависимости от связи с делом – 4 эксперта. На каждый объект, то есть на системные блоки, накопители на жестких магнитных дисках, ноутбуки, необходимо выносить отдельные постановления или отношения, чтобы в последствии при производстве экспертизы на каждый объект оформлялось отдельное заключение, поскольку на производство многообъектных экспертиз затрачивается больше времени, выводы перегружаются описанием информации с разных объектов и тяжелы для восприятия, а также могут быть допущены технические ошибки при оформлении экспертиз из-за перегруженности. Кроме того, не на каждом вещественном доказательстве может находиться нужная информация. В таком случае в последствии только одна экспертиза будет иметь значение для следствия, и она не будет перегружена описанием других объектов, что существенно затрудняет производство экспертизы, поиск информации, структурирование обнаруженной информации, оформление и дальнейшее восприятие данного заключения при ознакомлении, сортировку на каком объекте какая информация обнаружена);

4) Несвоевременность назначения экспертиз, доставки объектов в экспертное учреждение; несвоевременный ответ на запросы эксперта – 10 экспертов. Между изъятием и назначением экспертизы зачастую проходит значительное время от нескольких месяцев. В связи с этим, после назначения экспертизы оказывается, что сроки расследования преступления, как правило, уже заканчиваются и оказывается давление на экспертов на ускорение производства, при этом сроки производства других материалов, находящихся в очереди у экспертов, смещаются. Зачастую проходит значительное время после того, как инициатор выносит постановление до момента, когда постановление поступает в ЭКЦ, что снова сказывается на сроках;

5) Волокита в получении заключения выполненной экспертизы и объектов исследования – 3 эксперта;

6) Нехватка в ЭКЦ места для складирования вещественных доказательств – 3 эксперта. В связи с этим, из крупногабаритных объектов (системных блоков) необходимо извлекать накопители на жестких магнитных дисках (в обиходе винчестеры или жесткие диски). Для этого не нужно специальных познаний и данная процедура может производиться после основного изъятия дополнительным осмотром в кабинете инициатора исследования в присутствии понятых.

рис. 2.4 Результат опроса

На основе результата проведенного опроса, предлагаю перечень вопросов к вышеуказанным экспертизам:

1) Имеется ли на представленных на исследование объектах (перечень объектов) файлы, содержащие следующие ключевые выражения: (перечень ключевых выражений)?

2) Имеется ли на представленных на исследование объектах (перечень объектов) файлы, схожие по содержимому с представленными на исследование копиями документов (документов перечень)?

3) Имеются ли на представленных на исследование объектах файлы, содержащие изображения билетов Банка России?

4) Имеются ли на представленных на исследование объектах (перечень объектов) сведения о посещении иформационно-телекоммуникационной сети «Интернет»?

5) Имеются ли на представленных на исследование объектах (перечень объектов) сведения о переписки с использованием программ обмена сообщениями?

6) Имеются ли на представленных на исследование объектах файлы, содержащие изображение половых органов человека?

7) Имеются ли на представленных на исследование объектах (перечень объектов) программные продукты, атрибутирующие себя как (дать перечень наименований атрибутов)?

8) Имеются ли файлы, детектируемые антивирусной программой?

Необходимо отметить, что данный список не является исчерпывающим. В нем отражен перечень основных вопросов, которые ставятся перед экспертом при типичных фабулах преступлений рассматриваемой категории. В зависимости от ситуации он будет дополнен следователем иными вопросами.

2. Правовые меры.

Это меры, направленные на правовую регламентацию деятельности в сфере компьютерной криминалистики, подразумевающее составление отдельных правовых актов, правовую основу деятельности уполномоченных органов.

Были внесены изменения в ряд законодательных актов, в частности, Федеральным законом от 06.07.2016 № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» было указано дополнить ст. 6 ФЗ

«Об оперативно-розыскной деятельности» новым оперативно-розыскным мероприятием – получение компьютерной информации[1].

Несмотря на, несомненно, благие намерения, данное нововведение породило ряд вопросов. В частности, появилась необходимость законодательного закрепления понятия каждого оперативно-розыскного мероприятия. Связано это с тем, что такое оперативно-розыскное мероприятие, как получение компьютерной информации обладает специфичным названием, из которого ясно не следует, в чем будет заключаться суть данного мероприятия. Этим вопросом пришлось заниматься специалистам, занимающимся проблемами оперативно-розыскной деятельности[2].

Следует отметить, что с ст. 23 Конституции РФ закреплено, что, каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну. Также каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Данные права могут быть ограничены только на основании судебного решения[3].

В ст. 5 ФЗ «Об оперативно-розыскной деятельности» дополнительно подчеркивается, что «органы (должностные лица), осуществляющие оперативно-розыскную деятельность, при проведении оперативно-розыскных мероприятий должны обеспечивать соблюдение прав человека и гражданина на неприкосновенность частной жизни, личную и семейную тайну…».

---

[1] О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности: федер. закон от 06 июля 2016 № 374-ФЗ // Официальный интернет-портал правовой информации. URL:http://www.pravo.gov.ru/ (дата обращения: 07.01.2023).

[2] Налбандян Р. Г. Получение компьютерной информации как новая категория оперативно-розыскного законодательства // Проблемы экономики и юридической практики. 2018. № 1. С. 137-144.

[3] Конституция Российской Федерации : принята всенародным голосованием 12 декабря 1993 года с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ // Официальный интернет-портал правовой информации : URL: http://www.pravo.gov.ru (дата обращения: 07.01.2023).

Часто при проведении исследований компьютерной информации может возникнуть конфликт между защитой базовых прав человека и поиском истины и справедливости по делу.

Одной из самых основных проблем является недостаточность методических рекомендаций для уполномоченных лиц по производству криминалистических исследований компьютерной информации. В России почти полностью отсутствует какое-либо детализированное регулирование данной сферы, по большей части представлена обобщенная информация. Данный факт значительно усложняет работу экспертам и следователям.

В этом случае необходимо обратиться к зарубежному опыту, так как там имеется довольно подробное правовое регулирование компьютерной криминалистики.

В Великобритании в 2007 г. было принято «Техническое руководство по хранению, воспроизведению и удалению цифровых изображений». А в 2010 г. было принято «Практическое руководство по собиранию компьютерных доказательств». В 2014 году разработано и принято Практическое руководство при работе с цифровыми следами преступлений. В этом приложении рассматриваются функции цифровой криминалистики для идентификации, изъятии, сохранении, расследовании, оценки, отчетности и сохранности данных, извлеченных цифровых данных из стационарных и мобильных устройств. В этом руководстве излагаются методы работы с цифровой информацией, ее фиксация, соблюдение необходимых ограничений, обеспечение достоверности извлекаемой информации. В руководстве по анализу сайтов, местоположения абонентов даются рекомендации по получению необходимой доказательственной информации из технических устройств и соответствующих провайдеров связи, обработке этих данных, часто в сочетании с данными, полученными во время радиочастотной

фиксации; представление этих данных в виде карт и таблиц либо с фактическим, либо экспертным отчетом[1].

В данных документах указаны базовые принципы обращения с электронными доказательствами.

Многие организации предпринимают попытки как-то стандартизировать работу экспертов, специалистов и криминалистов в области исследования компьютерной информации, однако пока безрезультатно. На данный момент не принято каких-либо стандартов в этой области.

В то же время создание единого стандарта поспособствовало бы совершенствованию компьютерной криминалистики в целом[2].

При определении наиболее проблемных сфер в исследовании компьютерной информации нельзя обойти стороной работу экспертов. Нередко следователи ставят перед экспертом прямой вопрос, кто является автором или изготовителем компьютерной информации? В то же время сейчас не существует на столько проработанных методик и средств исследования, для ответа на подобные вопросы. Некоторые авторы предлагают использовать методики, используемые в других направлениях криминалистики.

Важно также заметить, что пока невозможно идентифицировать человека по кодовым средствам, даже по электронной цифровой подписи. Основной причиной является отсутствие непосредственной связи между кодовым средством и личностью человека[3].

Определенные сложности для экспертов вызывает необходимость решения проблемы преодоления защиты компьютера. При этом защита может функционировать на разных стадиях загрузки компьютера.

Ещё одной проблемой можно назвать смешение понятий идентифицируемого и идентифицирующего объекта при исследовании

---

[1] Code of Practice and conduct: Digital forensics-Cell Analysis. 2016. // https://www.gov.uk/government/collections/forensic-science-providers-codes-of-practice-and-conduct (дата обращения: 10.01.2023).

[2] Пастухов П. С. О необходимости развития компьютерной криминалистики // Пермский юридический альманах. 2018. № 1. С. 450-460.

[3] Яблоков Н. П. Криминалистика: Учебник, 3-е изд. М.: Юрайт, 2023. С. 204.

компьютерной информации. Проблемы в данном вопросе возникают при сопоставлении информации в электромагнитной форме с информацией на бумажном носителе. Информация на этих носителях не тождественна.

В рассматриваемом случае возможно проведение либо классификационных, либо диагностических исследований с целью установления признаков двух разных объектов – информации, находящейся в форме электромагнитного поля и информации на бумажном носителе.

Таким образом, можно сделать вывод, что в сфере криминалистического исследования компьютерной информации имеется достаточно большое количество пробелов и не состыковок, начиная с отсутствия понятийного аппарата и заканчивая отсутствием методических рекомендаций для эффективной работы, в то время, как для других видов криминалистических исследований они созданы.

В то же время в РФ предпринимаются попытки разрешить данную ситуацию, вносятся изменения в ряд законодательных актов, однако пока эти действия не возымели должного эффекта.

ЗАКЛЮЧЕНИЕ

Согласно ст. 6 ФЗ «Об оперативно-розыскной деятельности», при осуществлении оперативно-розыскной деятельности проводится в частности такое оперативно-розыскные мероприятие как получение компьютерной информации.

Перед использованием компьютерной информации необходимо первоначально ее исследовать.

В то же время следует заметить, что в законе также отсутствует определение криминалистического исследования компьютерной информации. Следовательно, необходимо обратиться к доктринальным источникам.

Криминалистическое исследование компьютерной информации – это система научных положений, на основе которых разрабатываются отдельные приемы, методы и рекомендации по использованию компьютерных технологий и информации, содержащейся в них для раскрытия, расследования и предупреждения преступлений.

Так, криминалистическое исследование компьютерной информации по своему содержанию включает: поиск компьютерных данных и их восстановлении в случае удаления; обработку данных и вычленение информации, представляющей особое криминалистическое значение. Формирование электронных доказательств; анализ полученных данных и их использование в целях раскрытие и расследование преступлений.

Глобальной целью является поиск, фиксация, обработка и анализ компьютерной информации, которая в последующем будет использоваться как доказательство в суде.

В качестве функций компьютерной криминалистики можно назвать: познавательную, конструктивную, прогностическую.

В целом объектом криминалистического исследования компьютерной информации в целях раскрытия и расследования преступлений является непосредственно компьютерная информация.

В Примечании 1 ст. 272 УК РФ дается следующее определение данного понятия: «под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи».

Как можно заметить, данное определение не дает достаточной конкретизации, более того нам необходима привязка к цифровому, электронному характеру информации. В ФЗ № 149 от 27.07.2006 «Об информации, информационных технологиях и о защите информации» указывается, что компьютерная информация – это сведения, представленные в электронной форме. Важно заметить, что такая информация не может существовать без специальных приспособлений (электронно-вычислительной техники и электронных средств связи).

Компьютерная информация состоит всего из двух основных элементов: носитель информации, сама компьютерная информация (её содержание).

Если под объектом исследования подразумевается то, что непосредственно изучается в рамках конкретного направления, то предметом исследования является особая проблема, отдельные стороны объекта, его свойства и особенности, взаимосвязи.

Так, в предмет криминалистического исследования компьютерной информации входит:

1. Исследование процесса обработки и способов фиксации компьютерной информации.

2. Разработка и совершенствование криминалистической тактики и техники в указанной области. Создание новых способов и приемов поиска, фиксации и изъятия компьютерной информации.

Можно выделить следующие признаки компьютерной информации:

1. Компьютерная информация содержится на материальном носителе в виде кода, из чего следует, что она не доступна для человеческого восприятия.

2. Компьютерная информация не всегда привязана только к одному материальному носителю. Компьютерная информация может быть отделена от материального носителя без изменений.

3. Компьютерная информация может быстро создаваться, меняться, передаваться. Любой объём легко передаётся на любое расстояние по телекоммуникационным каналам связи компьютерных сетей.

4. Даже при изъятии информации с материального носителя она сохраняется в первоисточнике.

5. Компьютерная информация в некоторых случаях доступна для широкого круга пользователей.

Можно выделить две основные процессуальные формы проведения криминалистического исследования компьютерной информации:

1. С участием специалиста.

Специалист привлекается для осуществления действий, связанных с поиском, исследованием (по поручению следователя), фиксацией и изъятием компьютерной информации.

Специалист обладает специальными знаниями в указанной области, однако, если возникает риск утраты или изменения исследуемой информации, то уже привлекается эксперт. Также эксперт привлекается в целом при решении более сложных криминалистических задач.

На специалиста в сфере компьютерной криминалистики возлагаются следующие функции: сбор данных; дублирование и сохранение данных; восстановление данных; поиск документов; преобразование мультимедиа; выступление в качестве экспертов свидетелей в суде; исследование компьютерных данных и так далее.

2. С участием эксперта.

Эксперт проводит компьютерно-техническую экспертизу, которая проводится как в отношении компьютерной информации, так и в отношении компьютерного оборудования.

Можно выделить следующие виды судебных экспертиз, назначаемых при изучении компьютерной информации:

1) Судебная аппаратно-компьютерная экспертиза.
2) Судебная программно-компьютерная экспертиза.
3) Судебная информационно-компьютерная экспертиза (данных).
4) Судебная компьютерно-сетевая экспертиза.

Эксперт – это специалист, дающий заключение при рассмотрении какого-либо вопроса. Эксперты обладают специальными знаниями в своей работе пользуются специфической профессиональной лексикой.

Следователь предварительно очерчивает круг вопросов, которые необходимо рассмотреть в рамках исследования. Эксперт просматривает все предоставленную ему информацию, однако в дальнейшем изучает только тот объем и только те файлы, которые дадут ответ на следственные вопросы.

В экспертном заключении должны указывать средства и методы, применимые при исследовании компьютерной информации в ходе проведения экспертизы.

Можно выделить две основные меры, которые необходимо соблюдать при решении вопроса об эффективном противодействии преступности в области высоких технологий:

1. Организационные меры.

Это меры, направленные на организацию и корректировку процесса работы, в том числе подразумевающее создание отдельных подразделений, техническое оснащение этих подразделений, повышение квалификации сотрудников.

Так, например, можно выделить список типичных ошибок следователей при назначении судебных экспертиз:

1) Неверное наименование экспертизы;
2) «Шаблонность» вопросов, которые ставят перед экспертом без учета конкретной ситуации.

3) Избыточность объектов с постановкой вопросов, по каждому из них вне зависимости от связи с делом.

4) Несвоевременность назначения экспертиз, доставки объектов в экспертное учреждение; несвоевременный ответ на запросы эксперта.

5) Волокита в получении заключения выполненной экспертизы и объектов исследования;

6) Нехватка в ЭКЦ для складирования вещественных доказательств.

2. Правовые меры.

Это меры, направленные на правовую регламентацию деятельности в сфере компьютерной криминалистики, подразумевающее составление отдельных правовых актов, правовую основу деятельности уполномоченных органов.

Также проблемным является то, что оперативно-розыскное мероприятие, как получение компьютерной информации обладает специфичным названием, из которого ясно не следует, в чем будет заключаться суть данного мероприятия.

Следует отметить, что часто при проведении исследований компьютерной информации может возникнуть конфликт между защитой базовых прав человека и поиском истины и справедливости по делу.

При определении наиболее проблемных сфер в исследовании компьютерной информации нельзя обойти стороной работу экспертов. Нередко следователи ставят перед экспертом прямой вопрос, кто является автором или изготовителем компьютерной информации? В то же время сейчас не существует настолько проработанных методик и средств исследования, для ответа на подобные вопросы.

Одной из самых основных проблем является почти полное отсутствие каких-либо методических рекомендаций для уполномоченных лиц по производству криминалистических исследований компьютерной информации.

В данном случае необходимо обратиться к зарубежному опыту, в частности к опыту Великобритании и США, так как там имеется довольно подробное правовое регулирование компьютерной криминалистики.

При проведении данного исследования были рассмотрены только некоторые проблемные аспекты криминалистического исследования компьютерной информации. Технический прогресс не стоит на месте, в этой связи данный проблемные вопросы требуют дальнейшей детальной проработки.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

I. Нормативные правовые акты и иные официальные документы

1. Конституция Российской Федерации : принята всенародным голосованием 12 декабря 1993 года с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ // Официальный интернет-портал правовой информации : URL: http://www.pravo.gov.ru (дата обращения: 07.01.2023).

2. Уголовный кодекс Российской Федерации от 13 июня 1996 № 63-ФЗ (ред. от 29 декабря 2022 №586-ФЗ) // Официальный интернет-портал правовой информации. URL:http://www.pravo.gov.ru/ (дата обращения: 02.02.2023).

3. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (с посл. изм. и доп. от 17 февраля 2023г. № 30-ФЗ) // Официальный интернет-портал правовой информации. URL:http://pravo.gov.ru/ (дата обращения: 07.01.2023).

4. Об оперативно-розыскной деятельности: федер. закон Рос. Федерации от 12 августа 1995 № 144-ФЗ (ред. от 28.12.2022) // Официальный интернет-портал правовой информации. URL:http://www.pravo.gov.ru/ (дата обращения: 07.01.2023).

5. О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности: федер. закон Рос. Федерации от 06 июля 2016 № 374-ФЗ // Официальный интернет-портал правовой информации. URL:http://www.pravo.gov.ru/ (дата обращения: 07.01.2023).

6. Об информации, информационных технологиях и о защите информации: федер. закон Рос. Федераци от 27 июля 2006 № 149-ФЗ (ред. от 29 декабря 2022 №604-ФЗ) // Официальный интернет-портал правовой информации. URL:http://www.pravo.gov.ru/ (дата обращения: 02.02.2023).

7. О государственной судебно-экспертной деятельности в Российской

Федерации: федер. закон Рос. Федерации от 31 мая 2001 № 73-ФЗ // Официальный интернет-портал правовой информации. URL:http://www.pravo.gov.ru/ (дата обращения: 05.02.2023).

8. О государственной тайне: закон РФ от 21 июля 1993 № 5485-1 (ред. от 05 декабря 2022 №498-ФЗ) // Официальный интернет-портал правовой информации. URL:http://www.pravo.gov.ru/ (дата обращения: 02.02.2023).

9. Модельный закон «Об оперативно-розыскной деятельности». Принят на двадцать седьмом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ (постановление №27-6 от 16 ноября 2006 года) // Информационная система «КОНТИНЕНТ». URL:http://continent-online.com/Document/?doc_id= 30161811 (дата обращения: 07.01.2023).

10. О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»: постановление Пленума Верховного Суда РФ от 15 декабря 2022 № 37 // Официальный сайт Верховного суда Российской Федерации. URL: https://vsrf.ru/documents/own/31913/ (дата обращения: 02.02.2023).

11. Об утверждении Стратегии развития отрасли информационных технологий в Российской Федерации на 2014 – 2020 годы и на перспективу до 2025 года: распоряжение Правительства РФ от 01 ноября 2013 № 2036-р (ред. от 18 октября 2018) // Официальный интернет-портал правовой информации: URL:http://www.pravo.gov.ru/ (дата обращения: 02.02.2023).

II. Учебная, научная литература и иные материалы

1. Алексанин А. С. О понятии и содержании оперативно-розыскного мероприятия «получение компьютерной информации» // Правовое государство: теория и практика. 2018. № 1 (51). С. 153-159.

2. Волеводз А. Г. Компьютерная информация как объект криминалистического следоведения // Криминалистическая техника: Учебник /

Отв. ред. И.М. Балашов, рук. кол. С.В. Маликов. М.: Юрлитинформ, 2008. 381 с.

3. Гриб Г. В., Тюнис И. О. Криминалистика и цифровые технологии // Российский следователь. 2019. № 9. С. 99–105.

4. Дерюгин Р. А. Киберпреступность в России: современное состояние и актуальные проблемы // Вестник Уральского юридического института МВД России. 2019. № 2. С. 46–49.

5. Долженко Н. И., Ярощук И. А. Киберпреступность как одна из ключевых проблем современности // Legal Concept. 2020. № 1. С. 152–157.

6. Егоров Н. Н. Криминалистика: учебник и практикум для вузов, 2-е изд., испр. и доп. / Н. Н. Егоров, Е. П. Ищенко. М.: Издательство Юрайт, 2023. 613 с.

7. Ищенко П. П. Актуальные проблемы судебно-экспертного обеспечения расследования организованной преступной деятельности // Пролог: журнал о праве. 2019. № 4. С. 40–45.

8. Карпова Д. Н. Киберпреступность: глобальная проблема и ее решение // Власть. 2014. № 8. С. 46–50.

9. Климова Я. А. Цифровая криминалистика: перспективы развития // Вестник Волгоградской академии МВД России. 2020. № 4. С. 128–132.

10. Кондратьев Ю. А., Сафонов О. М. Особенности толкования термина «компьютерные технологии» для целей уголовно – правового регулирования // Конвенционные начала в уголовном праве: материалы Международной научно-практической конференции (Москва, 22 ноября 2013 года). М.: РПА Минюста России. С. 165–168.

11. Криминалистика в 3 ч. Часть 1 : учебник для вузов, 2-е изд., испр. и доп. / Л. Я. Драпкин [и др.]. М.: Издательство Юрайт, 2023. 246 с.

12. Криминалистика в 5 т. Том 5. Методика расследования преступлений : учебник для вузов / И. В. Александров [и др.]. М.: Издательство Юрайт, 2022. 242 с.

13. Мицкевич А. Ф., Суслопаров А. В. 5. 3. Понятие компьютерной информации по российскому и зарубежному уголовному праву // Пробелы в российском законодательстве. Юридический журнал. 2010. № 2. С. 206-209.

14. Налбандян Р. Г. Получение компьютерной информации как новая категория оперативно-розыскного законодательства // Проблемы экономики и юридической практики. 2018. № 1. С. 136-144.

15. Омелин В. Н. Оперативно-розыскные мероприятия и оперативно-розыскные действия: критерии разграничения // Закон и право. 2018. № 11. С. 132-134.

16. Пастухов П. С. О необходимости развития компьютерной криминалистики // Пермский юридический альманах. 2018. № 1. С. 450-460.

17. Полянская Е. П., Никоноров А. А. Информационное взаимодействие следователя со службами негосударственных организаций и подразделениями правоохранительных органов как основа успешного расследования преступлений в сфере высоких технологий // Вестник экономической безопасности. 2021. № 1. С. 49–51.

18. Расследование преступлений в сфере компьютерной информации и электронных средств платежа: учебное пособие для вузов / С. В. Зуев. М.: Издательство Юрайт, 2023. 243 с.

19. Россинская Е. Р., Шамаев Г. П. Новый раздел криминалистики: криминалистическое исследование компьютерных средств и систем // Baikal Research Journal. 2015. Т. 6. № 1. С. 317-325.

20. Скобелин С. Ю. Использование цифровых технологий при доказывании преступной деятельности // Российский следователь. 2019. № 3. С. 26-28.

21. Смушкин А. Б. Цели, задачи и функции электронной цифровой криминалистики // Криминалистика: вчера, сегодня, завтра. 2020. № 1 (13). С. 103-107.

22. Яблоков Н. П. Криминалистика: Учебник, 3-е изд. М.: Юрайт, 2023. 239 с.

23. Code of Practice and conduct: Digital forensics-Cell Analysis. 2016. // https://www.gov.uk/government/collections/forensic-science-providers-codes-of practice-and-conduct (дата обращения: 10.01.2023).

III. Эмпирические материалы

1. Уголовное дело № 0003 // Арх. ОМВД России по Кармаскалинскому району РБ. Оп. 1. 145-149 л.

2. Уголовное дело № 0001 // Арх. ОМВД РФ по Уфимскому району РБ. Оп. 1. 101-110 л.

3. Уголовное дело № 0002 // Арх. ОМВД РФ по Уфимскому району РБ. Оп. 1. 134-142 л.

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

_____

(Подпись, Ф.И.О.)

ПРИЛОЖЕНИЕ 1

ФЕДЕРАЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
БАШКИРСКАЯ ЛАБОРАТОРИЯ СУДЕБНОЙ ЭКСПЕРТИЗЫ
МИНИСТЕРСТВА ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Р. Зорге ул., д.60, Уфа, 450054, тел., факс (347) 248-73-63, E-mail: bash-lse@mail.ru

ЗАКЛЮЧЕНИЕ ЭКСПЕРТА
по КУСП

«20» декабря 2022 г.

Экспертиза начата: в 14 часов 00 минут, 21 декабря 2021 г.
Экспертиза окончена: в 15 часов 30 минут, 20 января 2022 г.

21 декабря 2021 года в ФБУ Башкирская ЛСЭ Минюста России с постановлением следователя СО ОМВД России по Кармаскалинскому району старшего лейтенанта юстиции от 15 декабря 2021 года для производства первичной судебной компьютерно-технической экспертизы предоставлен «полимерный пакет в котором находится системный блок черного цвета №ART ФФ14».

Производство первичной компьютерно-технической экспертизы поручено старшему государственному судебному эксперту специализированного экспертного отдела по производству экспертиз и экспертных исследований по делам, связанным с проявлением экстремизма, , имеющему высшее образование по специальности «Математика», аттестованному на право самостоятельного производства экспертиз по экспертной специальности 21.1 «Исследование информационных компьютерных средств», свидетельство Минюста России № 01035, стаж экспертной работы по указанной специальности с 2016 года.

Об ответственности за дачу заведомо ложного заключения по статье 307 Уголовного кодекса Российской Федерации государственный судебный эксперт Любаев Р.Е. предупрежден 21.12.2021.

На разрешение эксперта поставлены следующие вопросы:

«- Имеются ли на представленном системном блоке черного цвета №ART ФФ14 вредоносные программы?»

«- Если да какие характеристики они имеют?».

Визуальным осмотром установлено, что целостность упаковки не нарушена, доступа к содержимому не имеется (фото № 1-3 в фототаблице к заключению эксперта).

Местом проведения экспертизы является ФБУ Башкирская ЛСЭ Минюста России.

Из постановления о назначении судебной компьютерно-технической экспертизы известно следующее:

«15.10.2021 в дежурную часть ОМВД России по Кармаскалинскому району поступило обращение 31.05.1966 г.р. проживающей по адресу: , о том, что 20.09.2021 произведен несанкционированный вход на сервер ООО ПХ «Аретемида», расположенный по адресу: В результате чего вся

информация, хранившаяся на сервере была повреждена вредоносной программой.
В ходе ОМП по адресу: [redacted]
изъят системный блок черного цвета №ART ФФ14, упакован в полимерный пакет и снабжен пояснительной надписью.

ИССЛЕДОВАНИЕ

Список литературы:

1. Производство судебно компьютерно-технической экспертизы: Часть I: Общая часть; Часть II: Диагностические и идентификационные исследования аппаратных средств: метод. пособие/Л.Г. Эджубов [и др.]; под ред. А.И. Усова. – М.: ГУ РФЦСЭ, 2009. - 80 с.
2. Производство судебной компьютерно-технической экспертизы: Часть III: Специализированный словарь компьютерной лексики для экспертов судебной компьютерно-технической экспертизы: метод. пособие / Л.Г. Эджубов [и др.]; под ред. А.И. Усова. – М.: ГУ РФЦСЭ, 2009. - 115 с.
3. Производство судебной компьютерно-технической экспертизы: Часть IV: Актуальные комплексные экспертные задачи: метод. пособие / Л.Г. Эджубов [и др.]; под ред. А.И. Усова. – М.: ГУ РФЦСЭ, 2011. - 296 с.
4. Производство судебной компьютерно-технической экспертизы: Часть V: Актуальные задачи исследования компьютерной информации: метод. пособие / Л.Г. Эджубов [и др.]; под ред. А.И. Усова. – М.: ГУ РФЦСЭ, 2011. - 271 с.
5. Усов, А.И. Судебно-экспертное исследование компьютерных средств и систем: основы методического обеспечения: учеб. пособие / А.И. Усов; под ред. Е.Р. Россинской. – М.: Экзамен: Право и закон, 2003. – 367 с.
6. Фридланд, А.Я. Информатика и компьютерные технологии: Основные термины: толк. слов. / А.Я. Фридланд, Л.С. Ханамирова, И.А. Фридланд. – 3-е изд., исправ. и доп. – М.: ООО «Издательство Астрель», 2003. – 272 с.

Термины, используемые в тексте заключения:

Дефект (порок, изъян) — 1) каждое отдельное несоответствие продукции установленным требованиям [3]; 2) изменение первоначальных свойств изделия (поражения) под влиянием негативных факторов, возникающее в сфере производства, обращения, в процессе эксплуатации и появляющееся в соответствующих признаках.

Файл образ — файл, несущий в себе полную копию содержимого и структуры файловой системы и данных.

Исследование проводилось на стендовом компьютере эксперта.

Аппаратная конфигурация: процессор Intel Xeon Gold 5115 CPU (2 процессора); системная плата ASUS WS C621E SAGE; ОЗУ 64 Гб DDR4; 2 НЖМД ST600VX001-2BD186 Объемом 6.0 TB; Samsung SSD 860 PRO 518 GB блокирующие запись информации на НЖМД и SSD Tableau Forensic Bridge.

Программная конфигурация:

- операционная система «Microsoft Windows 10 Pro»;
- ПП «Microsoft Office 2019» (набор офисных приложений);
- ПП «AccessData FTK Imager» (специализированное программное обеспечение для работы с образами);
- ПП «Dr.Web Security Space» (антивирусное программное обеспечение);
- ПП «Kaspersky Virus Removal Tool» (антивирусное программное обеспечение).

План исследования

Исследование проведено в следующей последовательности:

1. Внешний осмотр.
2. Подготовка объекта к исследованию.
3. Восстановление удаленной информации.
4. Проверка на наличие вредоносных программ (антивирусная проверка).

1. Внешний осмотр

Объект исследования – «системный блок черного цвета с инвентаризационным номером №ART ФФ14» упакован в пакет черного цвета. Упаковка имеет размеры 420x190x350 мм (длина – ширина – высота, измерения эксперта). На верхнюю сторону упаковки наклеен лист бумаги белого цвета, на котором имеются надписи и подписи выполненные рукописным способом красителями синего цвета, а также оттиск печати синего цвета. Остальные стороны не имеют опознавательных элементов (фото № 1-2 в фототаблице к заключению эксперта).

Внешний вид предоставленного на исследования системного блока черного цвета с наклеенными инвентаризационным номером №ART ФФ14 и пр. информацией представлен в Фототаблице к заключению эксперта на фото № 1-7.

Предоставленный на исследование объект исследования в корпусе черного цвета с серебристой окантовкой. Корпус имеет следы эксплуатационного воздействия в виде многочисленных царапин, потертостей. Исследуемый системный блок имеет размеры 420x190x350 мм (длина – ширина – высота, измерения эксперта).

Передняя панель системного блока имеет: привод для работы с оптическими дисками; кнопки включения, перезагрузки компьютера, 2 порта USB; разъем для подключения микрофона (розовый); разъем для подключения наушников и стерео колонок (светло-зеленый).

Задняя панель системного блока имеет основные разъемы. В основные разъемы входят: разъем блока питания; порт для подключения мыши/клавиатуры PS/2; DVI – порт; VGA порт (для подключения монитора); 6 портов USB; Ethernet порт; порты звуковой карты (розовый – для микрофона, светло-зеленый – для наушников и стерео колонок, светло-голубой – линейный аудиовход).

2. Подготовка объекта к исследованию

Средствами ПП «AccessData FTK Imager» с предоставленного системного блока были сняты побитовые копии, сохранённые в файл образ. Далее исследование проводилось с использованием полученного файл-образа.

3. Восстановление удаленной информации

Средствами ПП «R-STUDIO» с НЖМД объекта исследования (системного блока) были найдены удалённые файлы.

Дальнейшее исследование проводилось с учетом найденных файлов.

4. Проверка на наличие вредоносных программ (антивирусная проверка)

В результате антивирусной проверки системного блока были обнаружены программы, идентифицируемые как «программы которые могут быть использованы злоумышленником для нанесения вреда компьютеру или пользовательским данным» (рис.1-2).

- ПП «Kaspersky Virus Removal Tool» - 1 программа;
- ПП «Dr.Web Security Space» - 2 программы;

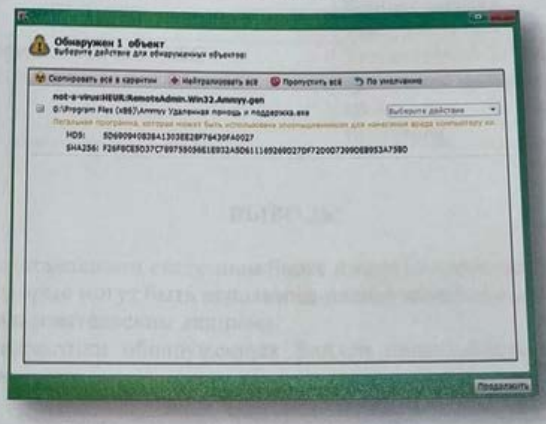

Рис. 1. Статистика антивирусной проверки исследуемого образа с НЖМД системного блока ПП «Kaspersky Virus Removal Tool».

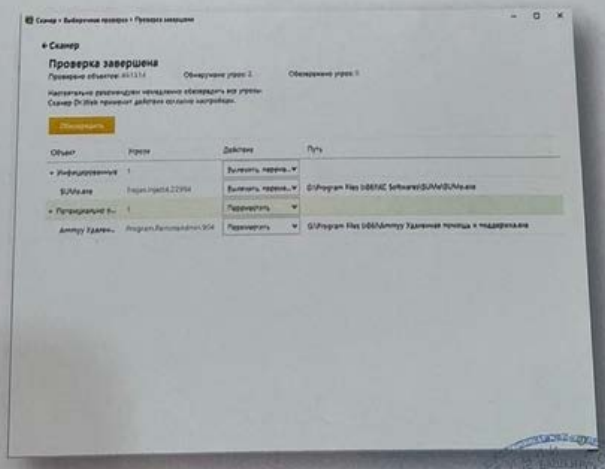

Рис. 2. Статистика антивирусной проверки исследуемого образа с НЖМД системн блока ПП «Dr.Web Security Space».

Описание вирусов даётся в соответствии с вирусной энциклопедией Dr.Web Security Space (таблица 1).

Таблица 1

№ п/п	Расположение и имя зараженного файла(-ов)	Название вредоносной программы и краткое описание
1	\Program Files (x86)\Ammyy Удаленная помощь и поддержка.exe	Program.RemoteAdmin.904 потенциально опасная программа на основе технологии проникновения и управления удаленным компьютером.
2	\Program Files (x86)\KC Softwares\SUMo\SUMo.exe	Trojan.Inject4.22994 семейство троянских программ, внедряющих свой код в память других программ.

ВЫВОДЫ

1. На представленном системном блоке имеются программы, идентифицируемые как «программы, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или пользовательским данным».
2. Характеристики обнаруженных файлов представлены в исследовательской части данного заключения.

Приложение к заключению:
- фототаблица с 7 иллюстрациями на 8 листах;

ПРИЛОЖЕНИЕ 2

Уважаемый респондент!

Кафедра криминалистики Федерального государственного казенного образовательного учреждения высшего образования «Уфимский юридический институт МВД России» проводит исследование по теме «Криминалистическое исследование компьютерной техники и информации в целях раскрытия и расследования преступлений».

Просим Вас принять участие в опросе и высказать своё мнение по вопросам, касающимся криминалистического исследования компьютерной информации и техники. Внимательно ознакомьтесь с вопросами.

Мы выражаем Вам искреннюю благодарность за время, которое Вы уделяете для ответа на вопросы анкеты. Опрос анонимный, материалы будут использоваться в обобщённом виде.

Вопросы:

1) Какие типичные ошибки допускают следователи при назначении судебных экспертиз, объектами которых являются компьютерная информация и техника?

2) Какие существуют иные причины, препятствующие своевременному и полному проведению назначенных экспертиз, объектами которых являются компьютерная информация и техника?

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

_____ Д.Д. Асфандиярова