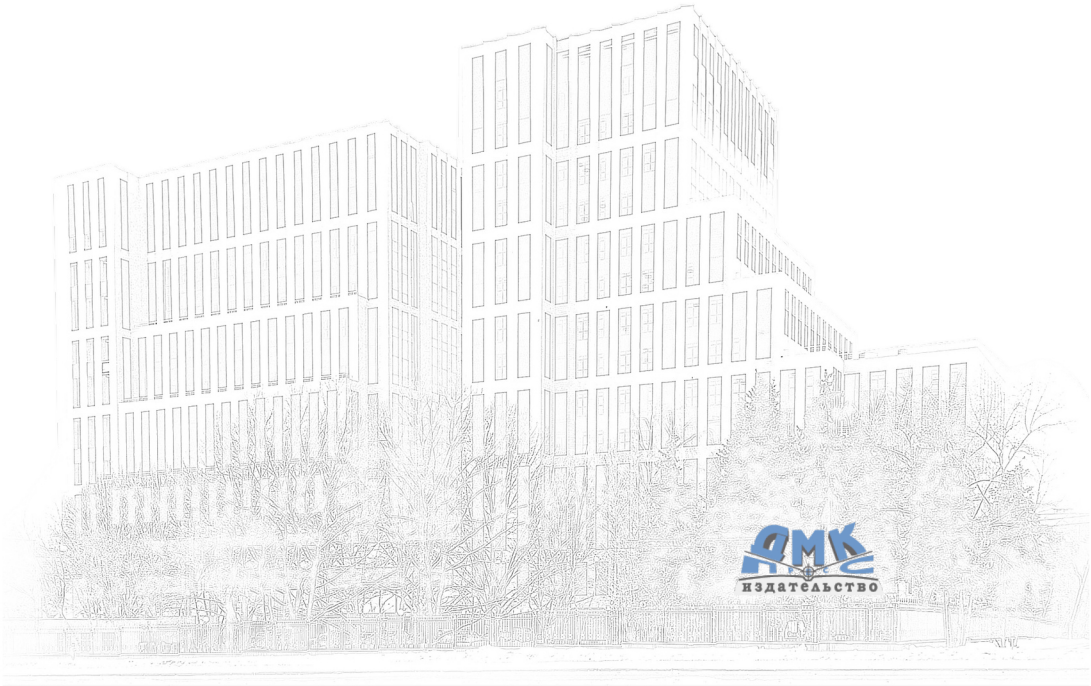
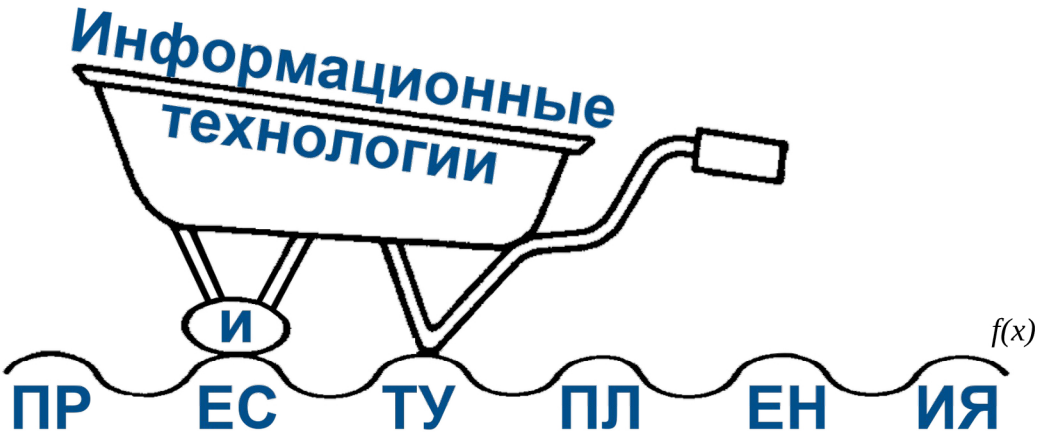
С. С. Минаков П. В. Закляков



Информационные технологии и преступления

(взгляд на цифровые следы со стороны следствия)

В нашу жизнь довольно быстро вошли информационные технологии. На страницах они рассматриваются как орудие совершения традиционных преступлений, в первую очередь не связанных с самими информационными технологиями. Содержимое книги полно и ярко описывает взгляд со стороны следствия на происходящее, с освещением сопутствующих проблем, а также возникающих при этом комичных жизненных ситуаций.



ISBN 978-5-93700-194-8

С.С.Минаков, П.В.Закляков

Информационные технологии и преступления

(взгляд на цифровые следы со стороны следствия)

Учебное пособие

Данное учебное пособие обладает большой практической значимостью, может быть интересно студентам вузов обучающимся по укрупнённым специальностям «Юриспруденция» и «Информационная безопасность», включая специальности: «Безопасность информационных технологий в правоохранительной сфере», «Правовое обеспечение национальной безопасности», «Правоохранительная деятельность», «Судебная экспертиза», а также аспирантам и молодым учёным, экспертам и работникам правоохранительных органов, специализирующимся на противодействии уголовной преступности в сфере информационных технологий.

ДМК ПРЕСС
ИЗДАТЕЛЬСТВО
Москва, 2023

УДК 343:004.9 (075.8)
ББК 67.408я73
М61

Рецензенты:

Михайленко Н. В. – доцент кафедры противодействия преступлениям в сфере информационно-телекоммуникационных технологий Московского университета МВД России им. В.Я. Кикотя (МосУ МВД РФ), кандидат юридических наук, доцент.

Семикаленова А. И. – доцент кафедры судебных экспертиз Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), кандидат юридических наук, доцент.

Терентьев Р. А. – начальник Управления международного сотрудничества МВД России.

Минаков С. С., Закляков П. В.

М61 Информационные технологии и преступления: учеб. пособие – М.: ДМК Пресс, 2023. – 160 с.

ISBN 978-5-93700-194-8

В данном пособии приводится взгляд на цифровые следы со стороны следствия, в фокусе которого поэтапно изложены наиболее важные аспекты доказывания по уголовным делам, связанным с использованием информационных технологий, рассмотрены понятия и предмет доказывания и доказательств, приведена их классификация и виды, описаны вещественные и цифровые доказательства, показана значимость привлечения специалиста, отмечены проблемы объективного вменения и казуса, связанные со спецификой техногенного «виртуального» мира.

Значительная доля материала посвящена организации и особенностям сбора и фиксации доказательств по уголовным делам, связанным с использованием информационных технологий, описанию вариативности тактик следствия и процессуальных мероприятий по доказыванию и проверке доказательств.

Отдельно рассмотрены вопросы участия специалиста (эксперта) и представления ими доказательств в ходе судебных заседаний по уголовным делам, связанным с использованием информационных технологий. Приведены разнообразные случаи из жизни.

УДК 343:004.9 (075.8)
ББК 67.408я73

ISBN 978-5-93700-194-8

Любимой жене, дочери и сыну
с благодарностью за поддержку и понимание,
проявленные ко мне при написании данной работы.
С. Минаков

Введение

В нашу жизнь довольно быстро вошли информационные технологии.

Согласно определению «ЮНЕСКО»: *информационные технологии (ИТ) – это комплекс взаимосвязанных научных, технологических, инженерных дисциплин, изучающих методы эффективной организации труда людей, занятых обработкой и хранением информации; вычислительную технику и методы организации и взаимодействия с людьми и производственным оборудованием, их практические приложения, а также связанные со всем этим социальные, экономические и культурные проблемы. Сами ИТ требуют сложной подготовки, больших первоначальных затрат и наукоёмкой техники. Их внедрение должно начинаться с создания математического обеспечения, моделирования, формирования информационных хранилищ для промежуточных данных и решений.*

Как видно, за столь ёмким определением скрывается большое число проблем и вопросов, требующих изучения и решения. Несомненно, это работа не только для технических специалистов. Свою лепту предстоит вложить юристам, экономистам, социологам, политологам, маркетологам и др.

Легко догадаться, что решение современных проблем управления обществом, как и лидерство Российской Федерации на мировой арене, непосредственно связаны с развитием информационных процессов в нашей стране и за её пределами.

Отставание в понимании, так и применении в своей работе, информационных технологий у таких работников как следователь, криминалист, прокурор, судья, оперативный работник ведёт к тому, что сложившийся баланс вокруг уголовного права, как отрасли права, представляющей собой совокупность норм, определяющих преступность и наказуемость деяний, опасных для господствующей системы общественных отношений, меняется в сторону уменьшения защищённости личности, общества и государства от криминала.

Данное учебное пособие есть маленький кирпичик в фундаменте знаний доказывания по уголовным делам с учётом меняющихся реалий. Авторы издания скорее рассматривают информационные технологии как орудие совершения традиционных преступлений, в первую очередь не связанных с самими информационными технологиями. Если быть более точными данное издание есть взгляд на цифровые следы (как следствие развития информационных технологий) со стороны следствия.

Перед тем как Вы, дорогой читатель, перейдёте от введения к главам нашего учебного издания хочется у Вас спросить, а «*Что поменялось примерно за последние 20 лет при совершении преступлений?*».

Узнать Ваши ответы, поддержать их или возразить, то есть погрузиться в дискуссию с Вами, мы не сможем, если только Вы не напишите письмо на электронную почту издательства *dmkpress@gmail.com* с просьбой передать его содержимое авторам. Поэтому, мы приведём одну из возможных точек зрения, которая нам оказалась близкой в момент написания данного пособия, а Вы сможете лучше понять как развивались мысли авторов по мере изложения всего последующего текста.

Глава 1. Совершение преступлений

Общетеоретические вопросы и актуальные проблемы доказательств и доказывания по уголовным делам о преступлениях, совершённых с использованием информационно-телекоммуникационных технологий.

Обсудим вопрос, заданный во введении: «Что поменялось примерно за последние 20 лет при совершении преступлений?» и попробуем на него ответить.

Прежде всего необходимо убедиться, что читатель и авторы под заданным вопросом понимают одно и тоже, пользуются общими терминами, одинаковыми понятиями. Соответственно, профессионалы и специалисты со стажем, дабы не читать трюизмы могут пропустить первую главу и перейти сразу ко второй. Всем остальным желательно просмотреть содержимое хотя бы «по диагонали», сверившись с терминологией (аксиоматикой) используемой авторами.

Договоримся о следующем:

Предметом регулирования уголовного права являются уголовно-правовые отношения, – специфические общественные отношения, возникающие между государством и лицом, нарушившим уголовно-правовой запрет. Случаи использования уголовно-правового дозволения причинять вред при наличии определённых обстоятельств (например, при обоснованном риске или при исполнении приказа и т. п.) не рассматриваются.

Уголовное право регулирует главным образом нежелательные для общества (негативные) отношения, возникающие в связи совершением преступлений. Таким способом, оно охраняет от преступных посягательств позитивные отношения, в существовании и развитии которых общество заинтересовано. Регулирование в этих областях производится другими отраслями права (конституционным, административным, предпринимательским, финансовым и т. д.).

Такие положения уголовного права, как: принципы уголовного права, действие уголовного закона в пространстве и во времени, понятие преступления, объект преступления, субъект преступления, субъективная и объективная стороны преступления, соучастие в преступлении, обстоятельства, исключающие преступность деяния и т. п. учитываются, но не рассматриваются подробно, в предположении, что читатель с ними уже знаком.

Предполагается, что совершено некоторое деяние (собственно преступное проявление человека), выражающееся в действии или бездействии, вследствие чего в порядке уголовного судопроизводства появляется понятие уголовного преследования, заводится уголовное дело, дело рассматривает суд.

Одним из этапов производства по уголовному делу является доказывание тех или иных фактов (выяснение обстоятельств) в отношении совершённого деяния. Полный перечень обстоятельств, подлежащих доказыванию в Российской Федерации[1], определяется статьёй № 73 уголовно-процессуального кодекса Российской Федерации (далее УПК РФ).

[1] Для международного уголовного преследования – по законам других стран.

До данного момента существенных изменений, произошедших в уголовном процессе в связи с бурным развитием информационных технологий нет.

А что же поменялось далее? А то, что между людьми в их жизни, как повседневной и законной, так и противозаконной (криминальной) стали использоваться те или иные информационные технологии. Это и компьютерная техника и средства связи и т. д.

Здесь важно оговориться и развести понятия, сказав, что есть компьютерные[2] и «компьютеризированные»[3] преступления, т.е. преступления, совершённые с использованием информационных технологий (IT) по их прямому назначению.

Например, использование мобильного телефона как предмета (орудия) для нанесения повреждений кому-либо или чему-либо не подпадает под определение компьютеризированных преступлений, а вот использование мобильного телефона для совершения звонка и осуществления, например угрозы здоровью гражданина уже подходит под понятие компьютеризированного преступления и тематику данного издания.

А что же поменялось, ведь телефоны и телефоны автоматы существовали и ранее, а то, что они стали «цифровыми» и могут нести на себе «цифровой след». Это не имеет отношения к отпечаткам пальцев, оставляемым на трубке телефона, а относится к электронным внутренним журналам, например, регистрации звонка. Если ранее для определения факта или времени совершения звонка (в рамках расследования какого-нибудь уголовного дела) нужно было обращаться на телефонную станцию (что не всегда вело к успеху обнаружения следов звонка, в условиях прямой коммутации каналов связи на АТС), то сейчас подобная информация за счёт распространения и использования «интернета вещей» может накапливаться в огромном количестве окружающих человека устройств. Вопрос лишь в правильном и законном её получении и приобщении к делу с целью последующего использования как доказательства.

Под «правильным получением» интересующей следователя информации понимается как физическое её получение, поскольку она, как сосульки летом, может быстро

[2] ***Компьютерные преступления*** – общественно опасные посягательства на установленный порядок хранения, обработки или передачи компьютерной информации либо эксплуатации информационно-коммуникационных сетей и оконечного оборудования (глава 28 УК РФ - ст. 272, ст. 273, ст. 274, ст. 274.1).

[3] ***Компьютеризированные преступления*** – общественно опасные посягательства на традиционно охраняемые уголовным законом общественные отношения, опосредуемые информационно-коммуникационной инфраструктурой (ч. 3 ст. 141, п. «г» ч. 3 ст. 158, ст. 159^3, ст. 159^6, ст. 187 УК РФ), либо для которых использование информационно-коммуникационных технологий является значимо распространённым (в отдельных случаях квалифицирующим) способом осуществления общественно опасного деяния (п. «д» ч. 2 ст. 110, п. «д» ч. 3 ст. 110^1, ч. 2 ст. 110^2, ст. 137, ст. 138, ст. 138^1, ст. 146, п. «в» ч. 2 ст. 151^2, ст. 171^2, ст. 185^3, ст. 205^2, п. «б» ч. 2 ст. 228^1, ч. 1.1 ст. 238^1, п. «б» ч. 3 ст. 242, п. «г» ч. 2 ст. 242^1, п. «г» ч. 2 ст. 242^2 , п. «г» ч. 2 ст. 245, п. «б» ч. 2 ст. 258^1, ч. 2 ст. 280, ч. 2 ст. 280^1, ст. 282, ст. 354^1 УК РФ).

Замечание. Здесь и далее слова компьютерные преступления, *IT*-преступления (*IT* = = англ. *information technology* = *информационные технологии*), ИКТ-преступления (ИКТ = *информационно-коммуникационные технологии*), преступления в сфере высоких технологий и преступления, совершённые с использованием информационных технологий, являются синонимами «*компьютеризированных преступлений*», если не оговорено особо, как например, «*компьютерные*» преступления в виде преступлений в сфере компьютерной информации и «*компьютеризированные*» преступления (классификация дана по Е.А.Русскевичу [72], [75]).

исчезнуть, будучи перезатёртой другой информацией, так и юридическое оформление процесса.[4] Поскольку цифры (цифровые данные, полученные из той или иной системы) сами по себе часто не несут информации о привязке к способу её получения, могут возникнуть вопросы, например: «*А вы уверены, что данное видео было сделано в момент X в месте Y видеорегистратором Z и видеорегистратор не внёс искажений?*», чтобы на основании изучаемого видеофайла можно было сделать объективные выводы, ошибочно не обвинив невиновных?

Подобные вопросы и ответы обычно лежат в основе процесса доказывания в уголовном процессе по уголовным делам о преступлениях совершённых с использованием информационных технологий.

В настоящее время довольно часто можно наблюдать как в условиях действительной состязательности в суде сторона защиты, имеющая больший опыт в подобных делах выигрывает последние по формальным позициям, сводя многонедельный труд десятков человек из правоохранительных органов и стороны обвинения на нет. Полученный опыт из случаев подобных судебных заседаний мы приведём в конце пособия в параграфе «Не было бы так смешно, если не было бы так грустно» на стр. 131.

1.1. Доказывание и доказательства в уголовном процессе

Предмет и пределы доказывания, классификация доказательств и их допустимость и особенности по уголовным делам, связанным с IT-преступлениями. Понятие и сущность доказывания и доказательств в уголовном процессе. Соотношение предмета и пределов доказывания в уголовном процессе.

При использовании «цифровых следов» как доказательств важно понимание самого слова доказательство и важно понимание процесса.

Доказательство в философском понимании слова – это способ обоснования истинности суждения, системы суждений или теории с помощью логических умозаключений и практических средств.[5]

Таким образом можно утверждать, что доказательство в уголовном процессе – это способ получения сведений о фактах, имеющих значение для правильного (законного и справедливого) разрешения уголовного дела. Если сведения о фактах не будут выражены в той форме, которая определена действующим УПК РФ, то они не будут являться доказательствами по уголовному делу. И наоборот, сведения о фактах, закреплённые в установленной законом форме, являются доказательствами только тогда, когда они имеют значение для дела.

То есть, следуя вопросу из одного анекдота: «Вам шашечки или ехать?», – важно и то и другое. (И способ получения цифровых данных и их относимость к указанному делу.)

Замечание. Доказывание (процесс доказывания) – это осуществляемая в соответствии с требованиями УПК РФ деятельность органов дознания, дознавателей, следователей, суда, судей

[4] Здесь и далее в подобных случаях уместно использовать понятие волатильности информации. (От англ. *volatile* – непостоянный, изменчивый, неуловимый, хим. летучий, быстро испаряющийся.)
[5] Философский энциклопедический словарь. М., 1998. С. 180.

при участии иных должностных лиц, представителей общественности и граждан по собиранию, проверке и оценке фактических данных об обстоятельствах, достоверное установление которых необходимо для правильного разрешения дела.

Доказывание как деятельность, протекающая в рамках уголовного судопроизводства и направленная на решение его задач, регулируется уголовно-процессуальным законом. Уголовно-процессуальный закон, регламентируя процесс доказывания, упорядочивает деятельность по установлению фактических обстоятельств дела, создаёт надёжные гарантии равенства прав сторон в доказывании. В ходе доказательственной деятельности должна быть обеспечена охрана прав и законных интересов граждан и юридических лиц.

Замечание. При доказывании запрещается совершать действия, опасные для жизни и здоровья граждан или унижающие их честь и достоинство, домогаться показаний, объяснений, заключений, выдачи документов или предметов путём насилия, угроз, обмана и иных незаконных мер. Эти и другие правила доказывания устанавливаются и применительно к отдельным следственным действиям. В каждой стадии процесса в соответствии с её конкретными задачами и процессуальными формами доказывание имеет свои особенности, свои характерные черты, результатом доказывания могут быть только предусмотренные для данной стадии решения.

Задачи конкретной стадии, её процессуальная форма отражаются и в соотношении отдельных элементов доказывания, и в том, как происходит исследование доказательств (непосредственно или по письменным материалам) и, соответственно, какие выводы из оценки доказательств могут быть сделаны в той или иной стадии.

Само по себе доказывание состоит в собирании, проверке и оценке доказательств с целью установления обстоятельств, имеющих значение для законного, обоснованного и справедливого разрешения дел.

В науке уголовного процесса и на практике, довольно распространённым считается, что предметом доказывания являются обстоятельства, которые закреплены в ст. 73 УПК РФ, т. е. формально минималистический подход.

Для правильного разрешения уголовного дела важно чётко определить рамки его расследования и не бросаться из стороны в сторону. Чрезмерное сужение рамок, так и неосновательное расширение отрицательно сказываются на ходе и результатах предварительного расследования.

В случае сужения объёма исследования выявление существенных для дела обстоятельств окажется неполным, односторонним, что приведёт к принятию незаконного и необоснованного решения. Например, при просмотреть материалов с видерегистратора просматривали лишь один час, а не сутки и из-за сдвига времени не обнаружили интересующий следствие момент.

При неосновательном расширении границ исследования предварительное расследование и судебное рассмотрение дела неоправданно затянутся, дело окажется загромождённым ненужными, не относящимися к нему материалами, а это затруднит их оценку. Например, просматривали вручную три года видеозаписей с видеорегистратора и не смогли найти нужной минуты.

Пределы доказывания – это такие границы доказательственной деятельности, которые обеспечивают полноту и глубину исследования фактов, подлежащих установлению по делу, необходимый объём доказательств, достаточных для принятия правильного решения по делу.

Замечание. Объём доказательственной информации по любому уголовному делу должен позволять сформировать внутреннее убеждение у лиц, производящих расследование уголовного дела или судебное разбирательство, не только в реальности существования фактов, но и их достаточности для принятия законного и обоснованного решения. Практическое значение правильного определения пределов доказывания способствует собиранию и исследованию доказательств в объёме, необходимом для формирования государственного органа (должностного лица), ведущего процесс, достоверных выводов относительно предмета доказывания.

Очерченный законодателем круг обстоятельств, составляющих предмет доказывания, не исчерпывает всех обстоятельств, которые должны быть установлены по делу. Во многих случаях возникает необходимость исследовать и другие обстоятельства, которые имеют существенное значение для правильного разрешения уголовного дела. Они могут быть различного характера: имеющие значение для проверки доброкачественности и достоверности (компетентность эксперта, заинтересованность свидетеля в исходе дела, подлинность документов и т. д.); имеющие значение для законного и обоснованного применения мер процессуального принуждения; имеющие значение для правильного исполнения приговора; имеющие значение для охраны прав и законных интересов граждан (выяснение оснований для признания лица потерпевшим, гражданским истцом и т. д.).

Целью доказывания является установление обстоятельств совершённого преступления посредством правильного, адекватного отражения предметов и явлений действительности познающим субъектом. Лицо, в производстве которого находится уголовное дело, должно познать то, что имело место (произошло, случилось) в действительности, то есть познать конкретное преступление как определённую совокупность фактических признаков деяния. Выводы органов предварительного расследования и суда будут обоснованными тогда, когда они соответствуют тому, что имело место, произошло в действительности.

Определим предмет доказывания – обстоятельства, подлежащие доказыванию по уголовному делу. Согласно ст. 73 УПК РФ в ходе производства по уголовному делу подлежат доказыванию:

1) событие преступления (время, место, способ и другие обстоятельства совершения преступления);

2) виновность лица в совершении преступления, форма вины и мотивы;

3) обстоятельства, характеризующие личность обвиняемого;

4) характер и размер вреда, причиненного преступлением;

5) обстоятельства, исключающие преступность и наказуемость деяния;

6) обстоятельства, смягчающие и отягчающие наказание;

7) обстоятельства, которые могут повлечь за собой освобождение от уголовной ответственности и наказания;

8) обстоятельства, подтверждающие, что имущество, в отношении которого решается вопрос о конфискации (ст. 104.1 УК РФ):

- получено в результате совершения преступления;
- является доходами от этого имущества;
- использовалось или предназначалось для использования в качестве орудия преступления либо для финансирования терроризма, организованной группы, незаконного вооруженного формирования, преступного сообщества (преступной организации).

Замечание. Доказываться может не только наличие, но и отсутствие обстоятельств предмета доказывания. Названные обстоятельства принято называть главным фактом, поскольку от

доказанности или недоказанности этих обстоятельств напрямую зависит решение вопроса об уголовной ответственности – главного вопроса уголовного дела. Однако кроме главного факта в ходе производства по уголовному делу обычно устанавливаются и другие обстоятельства – так называемые доказательственные, или промежуточные, факты, которые в своей совокупности позволяют сделать логические выводы в наличии или отсутствии обстоятельств главного факта. Круг доказательственных фактов может быть весьма широк, а сами они разнообразны, в связи с чем дать в законе их исчерпывающий перечень обычно практически невозможно.

Ими могут быть, например: алиби обвиняемого; идентичность объектов, представленных на экспертизу, и образцов для сравнительного исследования; добросовестность свидетеля; добровольность дачи показаний и т. д.

Помимо этого, ряд процессуальных действий и решений имеют свой специфический (локальный) предмет доказывания. В частности, подлежат доказыванию: основания для задержания подозреваемого (ч. 1 ст. 91), для избрания мер пресечения (ч. 1 ст. 97); неисполнение участниками уголовного судопроизводства их процессуальных обязанностей как основание для наложения на них денежного взыскания (ст. 117); основания для обыска (ст. 182), выемки (ст. 183), наложения ареста на почтово-телеграфные отправления, их осмотра и выемки (ст. 185), контроля и записи переговоров (ст. 186), очной ставки (ст. 192); основания для приостановления и возобновления предварительного следствия (ст. ст. 208, 211); основания для проведения закрытого судебного разбирательства (ч. 2 ст. 241); наличие согласия обвиняемого с предъявленным ему обвинением и постановлением приговора без проведения судебного разбирательства (ст. 314); основания для решения вопросов, подлежащих рассмотрению судом при исполнении приговора (ст. ст. 397, 398); факт нарушения уголовно-процессуального закона (ст. 381), факт установления Европейским судом по правам человека нарушений Конвенции о защите прав человека и основных свобод при рассмотрении судом Российской Федерации уголовного дела как основание для возобновления производства по делу ввиду новых обстоятельств (п. 2 ч. 4 ст. 413) и др.

Доказывание осуществляется субъектами доказывания.

Субъекты доказывания – это те лица, на которых лежит обязанность собирания, проверки и оценки доказательств для принятия властных решений. При этом следует их разделить в зависимости от этапа их действий.

Основными критериями выделения субъектов доказывания из участников процесса были либо функции, которые они выполняют, либо возложение на них обязанности доказывания, а также те законные интересы, которые преследуют те или иные лица, участвующие в процессе доказывания.

Так, на стадии предварительного расследования, к ним будут относится следователь, дознаватель, а на судебных стадиях – только суд. При этом роль прокурора, представляющего государственное обвинение, по своей сущности будет представлять только участие в процессе доказывания на стадии судебного разбирательства.

Участники процесса доказывания, имеющие права представлять доказательства и заявлять ходатайства. К этой группе относятся подозреваемый, обвиняемый, защитник, потерпевший, его представитель, гражданский истец, гражданский ответчик и их представители, государственный и частный обвинитель и его представитель на стадии судебного разбирательства.

Участники процесса доказывания, которые являются «источниками» сведений о фактах. К этой группе необходимо отнести таких участников как подозреваемый, обви-

няемый, свидетель, потерпевший, эксперт, специалист, другими словами тех лиц, показания которых являются источниками доказательств.

Лица, выполняющие удостоверительную функцию в процессе доказывания: понятые, секретарь судебного заседания, переводчик, психолог, педагог, специалист.

Право участия в доказывании имеют подозреваемый, обвиняемый, защитник, общественный обвинитель, общественный защитник, а также потерпевший, гражданский истец, гражданский ответчик и их представители. К участию в собирании и проверке доказательств привлекаются эксперты, специалисты, понятые и другие, которые в порядке, установленном законом, выполняют определённые процессуальные обязанности.

Собирание и проверка доказательств производятся путём допросов, очных ставок, предъявления для опознания, выемок, обысков, осмотров, экспериментов, производства экспертиз и других следственных и судебных действий, предусмотренных законом.

Доказательство – это сведения, а процессуальный источник доказательства – это форма, в которой закреплены данные сведения.

Собирание, проверку, оценку доказательств на досудебных стадиях путём проведения следственных и других действий осуществляют дознаватель, следователь.

Замечание. Перечень доказательств определён в ч. 2 ст. 74 УПК РФ. Постановление Пленума Верховного Суда Российской Федерации от 05 марта 2004 г. № 1 «О применении судами норм Уголовно-процессуального кодекса Российской Федерации» разъяснил судам, что под перечнем доказательств, подтверждающих обвинение, а также под перечнем доказательств, на которые ссылается сторона защиты, понимается не только ссылка в обвинительном заключении на источники доказательств, но и приведение в обвинительном заключении, обвинительном акте или обвинительном постановлении краткого содержания доказательств. Надо помнить, что доказательства – это не сами факты (например, наличие вреда, причиненного преступлением), а сведения о таких фактах, которые содержатся в источниках доказательств. Доказательством по уголовному делу всегда являются имеющие значение дела сведения (информация), содержащиеся в показаниях допрошенных лиц, выводах экспертов, обнаруженные при осмотре и исследовании предметы и документы.

Поэтому всегда следует различать само доказательство, то есть, его физические (материальные, вещественные) и цифровые носители, и сам процессуальный источник.

Наличие у следствия или у суда предметов или документов, содержащих информацию о преступлении, вовсе не означает, что эта информация стала доказательством по делу, более того эти сведения должны быть в установленном законом порядке зафиксированы в процессуальном источнике, например, в протоколах осмотров, допросов, других следственных действий, постановлениях о приобщении к делу осмотренных предметов в качестве вещественных доказательств, протоколах судебного заседания и др.). Сам процесс фиксации доказательств в процессуальных актах требует выполнения процессуальных действий и соблюдения установленной УПК РФ процедуры их оформления. Только в этом случае информация становится доказательством.

Значение доказательств в уголовном процессе заключается в том, что с их помощью устанавливаются обстоятельства, входящие в предмет доказывания (ст. 73 УПК РФ), и, таким образом, с наибольшей вероятностью устанавливают обстоятельства совершенного деяния.

Определяя доказательства как любые сведения, закон предусматривает ряд условий, которым они должны отвечать, чтобы служить доказательствами в уголовном про-

цессе (правила об относимости, допустимости и достоверности доказательств), а все собранные доказательства в совокупности должны быть достаточными для разрешения уголовного дела (ст. 88 УПК РФ). Эти понятия также называют свойствами доказательств, которые обусловливают юридическую характеристику доказательств.

Относимость – это объективное свойство доказательств, означающее их способность освещать имеющие значение для дела (то есть существенные для него) обстоятельства.

Эта способность выражается в возможности извлечь из доказательства определенные сведения, определенную информацию, на основе которых органы расследования и суд смогут сделать достоверный вывод относительно подлежащих установлению обстоятельств дела. Относящимися к делу признаются только такие доказательства, посредством которых прямо или косвенно устанавливаются юридически значимые для дела обстоятельства.

Относимость доказательств – это использование по делу тех фактических данных, которые имеют значение для данного дела. Круг фактических данных, которые могут убедить следователя и суд в существовании тех или иных обстоятельств, законом не ограничен. Это – любые фактические данные, к которым предъявляется ряд требований, и прежде всего они должны обладать способностью подтверждать или опровергать интересующие следователя и суд обстоятельства дела. Для того, чтобы те или иные фактические данные обладали способностью устанавливать какие-либо обстоятельства дела, они должны быть причинно связаны с ними.

Замечание. Лицо, производящее дознание, следователь и прокурор при производстве предварительного расследования, а председательствующий – в судебном разбирательстве обязаны устранять все, что не относится к данному делу, направляя рассмотрение дела в сторону полного, всестороннего и объективного исследования всех его обстоятельств и установления истины.

Иными словами, решение вопроса об относимости доказательств имеет два аспекта: входит ли факт, для установления которого привлекается доказательство, в предмет доказывания; способно ли доказательство, с учётом его содержания, этот факт устанавливать.

В дальнейшем будет рассматриваться особый вид вещественных доказательств – «цифровые доказательства», несколько сужающие новый термин «доказательства в электронной форме», которые вообще говоря могут быть представлены и в виде допроса эксперта (специалиста) посредством видеоконференцсвязи. Цифровые доказательства невозможно непосредственно воспринимать органами чувств, их использование предполагает наличие как определённой технологии идентификации, сбора и верификации таких доказательств в и практической науки, т. н. частной криминалистической теории – «форензики» (цифровой или компьютерной криминалистики), см. [34, 60, 81, 85].

Фактические данные как доказательства должны быть достоверными.

Достоверность обусловливает отражение в материалах уголовного дела объективных, имевших место в реальном прошлом событий и явлений.

Достоверность предполагает известность, проверяемость и доброкачественность как самого источника, так и способа получения фактических данных, надежность процессуального носителя и средств фиксации.

Это особенно важно для цифровых доказательств, где исходя из особенностей процессов и законов логики построения информационно-телекоммуникационных технологий и скоротечности обработки данных, под сомнение может быть поставлена це-

лостность (неизменность) данных, или способ получения фактических данных в электронной форме или средства фиксации.

Достаточность доказательств имеет отношение к пределам доказывания. Субъект доказывания должен обладать совокупностью доказательств, позволяющей сделать единственный вывод о событии прошлого, а также роли в нём участников уголовного процесса.

Допустимость доказательств означает правопригодность их к использованию в уголовном процессе в качестве аргументов в доказывании. Это означает пригодность доказательств с точки зрения законности источников, законности методов, способов, приемов получения информации, соответствие закону формы их закрепления.

Замечание. Доказательства признаются допустимыми при условии, если они получены: из предусмотренного законом источника (ч. 2 ст. 74 УПК РФ); управомоченными на то органами и должностными лицами; законным способом (соблюдены правила собирания, фиксации доказательств).

Уголовно-процессуальный закон установил следующие условия признания доказательств допустимыми: доказательства должны быть получены надлежащими субъектами, правомочными по данному делу проводить то процессуальное действие, в ходе которого получено доказательство; фактические данные должны быть получены только из источников, установленных законодательством; доказательства должны быть получены с соблюдением правил производства следственного действия, в ходе которого получено доказательство, т. е. при помощи законных приемов и способов; при получении доказательств должны быть соблюдены все требования, предъявляемые к форме их закрепления.

Источниками получения фактических данных являются: показания свидетеля, показания потерпевшего, показания подозреваемого, показания обвиненного, выводы эксперта, вещевые доказательства, протоколы следственных и судебных действий, протоколы с соответствующими дополнениями, составленными уполномоченными органами по результатам оперативно-розыскных мероприятий, и другими документами.

Условия допустимости доказательств следующие: известность и возможность проверки её происхождения (информации); компетентность и осведомлённость лиц, от которых она исходит и которые её собирают; соблюдение общих правил доказывания (гарантирующих полноту и ясность фиксации); отказ включения в неё различного рода догадок и предположений.

Замечание. В качестве доказательств не могут быть допущены материалы, не приобщенные к данному делу, оперативно-розыскная информация, надлежащим образом не оформленная, анонимные письма и заявления, доказательства, полученные при производстве следственных действий при отсутствии понятых и т.д. В уголовно-процессуальном законе содержатся основания признания доказательств недопустимыми. Например, запрещается домогаться показаний обвиняемого и других участвующих в деле лиц путём насилия, угроз и иных незаконных мер. Не могут служить доказательствами сообщенные свидетелем данные, источник которых не известен. Закон установил, кто не может допрашиваться в качестве свидетеля и др. В силу презумпции невиновности все сомнения по делу, а следовательно, и сомнения относительно допустимости к использованию фактических данных в доказывании должны толковаться и разрешаться в пользу обвиняемого, подозреваемого и подсудимого.

Нарушение хотя бы одного из указанных требований приводит к утрате доказательства. Уголовно-процессуальный закон (ч. 1 ст. 75 УПК РФ) прямо говорит о том, что доказательства, полученные с нарушением требований УПК РФ, являются недопустимыми.

1.1.2. Недопустимые доказательства

Недопустимость доказательства – это признание отсутствия у конкретного доказательства свойства допустимости вследствие получения этого доказательства с нарушением требований УПК РФ или федерального закона.

В ч. 2 ст. 75 УПК РФ предусмотрены доказательства, которые признаются недопустимыми:

1. Показания подозреваемого, обвиняемого, данные в ходе досудебного производства по уголовному делу в отсутствие защитника, включая случаи отказа от защитника, и не подтвержденные подозреваемым, обвиняемым в суде. Это положение распространяется только на случаи, когда УПК РФ не предусматривает обязательное участие защитника. Неподтверждение ранее данных показаний может выразиться: в даче противоположных показаний в суде; в отказе от дачи показаний в суде.

Замечание. Запрет на использование показаний подозреваемого, обвиняемого, данных в досудебном производстве в отсутствие защитника, в случае их неподтверждения в судебном заседании, порождает ряд правовых последствий.

Во-первых, такие доказательства утрачивают свойство допустимости только в момент их неподтверждения подсудимым в суде, то есть, до этого момента такие доказательства являются допустимыми. При этом причина отсутствия защитника в досудебном производстве, в том числе добровольный отказ подозреваемого, обвиняемого от защитника, не имеет значения для признания таких показаний недопустимым доказательством;

Во-вторых, возникает вопрос допустимости иных доказательств, полученных в досудебном производстве на основании показаний подозреваемого, обвиняемого, данных в отсутствие защитника, и не подтвержденных в суде.

Например, можно ли признать законными следственные действия, произведенные на основании таких показаний в досудебном производстве (выемки, обыски, опознания и т. п.)? Такие доказательства должны признаваться полученными в результате законных следственных действий, и ставить вопрос о лишении их свойства допустимости «задним числом» нельзя.

На момент производства следственного действия доказательства, добытые на основании показаний подозреваемого, обвиняемого, признаются допустимыми при условии, что отсутствие защитника не нарушало закон, а сами показания не были получены с применением недозволенного принуждения. Правомерное получение показаний при правомерном отсутствии защитника не порождает основания для признания их недопустимыми до того момента, пока лицо не отказалось подтвердить их в суде. Дальнейший отказ подсудимого от показаний, данных в отсутствие защитника, влечёт недопустимость только его собственных первоначальных показаний, данных в отсутствие защитника.

2. Показания потерпевшего, свидетеля, основанные на догадке, предположении, слухе, признаются недопустимыми в силу отсутствия в них как объективного основания, так и содержательной информации о фактических, а не вымышленных или предполагаемых обстоятельствах дела, подлежащих доказыванию в силу ст. 73 УПК РФ.

Пояснение (что есть что). Догадка – это лишь субъективное предположение о вероятности, возможности чего-либо. Предположение – это та же догадка или некое субъективное предварительное соображение. Зачастую, предположение может быть выражено в виде мнения – некое суждение, выражающее личную субъективную оценку чего-либо, отношение к кому-то, взгляд на что-то. Мнение не является фактом, очевидностью.

Слух – это молва, известие о чём-нибудь или о ком-нибудь, обычно ещё ничем не подтверждённые. В основе слухов лежит, как правило, внешний посторонний текст, который сам может

быть основан не на восприятии реальности, а на домыслах, догадках, предположениях иного лица или множества лиц.

Показания, основанные на догадках, предположениях, мнениях или слухах, лишены какого-либо проверяемого объективного содержательного основания, поэтому они не могут быть положены в основу утверждений об обстоятельствах, подлежащих доказыванию.

Показания свидетеля, который не может указать источник своей осведомленности, по сути, схожи с показаниями, основанными на слухах.

Даже если источник слуха может быть точно указан свидетелем, потерпевшим, слух сам по себе остается ничем не подтвержденным высказыванием, как и в случаях, когда свидетель не может указать источник своей осведомленности, его показания не поддаются объективной проверке ни по источнику информации, ни по её содержанию. Такого рода сведения не отвечают самому понятию доказательства и являются недопустимыми.

3. Предметы, документы или сведения, входящие в производство адвоката по делам его доверителей, полученные в ходе оперативно-розыскных мероприятий или следственных действий, за исключением предметов и документов, указанных в ч. 1 ст. 81 УПК РФ.

Ведение адвокатского производства является необходимым по смыслу п. 3 ст. 8 ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации», а также ч. 9 ст. 6 Кодекса профессиональной этики адвоката. Адвокатское производство необходимо в целях: систематизации информации в процессе оказания юридической помощи доверителю, эффективного использования сведений для защиты прав доверителя, в том числе о способах доказывания по уголовным делам; оценки качества работы адвоката при претензии к нему доверителя; сохранения адвокатской тайны (содержащиеся в нём предметы, документы или сведения не могут быть использованы стороной обвинения в качестве доказательств).

Замечание. Адвокатское производство оформляется адвокатом со дня принятия поручения от доверителя. Материалы такого производства, как правило, в копиях хранятся в папке или файле. Такое производство ведется как на бумажных, так и на цифровых носителях.

В адвокатском производстве по уголовным делам находятся копии (выписки) не только процессуальных документов (например, постановления о возбуждении уголовного дела; постановления о привлечении в качестве обвиняемого; протоколы допроса подозреваемого и обвиняемого; заявленных ходатайств и ответов на такие просьбы; постановления об избрании меры пресечения, обвинительного заключения, протокола судебного заседания), но и аудиозапись судебных заседаний, таблицы и схемы, помогающие ориентироваться в уголовном деле, замечания на процессуальные документы, даты свиданий с подзащитным (их продолжительность, вопросы, которые обсуждались и которые предстоит выяснить для определения тактики защиты), проект защитительной речи и иные записи адвоката.

4. Иные доказательства, полученные с нарушением требований УПК РФ. Пленум Верховного суда Российской Федерации в постановлении № 8 от 31 октября 1995 г. «О некоторых вопросах применения судами Конституции Российской Федерации при осуществлении правосудия» в пункте 16 разъясняет, что доказательства должны признаваться полученными с нарушением закона, если при их собирании и закреплении были нарушены:

- гарантированные Конституцией Российской Федерации права человека и гражданина;

- установленный уголовно-процессуальным законодательством порядок их собирания и закрепления, а также, если собирание и закрепление доказательств осуществлены ненадлежащим лицом или органом;
- доказательства получены в результате действий, не предусмотренных процессуальными нормами.

Любое из указанных нарушений даёт право участникам процесса требовать признания доказательства недопустимым.

Выявление нарушений УПК РФ или иного федерального закона при получении доказательства или заявление участника о подобном нарушении требует специальной процедуры признания доказательства недопустимым или отказа в этом.

Процедура признания доказательства недопустимым регламентирована ст. 235 УПК РФ – Ходатайство об исключении доказательства. Ввиду того, что недопустимые доказательства не имеют юридической силы, стороны в стадии назначения судебного разбирательства наделяются правом заявить ходатайство об исключении из перечня доказательств любого доказательства, которое они считают недопустимым.

Доказательства, признанные недопустимыми, с этого момента утрачивают юридическую силу и не могут использоваться субъектами доказывания, во-первых, для обоснования обвинения, во-вторых, для позитивного утверждения о наличии и доказанности любого из обстоятельств, перечисленных в ст. 73 УПК РФ. К таким же последствиям должно приводить и получение доказательств, с применением принуждения к даче показаний подозреваемого, обвиняемого, потерпевшего, свидетеля; к даче заключения или показаний эксперта и специалиста. Подобное принуждение или образует состав преступления, предусмотренный ст. 302 УК РФ, или нарушает предписания ч. 2 ст. 9 УПК РФ о том, что никто из участников не может подвергаться насилию, пыткам, другому жестокому или унижающему человеческое достоинство обращению.

1.1.3. Классификация и виды доказательств

Основная классификация и виды доказательств в уголовных делах.

Любые сведения (доказательства), с помощью которых дознаватель, следователь, прокурор и суд устанавливают по уголовному делу положения, образующие предмет доказывания, и иные обстоятельства, имеющие значение для правильного разрешения дела, могут быть получены в рамках процессуального доказывания только из источников, указанных в законе и именуемых в теории уголовного процесса источниками доказательств.

Согласно ч. 2 ст. 74 УПК РФ к источникам доказательств относятся:

а) показания подозреваемого, обвиняемого;

б) показания потерпевшего, свидетеля;

в) заключение и показания эксперта;

г) заключение и показания специалиста;

д) вещественные доказательства;

е) протоколы следственных и судебных действий;

ё) иные документы.

Исходя из текущей конструкции ст. 74 УПК РФ указанный перечень является закрытым: исчерпывающим и расширительному толкованию не подлежит, что порожда-

ет определённые проблемы при использовании «цифровых доказательств», т. к. сведения, полученные из иных источников, являются недопустимыми.

Классификация доказательств – это их систематизация на основе, присущего их внутренним, объективным свойствам критерия. Классификация доказательств представляет собой их деление, распределение на виды и группы, категории по определённым основаниям. Классификация может быть проведена по признакам, относящимся к содержанию доказательства, либо к их форме (источнику) или их виду. Каждая классификационная группа доказательств обладает какими-либо только ей присущими свойствами.

В теории и практике уголовного процесса принято классифицировать доказательства по следующим критериям: по отношению к предмету обвинения – на обвинительные и оправдательные; по характеру источника доказательственной информации – на первоначальные и производные; по отношению к доказываемому факту – на прямые и косвенные; по способу формирования – на личные и вещественные.

Каждое доказательство по этим признакам может быть отнесено к той или иной группе. Это означает, что, исследуя доказательство, надо учитывать, получено ли оно из «первых рук» или надо установить первоисточник сведений, какова связь сообщаемого с тем, что надо установить, являются ли сведения по своему характеру обвинительными или оправдательными.

В юридической науке и на правоприменительной практике выработаны определенные правила, с учётом которых следует исследовать каждое доказательство в той или иной классификационной группе.

Использование признаков, положенных в основу классификации доказательств и правил собирания, проверки и оценки каждого вида доказательств, способствует формированию достоверных выводов по делу.

Первоначальные и производные доказательства. Доказательства делятся на первоначальные и производные в зависимости от того, получают ли информацию следователь, суд из первоисточника или из «вторых рук». Первоначальным доказательством будет, например, показание свидетеля, который лично наблюдал факты, о которых сообщает. Показание свидетеля о событии, которое он не наблюдал, но слышал о нём от другого лица, бывшего очевидцем, будет доказательством производным. При получении сведений из «вторых рук» обязательно должен быть установлен первоисточник сведений (например, очевидец) и допрошен. При этом учитывается, что очевидец события, явления рассказывает о нём точнее и полнее, чем тот, кто знает об этом по рассказам других лиц. Показания очевидца легче поддаются проверке, а поэтому более достоверны.

Замечание. Если установить первоисточник сведений о каком-либо факте, о котором сообщает допрашиваемый, не представляется возможным, то эти сведения теряют значение доказательства и должны быть отвергнуты. «Не могут служить доказательством фактические данные, сообщаемые свидетелем, если он не может указать источник своей осведомлённости» (ст. 74 УПК РФ). Такое же правило действует в отношении показаний потерпевшего. Сведения, полученные «по слухам», не могут быть проверены, а значит, не могут быть использованы в качестве доказательства.

Стремление использовать по возможности доказательства первоначальные не означает, что производные не могут привести к достоверным выводам, что они доказательства «второго сорта».

Категорический запрет использовать производные доказательства может лишить суд в ряде случаев важных доказательств, полученных из «вторых рук», если из первоисточника их получить невозможно (например, в случае смерти очевидца происшествия).

В основе деления доказательств на первоначальные и производные лежит наличие или отсутствие промежуточного носителя доказательственной информации. Под первоначальными доказательствами понимаются сведения, полученные из первоисточника (от лица, непосредственно воспринимавшего событие преступления, либо из подлинника документа, либо из подлинного вещественного доказательства, для цифровых доказательств – полученные от источника формирования цифрового потока – камеры или смартфона, файлов жесткого диска компьютера, данных датчика системы СОПКА и т.п.).

Производными являются доказательства, полученные из опосредованного источника (например, сведения, сообщенные свидетелем со слов другого лица, или данные, содержащиеся в копии документа). В производных доказательствах всегда содержится вероятность утраты части информации, её искажения. Чем больше промежуточных звеньев, тем больше опасность их утраты. Поэтому теория и практика уголовного процесса отдают предпочтение первоначальным доказательствам. Производные доказательства допускаются: в случаях невозможности получения первоначальных доказательств, в связи с утратой их источника; для отыскания первоначальных доказательств; для проверки первоначальных доказательств; для восполнения первоначальных доказательств, когда их недостаточно для безошибочных выводов (например, наблюдавший определенное событие забыл отдельные детали, а лицо, которому он об этом рассказал, хорошо помнит их).

Обвинительные и оправдательные доказательства. Деление доказательств на обвинительные и оправдательные зависит от содержания полученных сведений и установления доказательств. Доказательства совершения преступления обвиняемым, его вины или обстоятельства, отягчающие ответственность обвиняемого, являются обвинительными: а доказательства, которые опровергают обвинение, свидетельствуют об отсутствии общественно опасного деяния или вины обвиняемого либо смягчают его ответственность, - оправдательными.

Требование собирать обвинительные и оправдательные доказательства закреплено в законе: ст. 20 УПК РФ предписывает выявить по каждому делу доказательства как уличающие, так и оправдывающие обвиняемого, а также отягчающие и смягчающие его вину обстоятельства: ст. 69 УПК РФ указывает, что доказательства могут устанавливать «наличие или отсутствие общественно опасного деяния»: отнесение доказательства к обвинительному или оправдательному возможно в результате оценки всех доказательств в совокупности. Бывает так, что доказательство, первоначально отнесенное к обвинительным, окажется оправдательным.

Проверенные и оцененные обвинительные и оправдательные доказательства должны быть отражены в важнейших процессуальных документах: обвинительном заключении (ст. 205 УПК РФ) и приговоре (ст. 314 УПК РФ). Это означает, что при вынесении обвинительного приговора надо указывать те доказательства, которые положены судом в основу обвинения, с приведением мотивов, почему эти доказательства приняты судом и почему судом отвергнуты оправдывающие подсудимого доказательства: при вынесении оправдательного приговора следует указывать доказательства, которые

положены судом в основу оправдания, с приведением мотивов, почему суд отверг те, на которых основано обвинительное заключение.

Прямые и косвенные доказательства. Деление доказательств на прямые и косвенные основано на том, что одни из них содержат сведения об обстоятельствах, составляющих предмет доказывания, другие - о так называемых «доказательственных», «промежуточных», «вспомогательных» фактах. Деление доказательств на прямые и косвенные основано на логическом отношении между доказательством и доказательным тезисом.

Если заключенная в доказательстве информация прямо устанавливает доказательственный факт – это прямое доказательство.

Если доказательство не указывает прямо на доказательственный факт, но позволяет сделать вывод о нём на основе промежуточных фактов, то такое доказательство считается косвенным.

Прямыми доказательствами являются доказательства, указывающие на совершение лицом преступления, т. е. доказывающие так называемый «главный факт». Эти обстоятельства, указанные в п. 1, 2 ст. 68, дают основания для ответов на вопросы, поставленные в п.1, 3, 4 ст. 303, в п. 1, 2,3 ч. 1 ст. 449 УПК РФ. Показания обвиняемого, признающего свою вину и объясняющего, по каким мотивам, когда, где и при каких обстоятельствах он совершил преступление, являются прямым доказательством. Прямым доказательством является показание свидетеля о том, как обвиняемый использовал чужое электронное средство платежа (например: смартфон с программой оплаты) потерпевшего. При использовании прямых доказательств задача состоит только в установлении их достоверности (т. е. надо установить, говорит ли обвиняемый, свидетель правду), так как значение сообщенных сведений для установления предмета доказывания здесь очевидно. Для установления достоверности доказательства каждое из них должно быть рассмотрено в совокупности всех доказательств. Никаких преимуществ в силе прямое доказательство не имеет, поэтому недопустимо считать «главным» доказательством, такое прямое доказательство, как признание обвиняемым своей вины (ч. 2 ст. 77 УПК РФ).

Косвенные доказательства содержат сведения о фактах, которые предшествовали, сопутствовали или следовали за доказываемым событием и по совокупности которых можно сделать вывод о том, имело ли место событие преступления, виновен или не виновен обвиняемый. Так, при расследовании дела об нарушении правил эксплуатации ЭВМ или сети ЭВМ (ст. 274 УК РФ) на основании косвенных доказательств – принадлежность биологических следов (перхоть, потожировые отпечатки) обвиняемому на ЭВМ в центре обработки данных (далее – ЦОД), где произошла авария, установление неприязненных отношений обвиняемого и владельца сети ЭВМ (потерпевшего) и других фактических данных (наличие пропуска и права работать в ЦОД) формируется вывод следователя, суда о совершении обвиняемым данного преступления. Путь установления обстоятельств дела с помощью косвенных доказательств более сложный, чем при прямых доказательствах.

Косвенные доказательства, как правило, содержат сведения о побочных, частных фактах, отдельных деталях исследуемого события, которые, будучи установленными, позволяют сделать вывод об искомых фактах.

Замечание. Отнесение доказательств к прямым или косвенным зависит от конкретного состава преступления, например, совершённого с использованием информационных техноло-

гий. Например, наличие специальных знаний у обвиняемого или владение вычислительным устройством с конкретным идентификационным номером может служить косвенным доказательством по делу об нарушении работоспособности какого-либо интернет-сайта и прямым доказательством по делу о краже такой вычислительной техники.

Показания о том, что обвиняемый приглашал иное лицо (свидетеля) в социальную группу борцов за чистоту мусульманской веры на одном их форумов сети «Интернет» и размещал там же рассуждения и призывы о целесообразности лишения жизни конкретных лиц из-за из религиозной принадлежности (например, к христианству), является прямым доказательством по делу об действиях экстремистского характера и косвенным – по делу по обвинению в угрозе убийством указанных лиц.

Доказательства личные и вещественные. Личные доказательства означают доказательства, исходящие от лица, передаваемые лицом (человеком). Это те сведения об обстоятельствах известного ему преступления, которые сохранились в его памяти. Иными словами, личные доказательства – это мысленное отображение информации, имеющей значение для дела. Поэтому иногда их называют идеальными.

Личными доказательствами выступают такие доказательства, которые исходят от человека. К ним относятся дача показаний, различные документы (в том числе, процессуальные), экспертные заключения. Вещественные доказательства − это материальные объекты, фрагменты обстановки (орудие преступления, предметы со следами преступления и прочие.

Между вышеизложенными видами доказательств имеются кардинальные различия, которые обязательно нужно учитывать при их оценке. Содержание личных доказательств формируется в силу субъективного мышления человека, который её добывает. По-этому она не может быть полностью объективной и независимой. Общеизвестно, что не существует одинаковых показаний об одном и том же происшествии, даже людьми, находящимися в одинаковой обстановке. Даже заключение эксперта, которое, на первый взгляд, носят исключительно научный характер, неминуемо проходит через субъективное восприятие эксперта, что, несомненно, отразиться в результатах исследований. И это относится не к стилистике подачи информации, нередки случаи, когда мнения экспертов по одному и тому же делу, совершенно противоположны.

К личным доказательствам относятся показания подозреваемого, обвиняемого, свидетеля, потерпевшего, эксперта и специалиста. Данное обстоятельство признается всеми учеными, занимающимися данным вопросом, что вполне логично, так как само понятие показание, означает, что речь идет о сведениях, полученных на до-просе, значит от лица и оформленное в допустимую УПК РФ процессуальную форму.

Протоколы следственных действий (обыска, выемки, предъявления для опознания, следственного эксперимента и т.п.) многие ученые так же относят к личным доказательствам. Например, В. А. Лазарева[6] по этому поводу пишет, что в протоколах следственных действий «в знаковой форме зафиксированы результаты непосредственного восприятия следователем, дознавателем наглядно-образной и предметно-пространственной информации. В знаковой же форме выражена информация, выявленная, исследованная и истолкованная экспертом. В этом смысле заключение эксперта тоже личное доказательство.

[6] См. *Лазарева В.А.* Проблемы доказывания в современном уголовном процессе России: учеб. пособие / Самара: Изд-во «Самарский университет», 2007. – 303 с.

Таким образом к личным доказательствам относятся сведения, содержащиеся в показаниях свидетелей, потерпевших, обвиняемых, подозреваемых, заключениях экспертов, протоколах следственных и судебных действий и иных документах.

Вещественные доказательства представляют собой объекты материального мира (поэтому иногда их ещё называют материальными). Это объекты:

- несущие на себе различные следы-отображения (например, отпечаток обуви, пальцев и т. д. на каких-либо предметах);
- свидетельствующие об изменении состояния объекта или отдельных его свойств в результате воздействия на него;
- выполняющие определенную функцию в совершении преступления (орудия преступления, объекты преступного посягательства и т. д.);
- характеризующие отдельные элементы механизма преступления (способ, цель, условия и др.).

Так, например, А. А. Эйсман говоря об особенностях вещественных доказательств, указывает, что в вещественных доказательствах информация содержится в некодированной форме, в своем так сказать, естественном виде и воспринимается наглядно (например, кончик ножа отломан).

Интересную мысль, на наш взгляд высказал Б.В. Комлев[7] о том, что «*материальный объект – ещё не доказательство. Материальные же объекты любого физического состояния (твёрдого, жидкого, газообразного и иного) могут служить источником информации, используемой в качестве доказательства по уголовному делу и одновременно критерием её истинности*».

Исходя из вышесказанного, думаем, стоит согласиться с Г. П. Корневым[8], который считает, что «*вещественное доказательство представляет собой сложное образование, состоящее из двух компонентов, различных по форме своего бытия: вещественного и личного, объективного и субъективного...*» Предъявление доказательства со стороны его вещественного компонента выступает «аргументом» очевидности, в связи с этим, считаем, что классификация доказательств на личные и вещественные приобрела особо важное значение в силу сохранности и наглядности материального носителя информации.

В научной литературе и тематическом сообществе достаточно давно обсуждается [31] [42] [54] [59] [85] [117] возможность прямой аналогии вещественных доказательств с цифровыми в виде информационных объектов в рамках какой-либо автоматизированной или информационной системы, сайтов сети интернет, а также цифровые следы – отображения в операционных и файловых системах, базах и банках данных, самостоятельные цифровые объекты в виде файлов или упорядоченных записей информации на логическом или машинном носителе информации.

В заключение рассмотрения вопросов классификации приведём т. н. видовую классификацию в соответствии с УПК РФ:

- показания (подозреваемого, обвиняемого, свидетеля, потерпевшего, специалиста, эксперта, гражданского ответчика, гражданского истца и даже следователя или дознавателя – как свидетелей);
- заключения (специалиста или эксперта);

[7] См. *Комлев Б.В.* О понятии вещественного доказательства // Законность. 1998. № 4.

[8] См. *Корнев Г.П.* Методологические проблемы уголовно-процессуального познания. Нижний Новгород, 1995.

- вещественные доказательства (в т.ч. цифровые доказательства и их носители, зафиксированные в протоколах или заключениях);
- протоколы следственных действий и судебного заседания;
- иные документы, представленные и зафиксированные в ходе процессуальных действий.

Показания подозреваемого (ст. 76 УПК РФ) и обвиняемого (ст. 77 УПК РФ) – это сведения, сообщённые ими на допросе, проведённом в ходе досудебного производства, (применительно к обвиняемому ещё и в ходе судебного разбирательства дела) в соответствии с требованиями закона о производстве допроса (ст.ст. 187–190 УПК РФ).

Предмет показаний подозреваемого определён в ст. 46 УПК РФ – это обстоятельства, касающиеся имеющегося в отношении него подозрения.

Предмет показаний обвиняемого определён в ст. 47 УПК РФ – это обстоятельства, образующие содержание предъявленного ему обвинения.

Указанными обстоятельствами предмет показаний подозреваемого и обвиняемого не исчерпывается, в ходе дачи показаний они не только излагают ход событий, но и дают им своё объяснение, излагают мотивы и причины своих действий. Кроме того, они вправе давать в своих показаниях оценку имеющихся в деле и известных им доказательств, представлять контраргументы, то есть осуществлять свою защиту всеми средствами и способами, не запрещенными действующим законодательством.

Подозреваемый и обвиняемый (когда они объявлены таковыми) не предупреждаются об уголовной ответственности за дачу заведомо ложных показаний или за отказ от дачи показаний. Их показания – это их право, а не обязанность. Отказ подозреваемых, обвиняемых от дачи показаний не может рассматриваться как доказательство их виновности. Являясь с одной стороны источником доказательств, показания подозреваемого или обвиняемого с другой стороны – это один из способов защиты от обвинения, то есть способ, гарантирующий защиту их конституционных прав. Показания подозреваемого и обвиняемого могут лечь в основу обвинения лишь в том случае, когда будут подтверждены совокупностью других доказательств по уголовному делу (ч. 2 ст. 77 УПК РФ). Признательные показания, подтвержденные совокупностью других доказательств по делу, продолжают иметь доказательственную силу даже в случае отказа от них подозреваемого, обвиняемого. Однако нельзя переоценивать показания этих лиц. Значение в данном случае имеет не столько признательность показаний, сколько сообщенные фактические данные.

При оценке показаний подозреваемого и обвиняемого необходимо исходить из того, что они заинтересованы в исходе дела. Поэтому, сообщаемые ими сведения должны быть тщательно проверены, сопоставлены с другими имеющимися по делу доказательствами. Факт заинтересованности не должен вести к недоверию к показаниям, игнорированию их при принятии решения. В случае изменения указанными лицами данных ими ранее показаний необходимо, по мере возможности, выяснить причину этого: каковы мотивы, является ли оно добровольным или вынужденным.

Судебно-следственная практика исходит из того, что любое из показаний подозреваемого, обвиняемого имеет одинаковое доказательственное значение. Признательные показания указанных лиц помогают при расследовании преступлений, так как являются источником особо ценных доказательств, облегчают поиск других доказательств по делу, способствуют раскрытию преступлений, установлению важных обстоятельств по уголовному делу, известных только причастному к преступлению лицу.

Признательные показания рассматриваются уголовным правом как обстоятельство, смягчающее ответственность.

Однако признание вины не всегда является свидетельством виновности. Известны случаи самооговора, из-за шантажа и угроз, тяжёлого моральной и материального положения (нищенствования, бродяжничества) или вызванные стремлением освободить от уголовной ответственности близких лиц, получить вознаграждение от заинтересованных лиц, скрыть совершение более тяжкого преступления и др.

Иногда подозреваемые, обвиняемые дают заведомо ложные показания, оговаривая других лиц. Когда этот оговор находится в рамках предъявляемого обвинения, он рассматривается как защитная версия, ответственность за такие показания законом не предусмотрена. Когда оговор касается фактов по другому эпизоду или делу, в рамках которых версия о причастности указанных лиц ещё не проверялась, последние должны быть допрошены в качестве свидетелей, а это значит, что они предупреждаются об уголовной ответственности за отказ от дачи показаний и за дачу заведомо ложных показаний.

Кроме показаний, в которых содержится полное или частичное признание своей вины, подозреваемые и обвиняемые могут давать показания, в которых их вина отрицается. Несмотря на активную оборонительную позицию подозреваемого, обвиняемого задачей предварительного следствия является сбор совокупности доказательств, то есть установление преступника, вина которого должна быть подтверждена бесспорными, неопровержимыми доказательствами.

В случае, когда у расследующего преступление органа остаются сомнения по поводу виновности конкретного лица в совершении им конкретного преступления, эти сомнения толкуются в пользу обвиняемого, подозреваемого. Таким образом, расследующий преступление орган ни в коем случае не должен допускать в своей деятельности обвинительного уклона.

Показания потерпевшего (ст. 78 УПК РФ), свидетеля (ст. 79 УПК РФ) – это сведения, сообщенные ими на допросе, произведённом в ходе досудебного производства по уголовному делу или в суде в установленном законом порядке. Потерпевший и свидетель могут быть допрошены о любых обстоятельствах, подлежащих доказыванию при производстве по уголовному делу, в том числе о своих взаимоотношениях с подозреваемым, обвиняемым. Свидетель, кроме того, может быть допрошен и о личности обвиняемого, потерпевшего, о своих взаимоотношениях с ними и другими свидетелями.

Замечание. Показания потерпевшего по сравнению с показаниями свидетеля имеют ряд особенностей, обусловленных выполняемой им функцией, – они являются не только источником доказательств, но и процессуальным средством защиты его законных прав и интересов. Дача показаний свидетелем и потерпевшим – это не только право, но и их обязанность (п. 2 ч. 5 ст. 42, п. 2 ч. 6 ст. 56 УПК РФ).

Процессуальная природа показаний названных лиц определяется тем, что показания формируются в результате личного восприятия ими фактов, интересующих органы расследования и суд.

Определяя лицо, которое может быть свидетелем по делу, уголовно-процессуальный закон исходит из того, что такому лицу известны какие-либо обстоятельства, подлежащие установлению. Не могут служить доказательствами показания потерпевшего, свидетеля, основанные на догадке, предположении, слухе, а также показания свидетеля, который не может указать источник своей осведомленности (п. 2 ч. 2 ст. 75 УПК РФ).

Ни возраст, ни дружеские отношения с обвиняемым, ни служебное положение, ни заинтересованность свидетеля в исходе дела, ни родственные связи (за исключением близких родственников) не освобождают свидетеля от дачи показаний. Известные ограничения содержатся лишь в ч. 3 ст. 56 УПК РФ. Эти ограничения обусловлены процессуальным положением лиц, участвующих в деле, спецификой выполняемых ими функций, а также связаны с обеспечением достоверности получения показаний. То есть не подлежат допросу в качестве свидетелей: судья, присяжный заседатель, защитник подозреваемого, обвиняемого, адвокат, священнослужитель, член Совета Федерации, депутат Государственной Думы без их согласия – об обстоятельствах, которые стали им известны в связи с осуществлением ими своей профессиональной деятельности.

В качестве свидетелей могут быть допрошены следователи, дознаватели, в производстве которых находится уголовное дело. В этом случае они утрачивают право продолжать производство предварительного расследования по этому уголовному делу.

Не освобождаются от дачи показаний лица в связи с тем, что предмет их показаний составляет государственную, служебную или профессиональную тайну (например, сотрудники полиции). На судебно-следственные органы возлагается тогда обязанность обеспечить неразглашение этих сведений. С этой целью, в частности, проводятся закрытые судебные заседания (п. 5 ч. 2 ст. 231, ч. 2 ст. 241 УПК РФ).

1.1.3.1. Заключение и показания эксперта и специалиста

При производстве предварительного расследования по уголовным делам, связанным с использованием информационных технологий, а также в ходе дальнейшего судебного разбирательства возникает необходимость в получении заключений и показаний эксперта и специалиста в науке, технике, сетевых и программных технологиях, в вопросах сетевой торговли и цифровых бирж криптовалют. Данные действия допустимы в соответствии со ст. 80 УПК РФ.

Замечание. Предмет деятельности специалиста в уголовном судопроизводстве иной, чем у эксперта. Специалист призван содействовать следствию в обнаружении, закреплении и изъятии предметов и документов, применении технических средств в исследовании материалов уголовного дела, в постановке вопросов эксперту, а также в разъяснении сторонам и суду вопросов, входящих в его профессиональную компетенцию (содействие следствию по указанным выше направлениям; участие в качестве специалиста – инженера подразделения по информационным технологиям, связи и защите информации районного ОВД в допросе подозреваемого в создании вредоносной программы; допрос специалиста по информационным технологиями, явившегося в суд по инициативе сторон).

В отличие от специалиста эксперт становится участником уголовного процесса только по постановлению дознавателя, следователя, судьи, определению суда. Он производит самостоятельное экспертное исследование[9], тогда как специалист всегда участвует в процессуальных действиях в отношении IT-преступлений, производимых органом, ведущим расследование или судом. Заключение эксперта по своей юридической природе есть особый, самостоятельный специальный источник доказательств, поскольку производство экспертизы на базе имеющихся по делу доказательств может привести к появлению в уголовном процессе новых фактических данных (доказательств) и(или) способствовать переквалификации или расширения квалификации уголовного дела по статьям УК РФ.

[9] См. *Саркисян А. А.* Аккредитация в судебно-экспертной деятельности / А. А. Саркисян // Криминалистика: вчера, сегодня, завтра. – 2022. – № 1(21). – С. 136-141. – DOI 10.55001/2587-9820.2022.28.94.012. – EDN VIJHLE.

Задачей производства экспертизы является получение новых знаний за счёт проведения исследований профессионалами в области различных отраслей человеческой деятельности. Вопросы, поставленные перед экспертом, данное им заключение не могут выходить за пределы его специальных познаний – на разрешение эксперта нельзя ставить вопросы правового (юридического) характера (например, о виновности или невиновности, квалификации, контрафактности технических средств или программного обеспечения). Даже если эти вопросы поставлены и в заключении эксперта нашли ответы, доказательной силы они иметь не будут, так как решение этих вопросов – исключительная компетенция органов предварительного расследования и суда.

Эксперт может дать заключение по вопросам, хотя и не поставленным в постановлении о назначении судебной экспертизы, но имеющим отношение к предмету экспертного исследования. Заключение даётся от имени несущего за него полную ответственность эксперта. Кроме того, за дачу заведомо ложного заключения эксперт несёт ответственность по ст. 307 УК РФ.

Заключение эксперта – это представленные в письменном виде содержание исследования и выводы по вопросам, поставленным перед экспертом лицом, ведущим производство по делу, или сторонами. При необходимости разъяснения или уточнения данного заключения после его получения эксперт может быть допрошен, то есть, обязан дать показания.

Заключение специалиста – это представленное в письменном виде суждение по вопросам, поставленным перед специалистом сторонами. Его показания – это сведения, сообщённые им на допросе об обстоятельствах, требующих специальных познаний, а также разъяснение своего мнения в соответствии с действующим законодательством.

Вещественные доказательства (ст. 81 УПК РФ) – это обнаруженные и закрепленные в предусмотренном законом порядке объекты материального мира, свойства, качества, происхождение и использование которых имеют значение для разрешения уголовного дела. Это любые предметы, которые выступили орудиями, оборудованием или иными средствами совершения преступления или сохранили на себе следы преступления; деньги, ценности и иное имущество, полученные в результате совершения преступления; иные предметы и документы, которые могут служить средствами для обнаружения преступления и установления обстоятельств уголовного дела.

Замечание. Вещественные доказательства – это своего рода «немые свидетели», которые объективно, в силу своих качеств и связей с другими обстоятельствами служат средством к установлению относящихся к делу фактов. Фактические данные, источником которых выступает материальный объект, могут быть установлены свойствами, качествами самого этого объекта (нож, пистолет, фальсифицированный документ); принадлежностью объекта в сочетании с его местонахождением (предмет, принадлежащий обвиняемому, обнаруженный на месте происшествия, похищенное имущество в квартире обвиняемого).

Собиранию вещественных доказательств, служат, чаще всего, такие следственные процессуальные действия, как обыск, выемка, осмотр, а для IT-преступлений также и следственный эксперимент. Обнаруженный в ходе процессуальных действий предмет, имеющий признаки вещественного доказательства обследуется и осматривается. Только после этого он может быть приобщён к делу в качестве вещественного доказательства постановлением следователя, лица, производящего дознание, или определением суда.

Важным моментом при использовании цифровых доказательств или вещественных доказательств, получаемых из цифровых устройств (смартфонов, ЭВМ, фотока-

мер, оргтехники, устройств навигации и др.) и машинных носителей информации является вопрос отнесения к вещественным доказательствам.

А по уголовным делам о преступлениях в сфере экономики статья 81.1. УПК РФ предусматривает особый порядок признания предметов и документов вещественными доказательствами. Закон строго определяет: составы экономических преступлений, на которые распространяются нормы права; сроки вынесения постановления о признании вещественными доказательствами предметов и документов; возможность владельцу документов снять за свой счёт копии с изъятых документов, в том числе с помощью технических средств в ходе досудебного производства.

Замечание. Вещественные доказательства должны храниться при уголовном деле и по ходу движения уголовного дела передаются вместе с ним из одного органа в другой (ч. 1 ст. 82 УПК РФ). Вполне возможно передавать с делом один или несколько цифровых носителей информации (например, DVD или BD-R компакт-дисков), зарегистрированных и приобщённых к делу установленным порядком, но нельзя в силу объективных причин хранить саму локальную сеть корпорации, или сохранить всю информацию в ней обрабатываемую.

Действия же должностных лиц органов предварительного расследования и суда по хранению и дальнейшей судьбе вещественных доказательств определяется законом в зависимости от их наименования.

Как для вещественных доказательств аналогового мира, так и для цифровых, любая утрата, повреждение либо нарушение процедуры обнаружения, изъятия, осмотра, приобщения к материалам уголовного дела вещественных доказательств – явление необратимое, которое означает невозможность воспроизведения данного вещественного доказательства.

При вынесении приговора, а также определения или постановления о прекращении уголовного дела решается вопрос о вещественных доказательствах в соответствии с требованиями ч. 3 ст. 81 УПК РФ.

Протоколы следственных действий и судебного заседания (ст. 83 УПК РФ) и иные документы (ст. 84 УПК РФ) также являются источниками доказательств, то есть средствами установления обстоятельств совершения преступления. Как процессуальные носители информации о подлежащих установлению обстоятельствах они не однородны по своему содержанию.

Замечание. Фиксируя ход и результаты каждого следственного и судебного действия, протоколы являются обязательной формой закрепления фактических данных, без которых эти данные не могут быть допущены в качестве доказательств по уголовному делу.

Нарушение установленных правил и форм составления протоколов влечет лишение доказательственного значения удостоверяемых ими обстоятельств и фактов. Процессуальная процедура составления протоколов обеспечивает полноту и достоверность закреплённых в них фактических данных.

Признаками протоколов являются: фиксация результатов следственных действий; удостоверение непосредственного восприятия фактических обстоятельств дознавателем, следователем, прокурором, судом и другими участниками следственного действия; составление их в письменной форме; строгое соответствие их содержания диспозиции нормы уголовно-процессуального права.

Письменные акты (справки, характеристики, протоколы проверок, акты аудита, распечатки журналов регистрации и контроля и т. д.), фонограммы, схемы сети, чертежи устройств или планы поэтажного размещения как иные документы отличаются от аналогичных приложений к протоколам следственных и судебных действий тем, что

они составляются не в процессе указанных действий, а обнаруживаются (обыск, осмотр), изымаются или истребуются (запрашиваются) при предварительном расследовании или судебном рассмотрении уголовного дела, либо могут являться частью результатов оперативно-разыскной деятельности (далее – ОРД), в том числе материалами оперативно-технических мероприятий[10].

Важно: Не могут считаться доказательствами протоколы процессуальных действий, не относящихся к следственным, то есть не направленных на собирание, проверку, оценку доказательств (например, протоколы ознакомления), а также сами по себе протоколы и акты, составленные вне уголовного процесса (например, протоколы аудита, акты оценки защищённости, административные протоколы). Такие документы могут обрести доказательную силу будучи официально полученными: истребованными, изъятыми и прошедшими процессуальную процедуру осмотра – в качестве приложения к протоколу осмотра.

К протоколам в некоторых случаях, а для IT-преступлений – как правило, прилагаются машинные носители информации с электронными журналами (log'и), файлами реестров ОС, планами (схемами, рисунками), фотографии и снимки экранов (screenshot'ы), звуко- и видеозаписи и т.п. И только вместе с протоколом, будучи указаны в нём, они имеют доказательственную силу.

Таким образом, к иным документам (как самостоятельным средствам доказывания) относятся разнообразные по содержанию и форме документы. Их объединяет то, что удостоверяемые или излагаемые в них обстоятельства и факты имеют значение для уголовного дела.

Особенности таких документов:

- они составляются, как правило, за пределами следственных действий, независимо от производства по уголовному делу;
- могут иметь не только письменную, но и иную, в том числе электронную форму;
- составляются учреждениями, предприятиями, организациями, должностными лицами и гражданами, которые могут и не быть участниками по уголовному делу;
- в случае утраты или порчи их можно восстановить.

Собирание иных документов осуществляется путём их:

- истребования органами расследования и судом;
- представления по инициативе лиц или организаций;
- производства обыска, выемки или осмотра.

Очевидно в ряде ситуаций при предварительном расследовании компьютерных преступлений существует значительная неопределённость в вопросе где и какие следственные действия проводить, какие документы и в каких организациях изымать, здесь и далее по тексту авторы постараются дать всестороннее представление читателю по данному вопросу и вариантам его решения.

В данном параграфе лишь ограничимся целесообразно с рекомендацией об отдании следователем (дознавателем) органу дознания поручения о проведении ОРД и ОТМ с задачей поиска лиц, организаций и объектов информатизации и связи (интер-

[10] См. *Ковалев С. Д., Полуянова Е. В.* О соотношении понятий оперативно-розыскных мероприятий и оперативно-технических мероприятий // Борьба с пенитенциарной преступностью: опыт, проблемы, перспективы: материалы межвуз. науч.-практ. конф. Владимир, 2013. С. 69.

нет-провайдеров), обладающих какой-либо фактологической информацией или данным, связанными с инцидентом и компьютерным преступлением.

1.1.4. Цифровые и электронные доказательства

Цифровые и электронные доказательства как отдельный вид вещественных доказательств. Особенности российской и международной практики и технического регулирования в сфере цифровых доказательств.

Одновременно с развитием информационных технологий возрастает многообразие объектов, предназначенных для поддержания вычислительных процессов: персональные компьютеры, ноутбуки, планшеты, умные часы, смарт-браслеты, смартфоны, бытовые умные устройства – так называемый «интернет вещей» (IoT), маршрутизаторы, устройства беспородного доступа, серверы различных типов и видов, в том числе распределённые системы, построенные по принципу облачных технологий.

Все эти устройства предназначены для работы с цифровыми данными. Причём в случае с облачными хранилищами компьютерная информация хранится и обрабатывается уже не в одном месте, а «в нескольких центрах данных в различных географических точках».[11]

При этом осмотр и предварительное исследование:

- средств вычислительной техники, обнаруженных на месте происшествия либо в ходе обыска;
- информации, хранящейся на удалённых вычислительных ресурсах, в том числе построенных по принципу облачных технологий;
- цифровых данных, передающихся по компьютерным сетям,

значительно расширяют возможности процесса доказывания по уголовным делам, поскольку позволяют собирать криминалистически значимую компьютерную информацию о событиях или действиях, отражённую в материальной среде, в процессе её возникновения, обработки, хранения и передачи и представляющую собой цифровые следы.[12]

С криминалистической точки зрения можно говорить об особом виде доказательств – цифровых доказательствах.

По мнению зарубежных учёных-криминалистов к цифровым доказательствам (*англ. – digital evidence*) относятся данные в любом виде представления, которые можно извлечь из компьютерных (цифровых) систем для использования в доказывании, подтверждения либо опровержения проверяемых фактов и обстоятельств.[13]

Близкое, по сути, определение предлагают и российские криминалисты. Так, по мнению В.Б. Вехова [115], электронные доказательства – это любые сведения (сообщения, данные), представленные в электронной форме, на основе которых суд, прокурор, следователь, дознаватель в определённом процессуальным законодательством порядке

[11] См. Introduction to Cybercrime. United Nations Office on Drugs and Crime // https://www.unodc.org/e4j/en/tertiary/cybercrime.html (дата обращения 11.07.2021).

[12] См. *Россинская Е.Р., Семикаленова А.И.* Основы учения о криминалистическом исследовании компьютерных средств и систем как часть теории информационно-компьютерного обеспечения криминалистической деятельности // Вестник Санкт-Петербургского университета. Право. Том 11, вып. 3, 2020. – С.753. (с. 745–759).

[13] См. *Maras Marie-Helen*, Cybercriminology: Oxford University Press, 2016. P. 44.

устанавливает наличие или отсутствие обстоятельств, подлежащих доказыванию при производстве по делу, а также иных обстоятельств, имеющих значение для правильного рассмотрения и разрешения дела.[14]

Цифровые следы являются следами материальными, так как, будучи оставленными в результате определённых событий, отражаются на материальных объектах, хотя в некоторых случаях период их существования весьма невелик.

По происхождению цифровые следы являются технологическими, поскольку формирование данных следов обусловлено спецификой реализации информационных технологий. Информационная составляющая становится доступной для восприятия только после их интерпретации с помощью прикладного программного обеспечения и с использованием средств вычислительной техники и ввода-вывода (как микрофлора через микроскоп).

Поэтому в процессе поиска и изъятия цифровых следов следователь (дознаватель) практически не использует чувственную форму познания.

Собирание цифровых следов производится в процессе следственных действий вне зависимости от стадии (до возбуждения уголовного дела или после такого возбуждения) с применением специализированных программно-технических комплексов и программных средств[15], разработанных для криминалистических задач: *Belkasoft Evidence Center, «Мобильный Криминалист», Elcomsoft Premium Forensic, Forensic Assistant;* для инженерно-технологических нужд *ACELab PC-3000, «Урок»/«Урок-9М»*; для проведения аудита (контроля) *МКА-ИБИС*, а также программные комплексы с открытым кодом: *Kuiper Digital Investigation Platform, Wireshark, Kali (BackTrack) Linux* и ряд других подобных.

С учётом этого при проведении следственных действий требуется обязательное применение специальных технических средств, что обусловливает многократно возрастающую роль специалиста и требований, предъявляемых к его компетенции.[16]

Только грамотно организованная работа по поиску, обнаружению и предварительному исследованию цифровых следов, имеющих криминалистическое значение, позволяет непосредственно на месте получить сведения о способах преступления, обнаружить, зафиксировать и изъять (в идеале — копировать) на электронном носителе информации эти цифровые следы, выявить иные обстоятельства происшествия.

Важно: Большинство компьютерных преступлений совершается в условиях неочевидности, когда потерпевший сталкивается с наступившими в результате совершённого деяния негативными последствиями, например, с утечкой конфиденциальной информации либо с несанкционированным списанием денежных средств со своего банковского счета, но ни способ преступления, ни преступник не известны.

В этом случае формальный подход к следственному действию может повлечь безвозвратную утрату доказательственной информации, что обусловлено, в первую очередь, такими свойствами цифровых следов как высокая скорость модификации в вычислительных системах, а также возможностями их уничтожения либо фальсификации с целью сокрытия преступления.

[14] См. *Вехов В.Б.* Электронные доказательства: проблемы теории и практики // Правопорядок: история, теория, практика. № 4 (11), 2016. – С. 46-50.

[15]Авторы указывают только российские инструментальные средства, сведения о которых опубликованы в сети «Интернет», в т.ч. в «Выписке из перечня средств защиты информации, сертифицированных ФСБ России». URL: http://clsz.fsb.ru/files/download/svedeniya_po_sertifikatam_04112022.doc (дата обращения: 12.11.2022).

[16] См. *Рядовский И. А.* Компетенции специалиста по работе с цифровыми следами при производстве следственных действий // Законы России. Опыт. Анализ. Практика, № 9, 2020. С. 94–100.

Международный опыт по регламентации работы с цифровыми следами преступления подтверждает значимость этой проблемы. Так, в 2012 году Международная организация по стандартизации (ИСО) и Международная электротехническая комиссия (МЭК) опубликовали международные стандарты, касающиеся обращения с цифровыми доказательствами[17]. В 2014 году для добровольного применения был переведён, гармонизирован и утверждён российский документ технического регулирования – национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 27037-2014 «*Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме*», идентичный указанному международному стандарту ИСО и МЭК[18].

Указанным стандартом предусмотрены четыре этапа обращения со свидетельствами, представленными в цифровой форме: идентификация, сбор, получение, сохранение. Рассмотрим эти этапы подробнее.

1. В ходе этапа идентификации производится выявление средств вычислительной техники, электронных носителей информации и иных устройств, которые могут содержать цифровые следы преступления либо иную криминалистически значимую информацию. Одновременно проводится анализ на предмет определения приоритетов в изучении устройств с учётом степени риска утраты хранящейся на них информации. Например, данные, содержащиеся в оперативной памяти работающего компьютера, характеризуется высокой степенью волатильности[19], в то время как состояние данных, хранящихся на внешнем энергонезависимом электронном носителе информации, не подключенном к компьютеру, стабильно. Но если такой носитель информации подключен к работающей компьютерной системе, неверная оценка в очерёдности работы с обнаруженными на месте следственного действия объектами может привести утрате доказательств при отключении электронного носителя информации от компьютера либо вследствие обесточивания компьютера в том случае, если данные на носителе информации были зашифрованы.

2. и 3. Собирание цифровых следов и получение цифровых «слепков» – дальнейший этап работы с данными. Базовый криминалистический принцип при работе с компьютерной техникой и электронными носителями информации, – сохранение в неизменном виде хранящихся на них цифровых следов.

На этапе сбора принимается решение об изъятии обнаруженных объектов для последующего осмотра либо проведения экспертизы. На такое решение могут влиять различные факторы. Например, как было указано выше, выключение работающего компьютера для изъятия приведёт к потере информации, содержащейся в оперативной памяти, либо к утрате доступа к зашифрованным данным на носителях информации. В то же время изъятию средств вычислительной техники могут препятствовать иные обстоятельства, такие как недопустимость приостановления непрерывного производственного процесса.

При необходимости осмотреть работающую систему, действия по манипуляции с данными должны быть строго выверены и отображены в протоколе. В иных случаях

[17] ISO/IEC 27037. Guidelines for identification, collection, acquisition and preservation of digital evidence // URL: https://www.iso.org/ru/standard/44381.html (дата обращения 11.07.2021).

[18] ГОСТ Р ИСО/МЭК 27037–2014. Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме // URL: http://docs.cntd.ru/document/1200112857 (дата обращения 11.07.2021).

[19] См. комментарий в сноске на стр. 6.

исследование информационных объектов производится посредством осмотра их копий, созданных с использованием специальных криминалистических средств – копировщиков и блокираторов, исключающих возможность внесения изменений в компьютерную информацию, хранящуюся на изъятых компьютерах и носителях.[20]

На этапе получения данных необходимо скопировать, сохранить данные из обследуемой системы. В случаях когда есть достаточные материальные криминалистические резервы (аналогичные накопители требуемого объёма), но имеется дефицит времени применяют и диск-дубликторы. Современные аппаратно-программные комплексы (копировальщики-дубликаторы[21]), хоть и менее функциональных указанных программ и комплексов, но упрощают процесс снятия побайтных копий, и зачастую помимо обеспечения безопасного процесса копирования информации, обладают рядом дополнительных возможностей, реализующих криминалистическую составляющую их функциональности, а именно верифицировать созданную копию и документировать результаты основных этапов работы в отдельный файл, в том числе фиксировать основные характеристики диска-источника, включая его модель и серийный номер, дату и время создания копии, контрольную сумму (хэш-значения) образа диска.

Ещё один криминалистический принцип при работе с цифровыми следами, на необходимость соблюдения которого прямо указано в стандарте ISO/IEC 27037, – это чёткое и полное отражение в протоколе манипуляций, производимых как с осматриваемыми физическими объектами (средствами вычислительной техники, электронными носителями информации), так и непосредственно с объектами информационными. Так, при случайном включении мобильного телефона данный факт регистрируется в журнале событий операционной системы устройства. Для обычного пользователя эта информация недоступна, однако при углублённом исследовании устройства с использованием специальных криминалистических средств данное событие будет выявлено и, в случае если оно не было отражено в протоколе, может рассматриваться как несанкционированный доступ к компьютерной информации, что, свою очередь, может повлечь признание результатов последующих осмотров данной техники недостоверными, а проведённых судебных экспертиз – недопустимыми доказательствами.

Если изготовление образов (побитовых копий) дисков невозможно, например, приходится осматривать работающую компьютерную систему либо размер диска слишком большой, а время ограничено, допустимо копирование значимых для расследования данных на логическом уровне, то есть файлов и папок либо содержимого адресного пространства диска. Учитывая, что при работе с цифровыми следами в активной функционирующей системе невозможно обеспечить неизменность информации, все манипуляции, связанные с поиском, изучением и копированием криминалистически значимой информации, также должны быть детально задокументированы, а в протоколе необходимо указать причины, которые повлияли на принятие такого решения.

4. На заключительном этапе – сохранении – обеспечивается сохранность полученных цифровых следов и средств вычислительной техники, в которых они могут содержаться. Особенность этого этапа в том, что он распространяется на все предыдущие этапы, начиная с идентификации, и на любые последующие исследования изъятой

[20] См. *Чекунов И. Г., Голованов С. Ю.* и др. Методические рекомендации по расследованию преступлений в сфере компьютерной информации: учеб. пособие, 2-е изд. / под ред. И.Г. Чекунова. М.: Московский университет МВД России имени В.Я. Кикотя, 2019. – С. 94.

[21] О наиболее часто применяемых и ввозимых в Россию иностранных дубликаторах носителей информации // URL: https://декларации-соответствия.рус/kompaniya/lan-proekt-inn-7723171378/

компьютерной техники и цифровых следов с целью предупреждения их повреждения и фальсификации.

Анализируя рассмотренные положения национального ГОСТ и международного стандарта ISO/IEC 27037, можно констатировать, что рекомендации, изложенные в нём, логичны и разумны, сложились из многолетней практики, подтверждаются российскими тактиками и могут быть адаптированы для национальных процессуальных законодательств. При этом необходимо отметить, что отечественное уголовно-процессуальное законодательство в большей части в процедурном плане может обеспечить соблюдение технических рекомендаций по обращению с цифровыми следами в ходе невербальных следственных действий. Так, ч. 2 ст. 164.1 УПК РФ предусмотрено обязательное участие специалиста в следственных действиях, в ходе которых производится изъятие электронных носителей информации. Таким образом, с одной стороны, обеспечивается выполнение рекомендаций относительно привлечения к работе с цифровыми следами компетентного технического специалиста, а с другой, – требование о детальном документировании манипуляций, произведённых с цифровыми устройствами и объектами.

Таким образом, при производстве невербальных следственных действий, в ходе которых осуществляется работа с цифровыми следами, важно соблюдать следующие правила:

- обеспечивать неизменность цифровых следов, хранящихся на осматриваемых устройствах;
- для поиска, изучения, изъятия и иных манипуляций с цифровыми следами привлекать специалиста, имеющего соответствующую подготовку;
- документировать в полном объёме действия по изъятию, хранению и передаче цифровых следов, доступу к ним и, соответственно, к устройствам, на которых они содержатся, обеспечивать их защиту и доступность для дальнейших судебных исследований.

Следует особо отметить значимость подготовительных мероприятий при проведении невербальных следственных действий для дел данной категории. Разумеется, подготовка обязательна при проведении любого следственного действия, однако отсутствие приготовительных мероприятий либо формальный подход к их проведению именно по делам о компьютерных преступлениях могут повлечь наибольший ущерб для расследования, выражающийся в утрате возможностей для сбора доказательств.

Пример. С такой характерной проблемой столкнулись сотрудники Управления ФСБ России по Ставропольскому краю, вскрывшие в 2017 г. организованную преступную группу, промышлявшую сбытом краденного топлива с АЗС. Воровство и сокрытие расхода топлива осуществлялась путём использования вредоносного программного обеспечения (далее – ВПО), внедрённого в систему управления АЗС и позволявшего осуществлять недолив топлива, подделывая электронные значения его учёта, как «фактически» перелитого.

Однако в ходе сбора электронной доказательной базы, допроса свидетелей и подозреваемых выявлено наличие стороннего удалённого сервера управления ВПО в сети Интернет, доступ к которому отсутствовал, что затруднило обоснование фактов его использования для осуществления хищений топлива, а также сбора доказательств причастности обвиняемых к управлению ВПО или организации такого использования ВПО.

Указанное обстоятельство и недостатки в тактике следствия, связанные с несвоевременными мероприятиями по организации сбора и фиксации цифровых доказательств по делу, утрате возможности их получить в рамках оперативно-технических мероприятий, потребовали

неоднократного продления в соответствии с законодательством следственных действий, что может поставить под сомнение судебную перспективу уголовного дела.[22]

Поэтому на этапе подготовки следователю требуется подыскать[23] и привлечь к проведению следственного действия соответствующего специалиста, убедиться в его компетенции, после чего совместно с ним уточнить обстоятельства дела, заранее собрать сведения о дате и времени совершения преступления, местонахождении скомпрометированной компьютерной системы, моделях и характеристиках вычислительных устройств, емкости их жестких дисков, сетевом окружении и т. п. Затем надлежит проверить обеспечение специалиста необходимым оборудованием и программным обеспечением для работы с цифровыми следами. Помимо специальных криминалистических средств, в перечень которых входят, в том числе, программы для снятия снимка оперативной памяти, блокираторы для исследования компьютерной техники, копировщики для копирования жестких дисков, при производстве невербальных следственных действий могут понадобиться переходники и кабели, электронные носители информации для консервирования компьютерных данных, латексные перчатки и иные средства защиты с целью предотвращения оставления специалистом каких-либо следов на осматриваемой технике, специальный упаковочный материал, служащий для безопасного перемещения и хранения компьютерной техники и электронных носителей информации, материал для маркировки портов и кабелей в случае изъятия всех элементов компьютерной сети.

Невербальные следственные действия проводятся для поиска, фиксации и изъятия цифровых следов преступления, которые могут быть обнаружены в местах автоматизированной обработки, хранения и передачи данных с использованием вычислительных мощностей:

- рабочее место преступника (компьютерные устройства, электронные носители информации, средства связи, записи);
- место происшествия (компьютерная система);
- сетевые ресурсы преступника (в локальной сети);
- сетевые ресурсы преступника (в глобальной сети);
- каналы связи преступника (сетевой трафик);
- легальные сетевые ресурсы, используемые в преступной деятельности (почтовые серверы, вычислительные мощности провайдеров хостинга, ресурсы провайдера по предоставлению доступа в интернет и т. п.).

Информация к размышлению. Постановление Координационного совещания руководителей правоохранительных органов Российской Федерации от 17 июля 2020 г. № 1 «*О состоянии работы правоохранительных и контролирующих органов по предупреждению, выявлению, пресечению и расследованию преступлений, связанных с посягательствами на безопасность в сфере использования информационно-телекоммуникационных технологий, включая критическую информационную инфраструктуру Российской Федерации*», вынесенное Председателем координационного совещания Генеральным прокурором Российской Федерации И. В. Красновым, безапелляционно свидетельствует о резко прогрессирующей тенденции роста числа киберпреступлений, зарегистрированных на территории Российской Федерации: с 2013 по

[22] В недоливе бензина обвинили вредоносную программу. Расследуется дело о хищениях на ставропольских АЗС. – Газета «Коммерсантъ» № 167 (6647) от 16.09.2019 (стр. 4).

[23] Найти хорошего специалиста бывает сложно, зачастую следователей не устраивают те или иные специалисты по причине их низкой квалификации, так как с ними запросто может возникнуть ситуация когда дело развалится прямо в суде.

2019 гг. в 20 раз, с 2018 по 1 кв. 2020 гг. в 5 раз, только за январь-март 2020 года было зарегистрировано около 102 000 тысяч преступлений, совершенных с использованием информационно-телекоммуникационных средств или в сфере компьютерной информации.[24]

Как отмечают исследователи, в Российской Федерации за последние годы почти каждое 20-е зарегистрированное преступление совершается при помощи использования сети интернет.[25] В свою очередь, социальные сети и мессенджеры нередко становятся особой средой для совершения самых различных преступлений (экстремистской и террористической направленности, незаконного оборота наркотиков, распространения детской порнографии и др.). Это, в первую очередь, связано с широкими функциональными возможностями социальных сетей и мессенджеров, спецификой компьютерно-опосредованной коммуникации, позволяющей личности сохранять свою анонимность и с легкостью публиковать различного рода информацию, которая становится впоследствии доступной широкому кругу лиц. Такие условия раскрывают перед злоумышленниками массу возможностей для реализации своих преступных умыслов посредством использования социальных сетей и мессенджеров. Такое положение дел индуцирует необходимость разрешения проблемных вопросов, связанных с отсутствием унифицированного подхода к обнаружению, фиксации и изъятию цифровых следов из социальных сетей и мессенджеров.

Как известно, обнаружение цифровых следов преступлений, оставленных в социальных сетях и/или мессенджерах, является поисковой деятельностью следователя, которая направлена на сбор криминалистически значимой информации, необходимой для познания истины и правильного разрешения уголовного дела. Обнаружение такой информации возможно посредством нескольких способов:

- поиск информации с использованием технических средств (ПК, ноутбука, электронного планшета и др.) для посещения страницы пользователя социальной сети (интересующий следствие ID), где потенциально содержатся следы преступления с последующей фиксацией и изъятием криминалистически значимой информации. При этом обнаружение криминалистически значимой информации таким способом возможно в случае, если цифровые данные, интересующие органы следствия, находятся в открытом доступе, либо удалось оперативно внедриться[26], например, подписаться на конкретную закрытую группу в социальной сети, в противном случае получение информации таким способом не представляется возможным;
- с электронного устройства подозреваемого/обвиняемого, потерпевшего при помощи авторизации через их аккаунт в социальной сети/мессенджере с их добровольного согласия или только с разрешения суда (ст. 185 УПК РФ). Однако при этом следует иметь в виду, что получение криминалистически значимой

[24] Портал правовой статистики Генеральной прокуратуры Российской Федерации [Электронный ресурс]. – Режим доступа: http://crimestat.ru/analytics (дата обращения: 18.05.2021).

[25] См. *Гужаева В. А., Прокофьева Е. В., Прокофьева О. Ю.* Преступность в сети Интернет: криминологические характеристики. / В. А. Гужаева, Е. В. Прокофьева, О. Ю. Прокофьева // Вестник экономической безопасности. –2019. – № 4 – С.112.

[26] Приказ МВД России № 776, Минобороны России № 703, ФСБ России № 509, ФСО России № 507, ФТС России № 1820, СВР России № 42, ФСИН России № 535, ФСКН России № 398, СК России № 68 от 27.09.2013 «Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд». // СПС «Консультант Плюс».

информации будет возможным только в отношении тех данных, к которым аккаунт конкретного пользователя имеет доступ;

- с электронно-вычислительных мощностей, содержащих информацию о пользователях социальной сети и/или мессенджеров (серверы компаний, предоставляющих услуги пользования конкретной социальной сетью, мессенджером).

В связи с тем, что каждый из вышеперечисленных способов имеет свою специфику, обусловленную как нормами международного права, так и национального законодательства Российской Федерации, то представляется целесообразным рассмотреть в главе 2.3 данного учебного пособия более подробно указанные способы обнаружения цифровых следов преступлений на веб-сайтах (веб-форумах), в социальных сетях и мессенджерах.

1.1.4.1. Жизненные случаи и юридические изъяны

Некоторые юридические «пробелы» в вопросе получения информации с удалённых компьютерных сетей и систем.

Отметим, что в настоящий момент в УПК РФ отсутствует норма, которая бы регламентировала порядок проведения следственного действия, связанного с получением компьютерной информации с удалённых компьютерных сетей и систем[27]. В этой связи на практике при проведении предварительной проверки по сообщению о преступлении, когда доказательственно релевантная информация находится на страницах социальных сетей пользователей в сети Интернет, следователи руководствуются статьями 176 и 177 УПК РФ, то есть осуществляют осмотр и последующую фиксацию и изъятие цифровых следов преступления в рамках проведения такого следственного действия, как осмотр предметов (документов).

Жизненный случай 1. Гражданин А. осуществлял незаконный сбыт наркотических средств и «вербовку» новых членов преступной группы при помощи использования аккаунта в социальной сети «Вконтакте» и мессенджере «Telegram», в частности, посредством размещения объявлений о вакансиях на различных контент-сайтах и каналах в приложении «Telegram», рассылок личных сообщений в социальной сети «Вконтакте»[28].

Обнаружение, фиксация и изъятие цифровых следов преступления в приведённом выше примере осуществлялись в рамках проведения такого следственного действия, как осмотр предметов (документов) в соответствии со ст. 177 УПК РФ.

Вместе с тем отметим, что в соответствии со ст. 164.1 УПК РФ участие специалиста в следственных действиях является обязательным в случаях, когда изъятие и копирование информации осуществляется с электронных носителей. Однако следует констатировать, что положения ст. 164.1 УПК РФ лишь отчасти способствуют опти-

[27] Семикаленова А. И., Рядовский И. А. Использование специальных знаний при обнаружении и фиксации цифровых следов: анализ современной практики // Актуальные проблемы российского права. – 2019. – № 6 (103). – С.180.

[28] Приговор Евпаторийского городского суда Республики Крым № 1-456/2019 от 24 декабря 2019 г. по делу № 1-456/2019. См., также, например: Приговор Новочебоксарского городского суд Чувашской Республики № 1-456/2019 от 19 декабря 2019 г. по делу № 1-456/2019; Приговор Стерлитамакского городского суда Республики Башкортостан № 1-567/2019 от 11 декабря 2019 г. по делу № 1-567/2019. [Электронный ресурс]. – Режим доступа: https://sudact.ru/. (Дата обращения: 21.07.2020).

мизации и эффективности проведения следственных действий, связанных с изъятием компьютерной и/или цифровой информации.

Во-первых, положения ст. 164.1 нельзя экстраполировать на удалённое получение информации с сайта в сети интернет. Это связано с тем, что согласно ст. 2 ФЗ «Об информации, информационных технологиях и о защите информации» сайт в сети Интернет – это «*совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети "Интернет" … по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети "Интернет"*»[29]. Однако, при осмотре сайта в сети интернет фиксация и последующее изъятие информации осуществляется не с электронно-вычислительных мощностей (серверов), при помощи которых поддерживается работоспособность определённого контент-сайта, а из информационно-телекоммуникационной сети интернет, отображающей информацию, хранящуюся в памяти устройств хранения информации (жёстких дисков серверов) электронно-вычислительных мощностей. В свою очередь, в ст. 164.1 УПК РФ ничего не сказано о получении информации с удалённых серверов, а речь идет лишь о изъятии и копировании информации с электронных устройств. Следовательно, в отношении обнаружения, фиксации и изъятия цифровых следов из сайтов в сети интернет, в частности, со страниц социальных сетей пользователей, в УПК РФ образовалась «правовая лакуна».

Во-вторых, согласно ч. 2 ст. 164.1 участие специалиста является обязательным, в частности в случаях, когда изъятию подлежат электронные носители информации. Однако диспозицию ч.2 ст. 164.1 УПК РФ вряд ли можно признать успешно сформулированной, так как анализ следственной практики показывает, что необходимость в привлечении специалиста к участию в следственных действиях, связанных с изъятием электронных носителей информации, возникает довольно редко.

Для непосредственного изъятия самого электронного носителя информации (мобильного телефона, электронного планшета, ноутбука и др.), например, в рамках производства выемки (ст. 183 УПК РФ) участие специалиста является вовсе не обязательным, так как в ряде случаев следователь в состоянии сам надлежащим образом произвести выемку электронного носителя информации и без участия специалиста, если изъятие электронного устройства не представляет сложностей и не требует для этого использования специальных знаний, которыми следователь не обладает. В этой связи С. Б. Россинский совершенно справедливо отмечает, что «*Участие специалиста в следственных действиях не является безусловным. Обладая необходимыми специальными знаниями и умея применять их на практике, следователь вполне может обойтись и без его помощи*»[30].

В то же время, по нашему мнению, участие специалиста обязательно, когда следователю нужно осуществить изъятие компьютерной и/или цифровой информации либо непосредственно с электронного носителя (ПК, мобильного телефона, электронного планшета и т. д.), либо с удалённых серверов (например, с определённого контент-сайта), а не самого электронного устройства (системного блока ПК, ноутбука, мобильного телефона и т. д.), так как фиксация и изъятие цифровых данных предопределяет

[29] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 01.10.2021) // СПС «Консультант Плюс».
[30] Россинский С. Б. Следственные действия: монография. – М.: Норма, 2018. – С.118.

необходимость соблюдения определённого порядка действий со стороны правоприменителя, вызванного спецификой данных объектов, с целью обеспечения их сохранности, достоверности и дальнейшей возможности приобщения в качестве вещественных доказательств по делу [62].

Следует также отметить, что в соответствии с Примечанием к ст. 272 УК РФ под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Однако, как представляется, такое определение компьютерной информации является не совсем корректным, так как процессором электронно-вычислительных мощностей могут обрабатываться цифровые данные, которые вовсе не обязательно должны быть представлены в форме электрических сигналов. Так, например, наверняка встречавшиеся взгляду нашего читателя за последнюю неделю всевозможные товары, продукты, документы или реклама, содержащие товарный штрихкох (*EAN-13*), *data matrix* или *QR*-код и др., позволяющие стандартизированно кодировать различные виды информации.[31] Причём, штриховой код может быть зафиксирован не на электронный, а иной носитель информации (бумагу, дерево, полимер и др.), да и наноситься он может кисточкой и краской без участия компьютера, т. е. в данном случае от цифровой информации (например, QR-кода) не будет исходить каких-либо электрических сигналов, но эта цифровая информация также может быть обработана любым электронным устройством (ноутбуком, смартфоном, электронным планшетом), позволяющим произвести оптическое считывание и декодирование.

Более того, само понятие «электрические сигналы» по своей сути является довольно широким. Связано это с тем, что при помощи электрических сигналов могут передаваться как цифровые, так и аналоговые данные (радио-/ телевещание), которые могут[32], но в общем случае не предназначены для их обработки процессором вычислительной техники (компьютером), а направлены для получение несущей частоты передатчика иным электронным устройством, например радиоприёмником или телевизором.

Наряду с этим также считаем, что следует разграничивать компьютерную информацию, которая может быть выражена как в аналоговом, так и в цифровом формате, но

[31] Количество различных «одномерных» (1D) штрихкодов велико: Code-11, Code-2of5 Inerleaved, Code-39, Code-39 Full ASCII, Code-128, GS1-128 (UCC/EAN-128), Фармакоды и другие. Длина полосы кода состоящей из чёрных и белых чёрточек напрямую влияет на максимальный объём кодируемой информации. Естественно, что чрезмерно длинные штрихкоды неудобны. Для кодирования большего объёма информации были придуманы несколько-полосные или двумерные (2D) штрихкоды: (Micro) QR Code, Data Matrix, Aztec, Codablock-F, Maxicode, (Micro) PDF417, Han Xin и другие.

Наше государство активно внедряет информационные технологии в повседневную жизнь: «Штриховой код, как технология автоматической идентификации и сбора данных, широко используется при осуществлении платежей физическими лицами. Использование символов штрихового кода на платёжном документе позволяет осуществить автоматизированный ввод реквизитов платежа и этим снизить трудоёмкость проведения операции приёма платежа, уменьшить количество ошибок, допускаемых клиентами и сотрудниками организаций, принимающих платежи, и сократить время оформления платежа. Для задания единых правил использования штрихового кода как поставщиками услуг при выставлении счетов (печати платёжных документов), так и принимающими платежи организациями возникла необходимость разработки общего стандарта.», – национальный стандарт Российской Федерации ГОСТ Р 56042-2014 «Двумерные символы штрихового кода для осуществления платежей физических лиц» // http://docs.cntd.ru/document/1200110981.

[32] См. технологию SDR – Software Defined Radio.

которая при этом должна подлежать обработке процессором электронно-вычислительных мощностей (компьютеров), от цифровой информации, которая может быть обработана как при помощи электронно-вычислительной техники (жёсткие диски, USB-накопители, CD-диски и др.), так без неё[33].

Принимая во внимание тот факт, что при помощи компьютерных средств может обрабатываться как аналоговая, так и цифровая информация, по нашему мнению, под компьютерной информацией следует рассматривать любые данные, сведения, сообщения (аналоговый/цифровой формат), которые обрабатываются процессором электронно-вычислительных мощностей.

Что касается поисковой деятельности следователя, связанной с обнаружением криминалистически значимой информации, находящейся на страницах пользователей социальных сетей, то представляется также целесообразным привлечение специалиста в области компьютерно-информационной безопасности для содействия в поиске и обнаружении доказательственно пригодной информации с удалённых серверов в соответствии со ст. 168 УПК РФ.

Такая необходимость обусловлена тем, что посредством визуального осмотра контент-сайта, не требующего использования специальных знаний, можно обнаружить лишь небольшую часть цифровых данных, интересующих органы следствия. Однако для получения детализирующей информации о цифровых данных, содержащихся на контент-сайте (странице пользователя социальной сети), необходимо использовать компилируемые программные модули, а в ряде случаев отдельные программные продукты, позволяющие выявить исходящие с контент-сайта цифровые данные, например, выраженные в виде скрытых ссылок. Более того, для обнаружения криминалистически значимой информации зачастую представляется необходимым производить анализ исходного кода страницы сайта.

Жизненный случай 2. Так, в Следственное управление по Северо-Западному административному округу г. Москвы от гражданина *N* поступило сообщение о совершении преступления, предусмотренного ст. 280 УК РФ. По факту поступившего сообщения в рамках осмотра предметов (документов) в соответствии со ст. 177 УПК РФ следователем осуществлялась проверка содержания контент-сайта «*XXXXXXX*» на предмет наличия/отсутствия в нём призывов к осуществлению экстремистской деятельности, предусмотренных ст. 280 УК РФ. В ходе следственной проверки было обнаружено, что на осматриваемом контенте помимо экстремистских материалов также размещена информация, способствующая незаконному сбыту наркотических средств, которая выражена в виде всплывающих окон. По факту обнаружения признаков составов преступлений, предусмотренных ст. 280 УК РФ, 228.1 УК РФ, было возбуждено уголовное дело.

Специалисту, участвующему в производстве следственного действия, удалось посредством анализа исходного кода страницы сайта определить путь к контенту сайта, из которого данная информация поступала для последующего размещения на проверяемом в ходе осмотра сайте.

В дальнейшем следствию удалось доказать не только причастность к совершённому преступлению, предусмотренному ст. 280 УК РФ, гражданина *A*, но и причастность к совершённому преступлению, предусмотренному ст. 228.1 УК РФ, гражданина *B* – обладающего правами администратора сайта, на след которого удалось выйти благодаря ответственному подходу спе-

[33] Например, декодирование QR-кода может быть проведено лицом, обладающим специальными знаниями в соответствующей области, и без использования электронно-вычислительной техники. См. Читаем QR код [Электронный ресурс] https://habr.com/ru/post/127197/, (Дата обращения: 21.11.2022).

циалиста при проведении осмотра исходного кода страницы сайта, проверяемого в ходе следственного осмотра[34].

Как видно из вышеприведённого примера, обнаружение цифровых следов преступлений, связанных с незаконным сбытом наркотических средств, оказалось возможным только лишь посредством анализа исходного кода страницы сайта, анализ которого невозможен без использования специальных знаний из области информационно-компьютерной безопасности. В этой связи привлечение специалиста для оказания помощи следователю в обнаружении доказательственно релевантной информации представляется нам также целесообразным.

Другой не менее важной проблемной собирания цифровых следов преступлений из социальных сетей и мессенджеров является отсутствие международно-правового акта общеобязательного характера по противодействию киберпреступности и (или) обеспечению кибербезопасности, который бы регулировал вопросы, связанные в том числе с собиранием криминалистически значимой информации с хостинг-провайдеров – иностранных компаний, предоставляющих услуги пользования конкретной социальной сетью или мессенджером.

Отметим, что у Российской Федерации имеется ряд заключённых договоров с иностранными государствами, в том числе регламентирующих оказание международно-правовой помощи сторонам при расследовании уголовных преступлений[35]. При этом следует учитывать складывающуюся международную обстановку и осознавать реальную возможность получения информации, интересующей органы следствия нашей страны, от иностранного государства. Проблемным является тот факт, что международные запросы могут быть оставлены без ответа[36], что связано с отсутствием международно-правовых норм, регулирующих порядок передачи компьютерной и/или цифровой информации между иностранными государствами.

Жизненный случай 3. Так, в ходе предварительного расследования уголовного дела СО УМВД России по г. Элисте по признакам преступления, предусмотренного ч. 1 ст. 272 УК РФ, было установлено, что 11 августа 2016 неизвестное лицо отправило сообщение от email: «xxxxx.x*xxxx@yyyyyyy.zzz*» на электронную почту Управления Федерального казначейства Республики Калмыкия, содержащее вредоносный программный код, который впоследствии проник в систему программно-аппаратного комплекса учреждения и модифицировал служебные файлы, тем самым частично парализовав деятельность всего учреждения.

Согласно полученным данным НЦБ Интерпола МВД России, установочные данные электронного почтового ящика «xxxxx.x*xxxx@yahoo.com*» могут быть получены от правоохранительных органов США в рамках оказания международной правовой помощи при расследовании уголовных преступлений.

Однако 22 ноября 2016 года предварительное следствие по данному уголовному делу было приостановлено в связи с неустановлением лица, подлежащего привлечению в качестве обвиняемого п.1 ч.1 ст. 208 УПК РФ)[37].

[34] Материалы из архива Лаборатории Касперского, 2015 – 2020 г.

[35] Официальный сайт Министерства юстиции Российской Федерации [Электронный ресурс]. – Режим доступа: https:// minjust.gov.ru/. (Дата обращения: 21.11.2021).

[36] *Ватрушкин А. А.* Правовые основы обеспечения кибербезопасности критической инфраструктуры Российской Федерации // Евразийская адвокатура. № 6 (31),2017. – С. 78–84.

[37] *Колычева А. Н., Васюков В. Ф.* Расследование преступлений с использованием компьютерной информации из сети Интернет: учебное пособие/ под ред. А. Г. Волеводза. – М.: Проспект, 2020. – С.25-26.

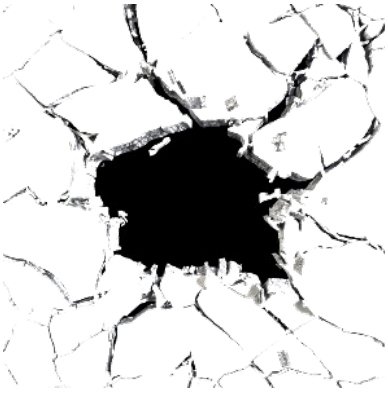
Как видно из вышеприведённого примера, запрос органов, ведущих расследование преступления на территории Российской Федерации, в правоохранительные органы США остался без ответа, в связи с чем предварительное расследование было приостановлено, так как дальнейший сбор доказательств оказался невозможен.

Следует отметить, что ныне действующая Будапештская Конвенция «*О преступности в сфере компьютерной информации*»[38] (далее – Будапештская Конвенция),

во-первых, по своей сути является устаревшей, так как закреплённые в ней положение едва ли способны отвечать реалиям следственной практики. В Конвенции рассматриваются преступления против конфиденциальности, целостности и доступности компьютерных данных и систем, подлог и мошенничество с использованием компьютеров, преступления, связанные с содержанием данных, в особенности преступления, связанные с детской порнографией, а также преступления, связанные с нарушением авторского и смежных прав (глава II, раздел I, части 1-4). Однако, как отмечалось нами выше, на сегодняшний день перечень составов преступлений, которые совершаются при помощи использования компьютерных средств и систем, в частности, посредством использования сети интернет, является гораздо шире, чем перечень видов преступлений, регулируемых Будапештской Конвенцией, по которым предусмотрено международное сотрудничество стран-участниц в сфере противодействия киберпреступности.

Анекдот. Проходит к концу совещание IT-специалистов с руководством компании «*X*». Последним выступает начальник отдела безопасности, который на повышенных тонах обращается к генеральному директору, в надежде на понимание:

–...Вы поймите, у нас дыра в безопасности!



– Слава Богу! Хоть что-то в этой компании в безопасности.

Во-вторых, отказ Российской Федерации от подписания Будапештской Конвенции нам представляется вполне логичным и правомерным, так как прописанные в п. «b» ст. 32 Будапештской Конвенции положения противоречат, в частности, ст. 4, ст. 23, п.1 ст. 24 Конституции РФ, а также ФЗ «*О персональных данных*»[39], так как п. «b» ст. 32 Будапештской Конвенции предусматривает возможность получения одной из стран без согласия другой страны компьютерных данных, хранящихся на серверах иностранного государства.

Исходя из вышеизложенного, получение криминалистически значимой информации с хостинг-провайдеров – иностранных компаний, предоставляющих услуги пользования социальной сетью или мессенджером (Facebook, Instagram, WhatsApp, Viber и др.), на практике вызывает сложности у правоохранительных органов, что, безусловно, препятствует расследованию преступлений, связанных с получением компьютерной и/или цифровой информации с хостинг-провайдеров – юридических лиц, зарегистрированных на территории иностранных государств.

[38] Конвенция «О преступности в сфере компьютерной информации» (ETS № 185) от 23.11.2001 (с изм. от 28.01.2003) // СПС «Консультант Плюс».

[39] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. от 02.07.2021) // СПС «Консультант Плюс».

Следует отметить, что по указанному вопросу Российская Федерации выступала с инициативой Проекта Конвенции ООН «*О сотрудничестве в сфере противодействия информационной преступности*» в 2017 году в Вене[40]. Проект по своей сути выступает альтернативой Будапештской Конвенции. В проекте отсутствуют аналогичные Будапештской Конвенции нормы, которые могут затрагивать безопасность и суверенитет государств и права их граждан (п.b ст. 32 Будапештской Конвенции). Вместе с тем в предложенном Российской Федерацией проекте Конвенции «*О сотрудничестве в сфере противодействия информационной преступности*» ст. 57 предусматривает создание круглосуточного контактного центра («24/7»), который предназначен для оказания экстренной помощи в целях расследования преступлений и сбора доказательств. Принимая во внимание тот факт, что специфика цифровых данных заключается, в частности, в том, что они могут быть уничтожены в довольно короткие сроки. Однако судьба данного проекта, к сожалению, остаётся неизвестной, как и ранее предложенного в 2011 году Российской Федерацией проекта Конвенции «*Об обеспечении международной информационной безопасности*».

Насущная необходимость принятия универсальной Конвенции о сотрудничестве в сфере противодействия информационной преступности не вызывает сомнений, так как её отсутствие в ряде случаев приводит к невозможности сбора цифровых данных, интересующих правоохранительные органы государств, и выступает для них непреодолимым «барьером» в расследовании преступлений. Более того, процесс реализации новой Конвенции после её принятия, очевидно, будет требовать достаточно большого количества времени, так как Конвенция может быть воплощена в жизнь странами-участницами только при условии, если нормы национального законодательства государств не будут препятствовать реализации Конвенции о сотрудничестве в сфере противодействия информационной преступности.

Таким образом, отсутствие международно-правовых норм в сфере противодействия киберпреступности в некоторых случаях затрудняют собирание цифровых доказательств из социальных сетей и мессенджеров, принадлежащих иностранным юридическим лицам, а в некоторых из них приводит правоохранительные органы Российской Федерации к абсолютной невозможности сбора цифровых доказательств, хранящихся на серверах иностранных компаний.

Вместе с тем, если у органов дознания или следствия возникает необходимость в получении доказательственно пригодной информации со страниц пользователей социальных сетей, представителями которых являются юридические лица, зарегистрированные в Российской Федерации (Вконтакте, Одноклассники и др.), то в соответствии с п. 1 под. 4, 10 ст. 13 ФЗ «О полиции» и п. 2 ст. 6 ФЗ «Об оперативно-розыскной деятельности»[41] в целях предупреждения, выявления и раскрытия преступлений может быть направлен запрос с просьбой предоставить сведения о конкретном пользователе, который интересует следствие [61].

[40] Официальный сайт Министерства иностранных дел Российской Федерации. Проект Конвенции Организации Объединённых Наций «О сотрудничестве в сфере противодействия информационной преступности» от 16 октября 2017 г. [Электронный ресурс]. – Режим доступа: https:// www.mid.ru/. (Дата обращения: 21.11.2021).

[41] Федеральный закон от 07.02.2011 № 3-ФЗ «О полиции» (ред. от 24.08.2021); Федеральный закон от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности» (ред. от 01.07.2021) // СПС «Консультант Плюс».

При этом представители юридического лица – социальной сети имеют право предоставить только те сведения, которые не затрагивают конституционные права человека и гражданина (адрес личной страницы пользователя; дата создания страницы; номер телефона и электронной почты пользователя; IP-адрес, с которых пользователь осуществлял вход на страницу; история изменений пароля, логина (имени пользователя), номера телефона; историю обращений в службу поддержки; история блокировок страницы пользователя).[42] Однако, если есть соответствующая санкция суда (ч. 2 ст. 23 Конституции РФ), то может быть представлена вся интересующая органы дознания или следствия информация о пользователе (ст. 185 УПК РФ, ст. 186[1] УПК РФ) [33] [61].

1.2. Особенности доказательств и доказывания

Особенности доказательств и доказывания в стадии возбуждения уголовного дела о преступлениях, совершённых с использованием информационных технологий.

1.2.1. Участие специалистов, применение специальных средств

Особое значение участия специалистов при сборе и фиксации доказательств и технико-правовые аспекты применения специальных технических средств по уголовным делам о преступлениях, совершённых с использованием информационных технологий.

В отношении преступлений, совершённых с использованием информационных технологий можно выделить следующее особенности:

Компьютерная информация характеризуется высокой скоростью трансформации, по своей природе электронные цифровые данные легко уничтожить и модифицировать. В связи с этим даже незначительное промедление с фиксацией обнаруженных цифровых следов может повлечь их утрату. Цифровые данные могут быть представлены практически бесконечным количеством копий, легко распространены в компьютерных сетях и быть доступны в любой точке мира, где имеется подключение к сети интернет.

Цифровизация привела к тому, что на смену традиционным «аналоговым» способам отображения объектов криминалистического исследования пришли их электронные аналоги, представленные в цифровом виде и фиксируемые в цифровом виде на специфических компьютерных носителях. Это касается аудио и видеозаписей, фотоизображений представления рукописных подписей, документов, дактилоскопических следов и отпечатков и др. в цифровом виде. Использование информационных технологий в сфере экономики (например, система «*1С-бухгалтерия*»), банковской сфере, в документообороте вызывает необходимость исследовать не традиционные документы бухгалтерской, банковский, финансово-экономической отчетности, а их трансформации, представленные в цифровом виде. – цифровые следы.

[42] Материалы из архива Лаборатории Касперского, 2015 – 2020 г.

Цифровые следы обладают только им присущими свойствами:

- существуют в виде компьютерной информации;
- характеризуются высокой скоростью трансформации;
- отличаются невозможностью восприятия непосредственно органами чувств, а только с помощью специальных устройств и программ;
- требуют новых, отличных от традиционных, способов, методов и процедур по обнаружению, фиксации и обеспечению сохранности;
- подтверждаются контрольными числами (хэш-суммами) либо иными данными, свидетельствующими об их целостности.

Перечисленные свойства цифровых следов обусловливают необходимость использования криминалистических технологий при их выявлении, сохранении и изъятии, а также судебно-экспертном исследовании.

Остановимся подробнее на пояснении значимости использования специальных программно-технических средств, привлечении специалиста, эксперта, а также получения вещественных доказательств с такими цифровыми следами.

По общему правилу, вопрос о применении технических средств целиком и полностью находится в компетенции лица, проводящего следственное действие, то есть следователя (дознавателя), при условии обязательного уведомления остальных участников следственного действия (ст. 164 УПК РФ). Исключение из данного правила составляют только положения ст. 179 УПК РФ, согласно положениям которой при проведении освидетельствования осуществление фотографирования, видеозаписи и киносъёмки допускается только с согласия освидетельствуемого лица.

Решение о применении технических средств может приниматься по соответствующему ходатайству участников следственных действий. В данном случае решение о применении технических средств относится к компетенции следователя (дознавателя), а в случае обжалования в порядке, предусмотренном ст. 124, 125 УПК РФ – решение о применении технического средства принимает суд, прокурор или начальник следственного органа. При этом, несмотря на то, что право ходатайствовать о применении технических средств закреплено только в общих правилах, регламентирующих порядок производства допроса (ст. 189 УПК РФ), и, исходя из буквального толкования норм закона, при осуществлении иных следственных действий подобного права участникам не предоставлено, полагаем, что в данном случае следует руководствоваться гл. 15 УПК РФ, предоставляющей право заявлять ходатайства, в том числе и о применении технических средств, в рамках проведения любого следственного действия.

Решение о применении технических средств может приниматься не по инициативе какого-либо лица, а в силу прямого указания закона. Уголовно-процессуальным законом предусмотрены обстоятельства, при которых применение технических средств является обязательным. При этом, представляется, что включение иных оснований обязательного применения технических средств является преждевременным. Следователь, дознаватель в каждом конкретном случае должны самостоятельно определять необходимость применения программно-технических средств, в том числе решать вопрос о привлечении для их применения специалиста.

Законом предусмотрено обязательное участие специалиста при изъятии и выемке электронных носителей информации (ст. 182 и 183 УПК РФ). По мнению автора, вопрос о привлечении специалиста при изъятии или выемке электронных носителей информации целесообразно оставить на усмотрение следователя, так как зачастую дей-

ствия по изъятию или выемке электронных носителей информации не имеют той степени сложности, которая требует наличия специальных знаний. Однако в рамках действующего законодательства отсутствие специалиста в данном случае может привести к признанию полученных доказательств недопустимыми.

Для законодательного разрешения проанализированных проблемных вопросов с учетом того, что современная законодательная техника предусматривает наличие как общих, так и специальных норм, регулирующих производство следственных действий, представляется необходимым ввести норму, предусматривающую общие положения применения электронных и технических средств при производстве следственных действий с учётом их особенностей и возможности использования полученных сведений в доказывании.

Прежде всего, следует выделять группу следственных действий, производство которых без применения технических (программно-технических) средств невозможно (следственные действия с обязательным техническим этапом). При этом данные следственные действия необходимо разграничивать со следственными действиями, при производстве которых в силу предписаний закона требуется обязательное применение технических средств, и с выделяемыми в юридической литературе технико-специальными следственными действиями.

В качестве особенностей следственных действий с обязательным техническим этапом необходимо отметить следующее:

1) применение технических средств вызвано объективной необходимостью, познавательная функция данных следственных действий может выполняться только посредством применения технических средств;

2) технический этап осуществляется за рамками уголовного процесса, однако предусмотрен обязательный осмотр следователем объектов, полученных в результате следственного действия;

3) сведения, полученные с помощью технических и электронных средств, фиксируются на материальном носителе информации, который предоставляется в установленном порядке;

4) материальный носитель информации, содержащий относимую к уголовному делу информацию, в полном объёме приобщается к материалам уголовного дела и хранится в опечатанном виде в условиях, исключающих возможность ознакомления с ним посторонних лиц и обеспечивающих его сохранность и техническую пригодность для повторного исследования, в том числе в судебном заседании.

Представляется, что наличие технического этапа в том или ином виде можно выявить в любом следственном действии, в котором по каким-либо причинам было использовано техническое средство, соответственно, должны быть выработаны общие нормы, регламентирующие порядок фиксации и хранения информации, полученной с помощью технических средств.

При проведении следственного действия в отсутствие понятых следователь обязан применить технические средства с целью фиксации его хода и результатов. Закон не предусматривает, какое конкретно техническое средство в этих случаях должно применяться. Представляется, что максимальную фиксацию, способную заменить понятых, могут обеспечить лишь те технические средства, посредством которых осуще-

ствляется видеозапись. При этом фотофиксация должна осуществляться дополнительно к видеозаписи хода следственного действия.

В случае изъятия мобильного телефона, иного технического устройства или электронного носителя информации, а также самой электронной информации, содержащих сведения о дате, времени, продолжительности соединений между абонентами и (или) абонентскими устройствами (пользовательским оборудованием), номерах абонентов, других данных, позволяющих идентифицировать абонентов, а также сведений о номерах и месте расположения приемопередающих базовых станций, при осуществлении процессуального действия, когда собственник электронного средства против его осмотра, требуется наличие разрешения суда. В случаях когда собственник не установлен или таковой отказывается от права на цифровую вещь, отрицает своё владение или даже пользование ею, что процессуально зафиксировано, то вещь объявляется временно бесхозной и осматривается на общих основаниях как объект предметного мира без решения суда.

Исключение из данного правила должны составлять ситуации, при которых основанием для производства следственных действий уже является решение суда (отсутствует необходимость получения дополнительного судебного решения) либо сведения о собственнике как и было сказано отсутствуют, а также в случае задержания подозреваемого в порядке ст. 91–92 УПК РФ.

Замечание. Закон не даёт общего определения такого вида уголовных доказательств, как показания. Вместе с тем, ст. 76-80 УПК РФ содержат в себе правовые дефиниции показаний подозреваемого, обвиняемого, потерпевшего, свидетеля, эксперта и специалиста. Если их обобщить, то можно выделить некоторые общие признаки, которые в разной степени свойственны различным видам показаний.

Показания имеют важное правовое значение в качестве самостоятельного вида уголовных доказательств. Учитывая состязательную природу российского уголовного процесса, показания могут получаться при производстве любых следственных и иных процессуальных действий, в рамках которых возможно представление вербальной информации о преступлении. Субъектами получения показаний могут выступать соответствующие государственные органы, должностные лица, а также адвокаты. Сущностью показаний в уголовном судопроизводстве являются любые сведения об обстоятельствах преступного события, полученные указанными субъектами доказывания посредством их восприятия в вербальной форме и процессуально закрепленные в соответствующем протоколе. Формой передачи субъектам доказывания фактических сведений о преступлении может быть свободный рассказ, ответы на вопросы, объяснения, а также письменная речь, мимические жесты и знаки.

Содержащиеся в показаниях сведения представляют собою определённым образом трансформированную сознанием человека информацию о воспринятых им обстоятельствах преступления.

Способом процессуальной фиксации показаний выступает их протоколирование в порядке, определённом уголовно-процессуальным законом.

Несмотря на различия в процессуальном статусе лиц, которые дают показания в установленном законом порядке, предмет таких показаний в принципе одинаков – это любые относящиеся к уголовному делу обстоятельства. Определённую специфику имеют лишь показания эксперта и специалиста, хотя в принципе они согласуются с общим предметом показаний в уголовном процессе.

Показания специалиста – сведения, сообщённые им на допросе об обстоятельствах, требующих специальных познаний, а также разъяснение своего мнения (ч. 4 ст. 80 УПК РФ).

Заключение специалиста – представленное в письменном виде суждение по вопросам, поставленным перед специалистом сторонами (п. 3 ст. 80 УПК РФ).

Заключение специалиста представляет собой письменные ответы на поставленные перед ним вопросы. Специалист привлекается сторонами или судом к участию в деле: для содействия в обнаружении, закреплении и изъятии предметов и документов в ходе любых следственных действий; применения технических средств в исследовании материалов уголовного дела; постановки вопросов эксперту; для разъяснения вопросов, входящих в его профессиональную компетенцию (ч. 1 ст. 58 УПК РФ). Соответственно, в своём заключении он может высказать суждения:

а) относительно ранее выполненных им действий в процессе обнаружения, закрепления и изъятия предметов и документов;

б) о вопросах, которые, с его точки зрения, следует поставить перед экспертом;

в) по другим специальным вопросам, разъяснения которых требуют стороны. Специалист, в отличие от эксперта, не вправе проводить каких-либо самостоятельных специальных исследований, и его заключение может содержать ответы только на такие вопросы, которые не требуют проведения подобных исследований. Заключение специалиста не может заменить собой заключения эксперта.

Заключение эксперта – представленные в письменном виде содержание исследования и выводы по вопросам, поставленным перед экспертом лицом, ведущим производство по уголовному делу, или сторонами (п.1 ст. 80 УПК РФ).

Заключение эксперта как доказательство обладает следующими признаками:

а) оно представляет собой результат экспертизы, которая назначается по поручению следователя, дознавателя или суда и проводится с соблюдением особого процессуального порядка;

б) исходит от лиц, обладающих специальными познаниями в интересующей производство по данному делу области;

в) является итогом проведения этими лицами самостоятельного исследования собранных по делу доказательств и иных материалов;

г) имеет форму доказательства особого вида.

Основная задача эксперта – дать ответы на вопросы, поставленные ему в постановлении (определении) о назначении экспертизы. Однако если при производстве судебной экспертизы эксперт установит обстоятельства, которые имеют значение для уголовного дела, по поводу которых ему не были поставлены вопросы, то он вправе указать на них в своём заключении (п. 4 ч. 3 ст. 57, ч. 2 ст. 204 УПК РФ).

Замечание. Вывод эксперта может быть:

1) категорическим – положительным (например, след протектора оставлен на асфальте шинами конкретного автомобиля) или отрицательным (след принадлежит другому автомобилю);

2) вероятным (некатегорическим);

3) о невозможности решить поставленный вопрос (сокращённо – НПВ от «не предоставляется возможным», например, установить, кем оставлены отпечатки пальцев на орудии преступления, не представилось возможным).

В соответствии с п. 4 ч. 3 ст. 57 УПК РФ эксперт не вправе выходить за пределы своей специальной компетенции, т. е. делать выводы по вопросам, которые не могут быть разрешены на основе его специальных познаний (например, компьютерно-технический эксперт не вправе делать вывод о контрафактном ПО или оборудовании, т. к. контрафактность – правовое, юридическое понятие, а специальные знания эксперта в соответствии с предметом компьютерной экспертизы распространяются на инженерно-техническую сферу).

Представляется обязательным отражать в заключении эксперта технические средства, использованные при проведении исследования в случаях, когда представленные ими эмпирические данные являются самостоятельными и влияют на конечные выводы по поставленным вопросам. Указанное позволит проверять достоверность сведений, полученных с помощью технических средств.

С заключением эксперта тесно связан такой вид доказательств, как показания эксперта. Они даются им только после получения его заключения и в связи с ним в целях разъяснения или уточнения данного заключения.

Если требуется дополнить заключение эксперта, т. е. провести дополнительные специальные исследования для более полного или глубокого ответа на поставленные ему вопросы, должна быть назначена дополнительная экспертиза. Разъяснения и уточнения заключения даются экспертом в форме показаний только тогда, когда это возможно без проведения самостоятельных исследований.

Заключения и показания эксперта и специалиста подлежат оценке наряду со всеми другими доказательствами, предусмотренными уголовно-процессуальным законом (ст. 88 УПК РФ). Они не имеют каких-либо преимуществ перед другими доказательствами, но обладают весьма существенной спецификой, поскольку представляют собой выводы и умозаключения, сделанные экспертом и специалистом на основе исследований и действий проведенных ими с использованием специальных познаний.

Заключение и показания эксперта и специалиста подлежат оценке с точки зрения относимости, допустимости и достоверности доказательств.

Оценивая материалы экспертизы (заключения эксперта) в процессуальном отношении, необходимо, прежде всего, проверить, соблюдены ли при назначении и проведении экспертизы права обвиняемого, предусмотренные законом, – знакомился ли обвиняемый с постановлением о назначении экспертизы, удовлетворены ли его обоснованные ходатайства, заявленные в связи с экспертизой, ознакомлен ли обвиняемый с экспертным заключением и протоколом допроса эксперта, если таковой имеется в деле, удовлетворены ли ходатайства обвиняемого о постановке дополнительных вопросов, назначения дополнительного или повторного исследования, проверялись ли заявления и объяснения обвиняемого по выводам эксперта.

Оценивая заключение и показания эксперта и специалиста необходимо проверить имеются ли в деле достаточные данные, свидетельствующие об их компетентности в решении поставленных перед ним вопросов (образование, стаж работы, рекомендации, характеристики).

Замечание. Очень важно уяснить является ли эксперт и специалист лицом беспристрастным, незаинтересованным в исходе уголовного дела, не участвует ли он в этом деле в ином процессуальном качестве, несовместимом со своим положением (свидетель, потерпевший, следователь, дознаватель, обвинитель, защитник и т. д.), не состоит ли в родственных связях с потерпевшим или обвиняемым, не находится ли в служебной или иной зависимости (например, в финансовой, имущественной: приобрёл или сбыл акции ИТ-компании, о деятельности которой выносит своё заключение).

Существенным элементом оценки является проверка, оформлено ли заключение эксперта и специалиста в соответствии с законом. Необходимо проверить: не вышел ли эксперт и специалист за пределы своей компетенции, т. е. не решал ли вопросов правового характера, не сформулированы ли выводы на основании материалов дела, не относящихся к предмету его исследования, вместо того, чтобы обосновать их результатами проведенных исследований, требующих применения специальных знаний.

Заключительным этапом оценки данных доказательств является определение роли установленных фактов в доказывании виновности или невиновности лица, привлеченного к уголовной ответственности, в решении вопроса о доказанности или недоказанности тех или иных обстоятельств, имеющих значение для дела.

По результатам оценки заключения эксперта и специалиста может быть проведен их допрос либо назначена дополнительная или повторная экспертиза. Допрос проводится для разъяснения или дополнения заключения, если это не требует дополнительного исследования (о сущности и надёжности примененной методики, о значении отдельных терминов и т. п.).

1.2.2. Использование косвенных доказательств, казус

Использование косвенных доказательств, казус и проблема объективного вменения в уголовных делах по преступлениям совершённым с использованием информационных технологий.

Косвенные доказательства устанавливают промежуточные факты объективной реальности, указывающие на предмет доказывания и в своей совокупности объективно устанавливающие его. Прямые доказательства главного факта (виновность, форма вины и мотивы) – это информация об обстоятельствах, подлежащих доказыванию, исходящая от субъектов, достоверность этой информации можно проверить при помощи прямых доказательств из других источников либо косвенными доказательствами. Однако в деле не всегда имеется достаточное количество прямых доказательств. Поэтому мы полагаем, что познание при помощи исключительно прямых доказательств не всегда может дать объективные знания об обстоятельствах преступления. Считаем, что объективное, всестороннее и полное познание в определённых случаях возможно лишь при учёте косвенных доказательств.

Идеальный вариант – это когда в деле есть и прямые, и косвенные доказательства, что очень важно для проверки правильности как показаний субъекта, воспринявшего событие преступления, так и умозаключений субъекта уголовно-процессуального познания, основанных на косвенных доказательствах и выведенных из них промежуточных фактах.

Поскольку косвенные доказательства играют существенную роль в проверке прямых доказательств, в установлении субъективной стороны преступления, полагаем, что они являются одним из самостоятельных ключевых элементов в достижении цели уголовно-процессуального доказывания – достоверного установления фактических обстоятельству головного дела (т. е. объективной истины об обстоятельствах, подлежащих доказыванию).

Косвенные доказательства непосредственно указывают на промежуточные факты, которые в силу своей объективной связи с предметом доказывания в своей совокупности устанавливают обстоятельства, подлежащие доказыванию.

Суммируя вышесказанное, предлагаем все улики (вещественные и цифровые) делить на косвенные доказательства главного факта и косвенные доказательства иных обстоятельств, подлежащих доказыванию (в соответствии со ст. 73 УПК РФ), определив главный факт как виновность определённого лица в совершении конкретного преступления, форму его вины и мотивы.

Достаточно известный во время репрессий (1934-40 гг.) советский учёный-юрист М. М. Гродзинский, обобщивший мировой исторический опыт использования косвенных доказательств в своей монографии, выступал против классификации улик.[43] Он утверждал, что классификация косвенных доказательств «не вытекает из самой сущности улик и поэтому является произвольной».

Он считал, что сущность косвенных доказательств выражается в их причинной связи с преступлением. Однако он допускал деление «всех фактов, являющихся уликами по делу, на те, которые могли обусловить совершение данного преступления, и те, которые могли явиться следствием совершения этого преступления обвиняемым»

Современный учёный А. А. Хмыров, внёсший большой вклад в теорию улик, в классификации косвенных доказательств исходил[44] из их отношения к обстоятельствам, подлежащим доказыванию, в соответствии с УПК РФ. Но наш взгляд, этот подход очень логичный и имеет большую практическую значимость. Данная классификация, помимо основных функций, помогает в построении системы доказательств по делу, что очень важно в доказывании при помощи косвенных доказательств.

По мнению А. А. Хмырова, классификация косвенных доказательств должна быть основана на базе подробного описания составляющих предмета доказывания и предметные косвенные доказательства подразделяются на три крупные группы обстоятельств, характеризующие: «1) событие преступления, 2) субъекта и субъективную сторону преступления и 3) иные обстоятельства преступления»

Сочетая эти подходы, можно все косвенные доказательства делить по их функциональному признаку на группу предметных и группу вспомогательных улик. Хоть эти группы и различны по своему объёму, но и та и другая включают в себя несколько особых видов улик. Каждая группа выполняет свою функциональную задачу.

Предметные доказательства устанавливают промежуточные факты, а уже через них устанавливаются связи указанных видов доказательств с доказываемым.

Тот факт, что предметные доказательства в рассматриваемой классификации подразделяются на группы согласно обстоятельствам, подлежащим доказыванию по уголовному делу, позволяет утверждать, что рассматриваемая классификация помогает следователю сформировать максимально логичную систему доказательств по уголовному делу.

Необходимо подчеркнуть, что косвенные доказательства главного факта (т. е. виновность лица в совершении преступления, форма его вины и мотивы) имеют особую значимость в доказывании. Однако предметные косвенные доказательства иных обсто-

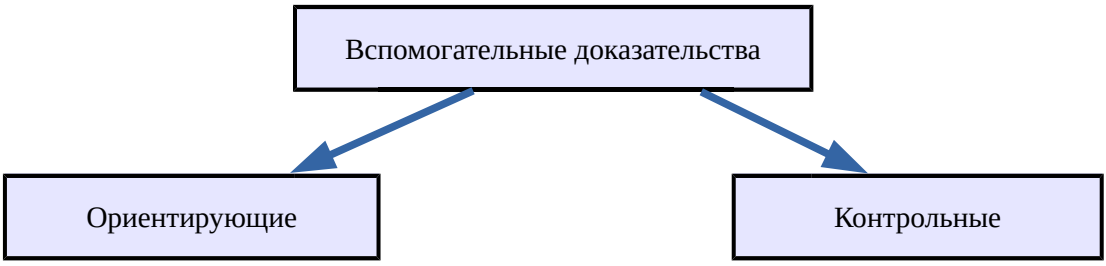
[43] Улики в советском уголовном процессе. Учёные труды. Вып. 7 / Гродзинский М.М. - М.: Юрид. изд-во НКЮ СССР, 1945. – 123 с.

[44] См. *Хмыров А. А.* Уголовно-процессуальное доказывание и усмотрение суда // Ученые записки. Т. 2. Вып. 3 (юбилейный). Краснодар: Северо-Кавказский фил. Российской акад. правосудия, 2006. С. 155-156.

ятельств, подлежащих доказыванию, безусловно, также важны для установления объективной истины по уголовному делу и для принятия судом законного и справедливого решения.

Если предметные доказательства имеют самостоятельное значение, то вспомогательные приобретают это значение только в совокупности с предметными. Это обусловлено тем, что вспомогательные косвенные доказательства не связаны ни с предметом доказывания, ни с промежуточными фактами непосредственно, но имеют причинно-следственную связь с предметными косвенными доказательствами. Они либо указывают на них, либо выполняют функцию по проверке их достоверности.

Таким образом, вспомогательные доказательства подразделяются на ориентирующие и контрольные[45].



Представляется, что выделение этих видов косвенных доказательств имеет важное теоретическое и практическое значение.

Однако, несмотря на все положительные моменты подхода А. А. Хмырова, не стоит забывать про остальные основания для классификации косвенных доказательств.

Итак, рассмотрев несколько подходов к классификации косвенных доказательств, полагаем, что в каждой из рассмотренных концепций есть положительные моменты. По нашему мнению, необходимо различать косвенные доказательства по их причинно-следственной взаимосвязи с событием преступления: причинные косвенные доказательства (т. е. указывающие на факты, способствующие совершению преступления) и косвенные доказательства последствий преступления (т. е. указывающие на факты следствия совершенного преступления).

Относительно главного факта (т. е. виновности лица в совершении преступления и формы его вины) необходимо различать улики – обвинительные косвенные доказательства и противоулики – оправдательные косвенные доказательства.

Классификация по функциональному признаку (т. е. деление улик на предметные и вспомогательные, которые, в свою очередь, делятся на ориентирующие и контрольные), безусловно, очень важна. Также косвенные доказательства (как и прямые) необходимо разделять на личные и вещественные, первоначальные и производные.

Необходимо отметить, что значение классификации доказательств не в том, чтобы выделить среди них «сильные» и «слабые», а в том, что она позволяет всесторонне исследовать особенности формирования, способы собирания и оптимальные методы использования каждой группы доказательств.

Необходимо различать косвенные доказательства по их причинно-следственной взаимосвязи с событием преступления: причинные косвенные доказательства (т. е. ука-

[45] См. *Хмыров А. А.* Косвенные доказательства в уголовных делах. – СПб.: Изд-во Р. Асланова «Юрид. центр Пресс», 2005. С. 135–137.

зывающие на факты, способствующие совершению преступления) и косвенные доказательства последствий преступления (т. е. указывающие на факты следствия совершенного преступления). Относительно главного факта (т. е. виновности лица в совершении преступления и формы его вины) необходимо различать улики – обвинительные косвенные доказательства и противоулики – оправдательные косвенные доказательства.

Что касается классификации косвенных доказательств по их отношению к отдельным элементам предмета доказывания, указанным в УПК РФ, то, на наш взгляд, существенным является разделение косвенных доказательств на косвенные доказательства главного факта и косвенные доказательства иных обстоятельств, подлежащих доказыванию.

Классификация по функциональному признаку (т. е. деление улик на предметные и вспомогательные, которые в свою очередь делятся на ориентирующие и контрольные), безусловно, очень важна. Также косвенные доказательства (как и прямые) необходимо разделять на личные и вещественные, первоначальные и производные.

Все имеющиеся в уголовном деле косвенные доказательства связаны с предметом доказывания через факты, не имеющие правового значения (факт присутствия на месте происшествия, факт обладания предметом и т. д.), однако способные всесторонне, полно и объективно установить обстоятельства, подлежащие доказыванию.

При доказывании с помощью косвенных доказательств надо, во-первых, установить, достоверны ли сведения, которые стали известны следователю, суду (говорит ли свидетель правду о наличии неприязненных отношений между обвиняемым - администратором сети и потерпевшим – владельцем фирмы, действительно ли на серверной стойке имелись отпечатки пальцев обвиняемого и т. д.): во-вторых, определить, связаны ли ставшие известными сведения с совершением преступления обвиняемым (например, обвиняемый – администратор при увольнении из фирмы мог быть в неприязненных отношениях с потерпевшим – владельцем фирмы, но это не повлекло за собой каких-либо преступных действий с его стороны: на месте преступления обнаружены отпечатки пальцев подозреваемого, но это не значит, что он был в момент преступления, так как ранее обслуживал сервера и стойки с носителями информации и т. п.). Поэтому при использовании косвенных доказательств важно установить не только какое-либо обстоятельство, но и объективную связь этого обстоятельства с устанавливаемыми по делу фактами. Формы этой связи могут быть различные (связь причинная, пространственно-временная, связь соответствия и др.). Установление этой связи определяет относимость доказательства.

Располагая косвенными доказательствами по делу, надо проверить их связь с доказываемым обстоятельством, чтобы исключить случайное стечение обстоятельств.

Из приведённой характеристики косвенных доказательств вытекают следующие правила их использования:

а) косвенные доказательства приводят к достоверным выводам по делу лишь в своей совокупности;

б) косвенные доказательства должны быть объективно связаны между собой и с доказываемым положением:

в) система (совокупность) косвенных доказательств должна приводить к такому обоснованному выводу, который исключает иное объяснение установленных обстоя-

тельств, исключает разумные сомнения в том, что обстоятельства дела были именно такими, как они установлены на основе этих доказательств.

Косвенные доказательства в своей совокупности могут служить основанием для вывода о фактах, входящих в предмет доказывания. Они могут быть использованы при проверке достоверности прямых доказательств[46], восполнять их пробелы, указывать путь получения новых доказательств.

Косвенные доказательства нельзя считать доказательствами «второго сорта». Эти доказательства чаще, чем прямые, встречаются при расследовании и рассмотрении уголовных дел и при правильном их использовании приводят к достоверным выводам.

Выявление объективных связей (причинно-следственной и др.) косвенных доказательств между собой и с предметом доказывания позволяет установить их относимость и достаточность для принятия законных, обоснованных и мотивированных решений, получить достоверное знание об обстоятельствах, подлежащих доказыванию, в соответствии с объективной реальностью.

Так как косвенные доказательства имеют многоступенчатую связь с предметом доказывания, их фальсификация и инсценировка казалось бы затруднены в силу сложности выявления их логической взаимосвязанности (хоть не исключены полностью). С одной стороны это обстоятельство обеспечивает достоверность и объективность полученной информации, с другой может послужить основой для объективного вменения.

Объективное вменение – это привлечение лица к уголовной ответственности без установления его вины. Объективное вменение может заключаться как в привлечении к уголовной ответственности за случайные последствия действий человека (например, в виде казуса), так и в привлечении к ответственности лиц, действия которых вообще не состоят в причинной связи с причинённым вредом, но деяния (слова, поступки – действия и бездействие) имеют какую-либо логическую взаимосвязь с событием преступления или имеются косвенные доказательства.

Например, владение помещением и (или) устройством беспроводной коммутации (WiFi-router), подключённым к провайдеру интернет, через беспроводное подключение к которому по радиоканалу путём взлома пароля неизвестные лица (как выяснилось после) совершили какое-либо деяние, подпадающее под квалификацию преступления по УК РФ.

Действующий Уголовный кодекс РФ в ч. 2 ст. 5 прямо запрещает объективное вменение. Однако, ряд учёных считают, что и в российском праве в отдельных случаях лицо может привлекаться к ответственности без учёта его субъективного отношения к отдельным признакам состава преступления. Например, некоторые авторы[47] [48] указывают, что характер объективного вменения имеют случаи, когда субъекту вменяется ответственность за казус или за отдалённые во времени от преступного деяния последствия: так, в судебной практике как наступление иных тяжких последствий при нарушении правил эксплуатации ЭВМ и сети ЭВМ, не обеспечении безопасности объектов критической информационной инфраструктуры, повлекшие в будущем неправомерное уничтожение, модификацию или копирование информации.

[46] Часто приводимый пример: показания свидетеля о том, что потерпевший находился в ссоре с обвиняемым, могут использоваться при оценке достоверности показаний потерпевшего.

[47] Епифанова Елена Владимировна Объективное вменение как реальность в современном уголовном праве // Вестник Самарской гуманитарной академии. Серия: Право. 2007. № 2. С.65-68

[48] Басенко О.С. Соотношение субъективного и объективного вменения. // Скиф. Вопросы студенческой науки, № 2 (18), 2018, С. 103-106.

– Папа, папа! ... (я сделала как ты сказал)... А что означает "Format C: complete"?

Казус (случай) или невиновное причинение вреда, урегулирован в ст. 28 УК РФ: деяние признаётся совершённым невиновно, если лицо, его совершившее, не осознавало и по обстоятельствам дела не могло осознавать общественной опасности своих действий (бездействия), либо не предвидело возможности наступления общественно опасных последствий[49] и по обстоятельствам дела не должно было или не могло их предвидеть (ч. 1 ст. 28 УК РФ).

При этом по замыслу законодателя (ст. 5 и ст. 28 УК РФ, ст. 1064 и ст. 1078 ГК РФ) в отечественном уголовном и гражданском праве, лицо не несёт ответственности за невиновное причинение вреда, каким бы тяжким он ни был. Таким образом, казус в уголовном праве граничит с преступной небрежностью. Обе формы психического состояния имеют сходные интеллектуальные элементы. Различие заключается в следующем: при небрежности лицо «могло и должно было», а при казусе «не должно было или не могло».[50]

В соответствии с ч. 2 ст. 28 УК РФ деяние признаётся также совершённым невиновно, если лицо, его совершившее, хотя и предвидело возможность наступления общественно опасных последствий своих действий (бездействия), но не могло предотвратить эти последствия в силу несоответствия своих психофизиологических качеств требованиям экстремальных условий или нервно-психическим перегрузкам.

Данная проблематика весьма актуальна для доказывания по уголовным делам о преступлениях, совершённых с использованием информационных технологий, в связи с тем, что активной стороной - инициатором действий, процессов и процедур в вычислительной, компьютерной микропроцессорной технике (в том числе в эмулируемой, облачной (*cloud*), виртуальной (*virtual*) компьютерной инфраструктуре) является также компьютерный процесс (*process*), т. е. активный элемент авторизованной программы операционной системы, имеющий возможность запускать (*initializate*) другие программы (процессы, потоки – *program, process, thread*) и как-либо реагировать на события (*events*) вне зависимости от аппаратных событий-прерываний (*interruption*). Субъект – человек лишь управляет средствами ввода информации цифрового устройства – сенсорным экраном, голосом, клавиатурой и манипулятором «мышь», работа которых фиксируется аппаратными прерываниями и программными событиями в операционной системе и может быть как проигнорирована, так и смоделирована (имитирована) в системе.[51]

[49] Например, скачивание и применение «безобидной» программы из магазина приложений Google Play. URL: https://www.cnews.ru/news/top/2022-11-30_100_tyschelovek_skachali_v_google

[50] Например, инженер группы информационных технологий в РОВД, осуществивший по команде (приказу в виде рапорта) форматирование накопителей (или обновление/переустановку системы) служебного ЭВМ следователя, находившегося в отпуске, что повлекло утрату данных, содержащих рабочие материалы и файлы с «цифровыми доказательствами» по какому-то уголовному делу, о чём инженер не мог и не должен знать, а должен выполнить прямую команду начальника РОВД, а следователь должен хранить цифровые доказательства на носителе информации, подшитым к уголовному делу с протоколом, налицо – казус. В данном выдуманном примере предполагается, что других документов в виде приказов, инструкций, положений, разъяснений и т. д., регламентирующих работу указанных лиц и вменяющих им в вину действие или бездействие по отношению к рассматриваемой ситуации, нет.

[51] См. *Минаков С. С.* Особенности доказывания по уголовным делам о преступлениях, совершённых с использованием IT-технологий: дис… магистра юриспруденции 40.04.01 / Минаков С.С. — Москва, 2022. — 85 с.

Особенно характерно это можно проиллюстрировать на примерах заражения (удалённого взлома, захвата управления) автономными компьютерными устройствами, например, бытовыми устройствами беспроводной коммутации (*WiFi-router*, далее – wifi-маршрутизатор), подключённых к провайдеру сети интернет и формирования из таких «зомбированных» устройств – т. н. Bot-сетей, которые можно использовать как для дальнейшего несанкционированного проникновения (вторжения, *intrude*) в ЭВМ и сети ЭВМ (в т. ч. виртуальные, эмулируемые), так и для организации массовых сетевых атак по каналам связи на отдельные ЭВМ и их ЭВМ, без участия их владельцев (операторов).

В таких случаях косвенные доказательства без сформулированного предмета доказывания или не образующие системы косвенных или прямых доказательств могут привести к ситуации объективного вменения в отношении владельца заряжённого компьютера или поражённого WiFi-маршрутизатора по статьям 272 и 274 УК РФ.

Поэтому система косвенных доказательств по уголовному делу должна формироваться из следующих структурных элементов: базовых – отдельно взятых косвенных доказательств (предметных и вспомогательных); синтезированных – совокупности косвенных доказательств, которые непосредственно устанавливают промежуточные факты; итоговых – промежуточных фактов, опосредованно устанавливающих те или иные обстоятельства, подлежащие доказыванию.

Для достоверного установления фактических обстоятельств уголовного дела на основе исключительно косвенных доказательств их совокупность должна обладать такими свойствами, как согласованность (внутренняя взаимосвязанность), однозначность (отсутствие возможности двоякой трактовки совокупности доказательств) и полнота (установление косвенными доказательствами всех элементов предмета доказывания).

При осуществлении поиска вещественных доказательств и собирании важной информации по делу, включая проверку её достоверности, на первый план выходит установление связей между имеющимися сведениями. Когда встает вопрос о принятии того или иного решения по уголовному делу, на первый план выходит связь каждого установленного при помощи косвенных доказательств промежуточного факта с обстоятельством, подлежащим доказыванию.

Система косвенных доказательств, устанавливающая все элементы предмета доказывания, может быть основой принятия процессуального решения и в отсутствие прямых доказательств. Однако эта система должна обладать такими свойствами как однозначность, полнота, согласованность и надежность. Это может быть обеспечено установлением взаимосвязанности всех имеющихся по уголовному делу косвенных доказательств.

Квалифицированное использование косвенных доказательств раскрывает альтернативные (дополнительные) возможности для установления обстоятельств, подлежащих доказыванию через сведения, прямо не указывающие на обстоятельства, подлежащие доказыванию, которые в своей совокупности позволяют их достоверно установить.

1.2.3. Особенности использования цифровых доказательств

Особенности использования цифровых доказательств на предварительном расследовании и в суде.

Казалось бы настоящая редакция УПК РФ имеет необходимые уголовно-процессуальные нормы для применения различных технических средств и способов обнаружения, фиксации и изъятия следов преступления и вещественных доказательств (ч. 6 ст. 164 «*Общие правила производства следственных действий*» УПК РФ), а также акцентирует следственные действия (осмотр, обыск или выемка) на изъятие или копирование электронных носителей информации (ст. 164.1. «*Особенности изъятия электронных носителей информации и копирования с них информации при производстве следственных действий*» УПК РФ).

В частности, в спорных случаях, когда копирование информации, в силу присущего этому техническому действию режима принудительного изменения даты и времени последней операции над файлами, сопряжённого с отсутствием возможности для его отмены, может воспрепятствовать установлению истины по делу, проводится не копирование информации, а выемка или изъятие самих аппаратных средств компьютерной техники. В последующем они представляются для экспертных исследований[52], заключения которых и признаются доказательствами. Тем самым в уголовном судопроизводстве искусственно происходит сужение круга доказательств по делам о преступлениях в сфере компьютерной информации [81].

В отношении связанных с этим уголовно-процессуальных вопросов и проблем цифровой (компьютерной) криминалистики, связанных с правомерностью и законностью[53], а также обеспечением фактического доступа к данным на машинных носителях информации, обладателем или владельцем (лицом, организацией, государством), которой предъявлены требования по её защите, в том числе криптовалют [62], в ходе следственных действий развёрнута научно-практическая дискуссия[54] [55] [56], часть вопросов в

[52] В ходе проведения которых гарантируется использование методик обращения с накопителями гарантирующих сохранение неизменности первоначальной информации. Например, это может быть перевод твердотельных жёстких дисков (SSD) в режим «только чтения», при котором фоновая служебная оптимизация внутри диска, при которой данные одних секторов памяти перезаписываются в другие также блокируется и т.п.

[53]Неправомерный доступ к охраняемой законом компьютерной информации (личная, коммерческая, профессиональная, служебная, военная тайны и пр.), если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, как и незаконное собирание сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия, составляет самостоятельную диспозицию статей 272 и 137 УК РФ, соответственно.

[54] См. *Машинская Н.В.* Проблемы законодательного регулирования изъятия электронных носителей информации при производстве следственных действий // Общество и право. 2022. № 1 (79). URL: https://cyberleninka.ru/article/n/problemy-zakonodatelnogo-regulirovaniya-izyatiya-elektronnyh-nositeley-informatsii-i-kopirovaniya-s-nih-informatsii-pri (дата обращения: 12.11.2022).

[55] См. *Саркисян А. А.* Некоторые проблемы исследования цифровых следов / А. А. Саркисян // Цифровой след как объект судебной экспертизы : материалы Международной научно-практической конференции, Москва, 17 января 2020 года. – Москва: РГ-Пресс, 2020. – С. 188-191. – EDN KPEFKD.

[56] См. *Минаков С. С., Михайленко Н. В.* Актуальные проблемы обеспечения информационной безопасности личности и общества при использовании технологий в условиях цифровой трансформации. // Криминологический журнал (Московский университет МВД РФ им. В.Я. Кикотя), № 5, 2022 г.

российской практике организационно-технически стандартизированы[57] [58] [59] [60], но не опираются полностью на нормы УПК РФ.

Вместе с тем правоприменительная практика[61] выявила новые актуальные уголовно-процессуальные проблемы следственных действий обусловленные широким внедрением облачных технологий обработки информации, применением технологий гиперконвергенции, виртуализации вычислений и инфраструктуры. К сожалению, изъятие носителей информации с целью их экспертного исследования не является «палочкой-выручалочкой на все случаи жизни».

В правоохранительной сфере осознан[62] факт необходимости новаций в уголовно-процессуальной сфере, в способах и инструментальных методах осуществления поиска, осмотра, выемки или изъятия документов и материалов в электронном виде с необходимым обеспечением их целостности при невозможности выемки или изъятия самого накопителя информации или остановки (выключения) автоматизированных систем.

Анекдотичный случай. К слову сказать, характерной немой сценой закончилась «экскурсия» для курсантов, молодых следователей и оперативных сотрудников по нескольким этажам с сотнями стоек одинакового оборудования в центре обработки данных (ЦОД) ПАО «Ростелеком»[63] после вопроса экскурсантам: «Если ваша компьютерная система распределённа в «облачной» инфраструктуре ЦОД, что и как вы здесь будете осматривать и изымать в соответствии с УПК? И где будете хранить изъятое?» (Для лучшего представления как всё выглядело на рис. 1 представлена фотография другой, относительно меньшей по размерам системы, – только одной комнаты (части) машинного зала центра обработки данных системы «Платон». На фото видно лишь 3 ряда по 9 стоек, против сотен введённых в 2022 году.)

[57]ГОСТ 6.10.4-84. Межгосударственный стандарт. Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники. Основные положения. Unified systems of documentation. Confirment of legal force to documents on software and machinogramme created by computers. General principles. Дата введения 01.07.1987. Группа Т54. ОКСТУ 0006.

[58]ГОСТ Р ИСО/МЭК 27037-2014. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме. ISO/IEC 27037:2012 Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence (IDT). Дата введения 2015-11-01. ОКС 35.040.

[59]ГОСТ Р 57429–2017. Национальный стандарт Российской Федерации. «Судебная компьютерно-техническая экспертиза. Термины и определения».

[60]СТО БР ИББС-1.3-2016. Стандарт Банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Сбор и анализ технических данных при реагировании на инциденты информационной безопасности при осуществлении переводов денежных средств. Дата введения: 2017-01-01.

[61] См. *Демичева Т. С.* Актуальные проблемы уголовно-процессуальной формы использования информационных технологий при рассмотрении сообщения о преступлении. // Государственная служба и кадры, № 2, 2022, С. 182-184. doi: 10.24412/2312-0444-2022-2-182-184.

[62] Постановление Координационного совещания руководителей правоохранительных органов Российской Федерации от 17 июля 2020 г. № 1 «О состоянии работы правоохранительных и контролирующих органов по предупреждению, выявлению, пресечению и расследованию преступлений, связанных с посягательствами на безопасность в сфере использования информационно-телекоммуникационных технологий, включая критическую информационную инфраструктуру Российской Федерации», вынесенного Председателем координационного совещания Генеральным прокурором Российской Федерации И.В.Красновым.

[63] См. новость от 17.11.2021 «Ростелеком-ЦОД» построит в Москве дата-центр на 6 710 стоек [Электронный ресурс] https://www.company.rt.ru/projects/digital_economy_rf/data-centers/d461176/, (дата обращения 01.12.2022).

Рисунок 1. Фотография машинного зала в ЦОД системы «Платон»

Так, изъятие в принципе невозможно в случаях, когда преступления совершаются в глобальных компьютерных сетях, а «виртуальные следы» находятся в сегментах таких сетей за границей страны.

1.3. Проблемы

В теории уголовного процесса и на практике ни у кого не вызывает возражений утверждение о том, что доказывание, является центральным компонентом всей уголовно-процессуальной деятельности, «сердцевиной» уголовного процесса[64].

Однако, проблемы доказательств и доказывания, несмотря на множество научных исследований всё также остаются на пике неутихающих, разносторонних дискуссий, как среди учёных, так и практических работников. Отдельные вопросы, касающиеся процесса доказывания и самих доказательств, в свете постоянно меняющейся правовой действительности и реформирования органов предварительного расследования и суда, нуждаются в более глубокой, существенной и детальной разработке.

Особое место в теории доказательств занимают проблемы, связанные с понятием самого доказывания, его гносеологической и методологической сущности, как разновидности человеческого познания. Среди учёных, занимающихся вопросами доказательств и доказывания можно встретить различные, порой, взаимоисключающие высказывания о понятии уголовно-процессуальных доказательств и их признаках, дис-

[64] См. *Шейфер С. А.* Собирание доказательств по уголовному делу: проблемы законодательства, теории и практики. М. : Норма, 2015. С. 12.

куссионными остаются вопросы классификации доказательств и их использования в процессе доказывания по уголовным делам, что показывает, что в науке нет единства мнений о цели, предмете и пределах доказывания в уголовном судопроизводстве.

Доказывание пронизывает все стадии уголовного процесса, однако в зависимости от задач конкретной стадии, характера процессуальных действий и отношений, складывающихся между её участниками, процесс доказывания приобретает свои специфические черты [76, 86].

Отметим, что традиционные методы познания преступной деятельности на основе метода материалистической диалектики постепенно вытесняются разработками в области исследования специфической формы объективной действительности, именуемой «виртуальным пространством», статус которого юридической наукой в криминалистической и уголовно-процессуальной сфере до сих пор однозначно не определён, несмотря на сложившуюся за почти три последних десятилетия практику. Смеем предположить, что одной из возможных причиной этому, является отсутствие системного подхода к изучению особенностей виртуального пространства и процессов, которые в нём проистекают.

Так, хотелось бы отметить, что на сегодня часто иные преступления, в которых вычислительные средства, сети и системы, программное обеспечение, не являются объектом посягательств или способом совершения преступления, в т.ч. посягающие на традиционно охраняемые уголовным законом общественные отношения, для которых использование информационно-коммуникационных технологий хотя и является возможным, однако выступает крайне редким, не типичным, фиксируемым от случая к случаю способом, и на современном историческом этапе не оказывает значимого влияния на степень общественной опасности деяния (ст. 105, 205, 281 УК РФ и др.) не рассматриваются. Их следует относить к числу так называемой смежной проблематики, не представляющей актуального значения для противодействия именно компьютеризированной преступности как уже сложившейся на текущий момент социально негативной практики.

Многие российские учёные и практики В.Б. Вехов, О.В Волынская, Б.Я. Гаврилов, А.В. Земскова, О.В. Мичурина, О.В. Химичева, Е.Р. Россинская, Е.А. Русскевич, А.И. Семикаленова, Чекунов И.Г. отмечают, что классический аппарат уголовно-правовой охраны часто «не срабатывает» (не дорабатывает) в отношении «новой» (изменившейся) преступности по причине цифровой трансформации сфер, в которых такая преступность развивалась (товарно-денежной, кредитно-финансовой, межличностного общения и т. п.).

Е.А. Русскевич предлагает [73] [75] выделить шесть сущностных признаков преступлений, совершаемых с использованием информационно-коммуникационных технологий:

1. Виртуальность – информационно-коммуникационная среда является краеугольным признаком исследуемой преступности. Обеспечивая анонимность и физическую дистанцию от непосредственного потерпевшего, виртуальное пространство выступает значимым преимуществом и одновременно мощной детерминантой совершения преступления. При этом в отличие от реального мира виртуальность снимает многие психологические барьеры на пути к осуществлению преступной деятельности, прежде всего, в связи с поддержанием чувства (и не всегда ложного) личной безопасности у преступника;

2. Экстерриториальность – глобальная доступность и распространённость информационно-коммуникационных технологий означает, что преступность в информационном пространстве естественным образом имеет экстерриториальное измерение;

3. Гипертаргетированность – преступлениям, совершаемым с использованием современных информационно-коммуникационных технологий, как никаким другим, свойственна нацеленность сразу на многих потерпевших и способность вызывать целые цепи многоуровневых общественно опасных последствий. При крупных вирусных атаках на финансовый сектор или банковские счета отдельных хозяйствующих субъектов или физических лиц количество потерпевших может измеряться сотнями и даже тысячами. В данном аспекте хотелось бы опереться и предметно развить теорему Станислава Лема[65], согласно которой «по мере технологического прогресса неуклонно возрастает разрушительная мощь малых групп»;

4. Мультипликативность – способность к самовоспроизводству. Наиболее ярко данный признак проявляется на примере распространения вредоносных компьютерных программ. Вирусная атака на конкретную организацию благодаря особенностям архитектуры глобальной информационной сети интернет может обернуться колоссальными последствиями не только для отдельно взятой страны, но даже целой группы государств. Компьютерный вирус или сетевой «червь», распространяясь по открытым каналам связи уже без участия человека, будет поражать все доступные ему цели, включая объекты социального обеспечения (больницы, школы и т.д.) и государственного управления. Другой стороной свойства мультипликативности является то, что появление какой-либо формы виртуальной преступной деятельности, как правило, вызывает новые посягательства на отношения информационной безопасности. Например, появление новой уязвимости в операционной системе широкого распространения, может порождать всплеск целевых атак на защищённые информационные ресурсы как отдельных граждан, так и государств;

5. Сверхизменчивость – появление новой информационной технологии на массовом рынке товаров или услуг практически незамедлительно оборачивается очередной «перезагрузкой» преступности. Злоумышленники оценивают новации как поле очередных возможностей для совершения атак на граждан или организации. Учитывая, что технологии совершенствуются стремительно и непрерывно, это соответственно обусловливает такой же динамичный и перманентный процесс цифрового обновления преступности, когда какие-то относительно устоявшиеся формы виртуальной преступной деятельности уходят в небытие и замещаются другими;

6. Системная латентность (гиперлатентность) – компьютерная преступность практически не поддаётся внятному количественному измерению. Объяснение этому имеет комплексный характер: противоречия действующего нормативного регулирования, несовершенство правоприменительной деятельности и механизмов статистического учёта, массовое несообщение о причинении вреда самими потерпевшими, а также постоянно видоизменяющаяся природа преступлений, совершаемых с использованием информационно-коммуникационных технологий.

[65] Речь идёт о выдержке из философского труда «Сумма технологии», в котором Станислав Лем предвосхитил создание виртуальной реальности, искусственного интеллекта, а также развил идеи автоэволюции человека, сотворения искусственных миров и многие другие. Станислав Герман Лем (1921–2006) – известный польский философ, футуролог и писатель (фантаст, эссеист, сатирик, критик). Прим. авт.

Изложенное свидетельствует, что информационно-коммуникационные технологии и явно, и опосредованно оказывают значительное воздействие на механизм уголовно-правовой охраны, что создаёт риск дизрупции уголовного права (бессистемного изменения уголовного закона, угрожающего разрушением субстанциональных признаков отрасли уголовного права).

Представляется, что данное учебное пособие углубит представления о доказательствах и доказывании в уголовном процессе по преступлениям, совершённым с использованием информационных технологий у правоохранительных органов, с учётом активизации криминальной деятельности и деятельности по раскрытию, расследованию и предупреждению преступлений в пределах специфической формы объективной действительности, именуемой «виртуальным пространством».

1.4. Вопросы для самоконтроля

1. Что и зачем регулирует уголовное право?
2. В чём состоит отличие понятий «компьютерные преступления» и «компьютеризированные преступления»?
3. Поясните в чём заключается процесс доказывания в уголовном процессе.
4. Что есть доказывание (процесс доказывания)?
5. Что значит формально минималистический подход в доказывании?
6. Что означает понятие «пределы доказывания»?
7. Какая цель у доказывания?
8. Что подлежит доказыванию согласно ст. 73 УПК РФ?
9. Каким образом производятся собирание и проверка доказательств?
10. В каком случае информация становится доказательством?
11. Каким условиям должны отвечать доказательства?
12. Что понимается под относимостью доказательств?
13. Что понимается под достоверностью доказательств?
14. Что понимается под достаточностью доказательств?
15. Каковы условия допустимости доказательств?
16. Что есть недопустимость доказательств?
17. Может ли слух лежать в основе доказательства?
18. Какие показания не могут быть положены в основу утверждений об обстоятельствах, подлежащих доказыванию?
19. Какие нарушения дают право участникам процесса требовать признания доказательств недопустимыми?
20. Каким номером статьи УПК РФ регламентируется процедура признания доказательства недопустимым?
21. Что относится к источникам доказательств согласно ч. 2 ст. 74 УПК РФ?
22. Поясните понятие «классификация доказательств». Какие классификации вы знаете?
23. Поясните различие: первоначальные и производные доказательства.
24. Что лежит в основе деления доказательств на первоначальные и производные?
25. Приведите примеры производных доказательств.
26. Приведите видовую классификацию доказательств в соответствии с УПК РФ.
27. Какие категории граждан не подлежат допросу в качестве свидетелей в соответствии с ч. 3 ст. 56 УПК РФ?
28. Могут ли быть допрошены следователи или дознаватели, в производстве которых находится уголовное дело, в качестве свидетелей?

29. В чём отличие специалиста от эксперта (согласно ст.80 УПК РФ)?
30. Каковая основная задача производства экспертизы?
31. Должны ли в соответствии с ч.1 ст.82 УПК РФ вещественные доказательства храниться при уголовном деле и по ходу движения уголовного дела передаваться вместе с ним из одного органа в другой?
32. В каком случае МНИ приложенные к протоколам имеют доказательную силу?
33. Как Вы понимаете термин «цифровые доказательства»?
34. Что под электронными доказательствами понимает В.Б.Вехов?
35. Какие применяются специализированные программно-технические комплексы и программные средства для собирания цифровых следов?
36. Какими документами регламентируется работа с цифровыми следами преступлений?
37. Какие четыре этапа (раскройте их) обращения со свидетельствами, представленными в цифровой форме, предусмотрены в ГОСТ Р ИСО/МЭК 27037-2014 «*Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме*»?
38. Назовите криминалистический принцип при работе с цифровыми следами, на
39. необходимость соблюдения которого прямо указано в стандарте ISO/IEC 27037?
40. Какие правила важно соблюдать при производстве невербальных следственных действий, в ходе
41. которых осуществляется работа с цифровыми следами?
42. Какие особенности можно выделить в отношении преступлений, совершённых с использованием информационных технологий?
43. Какие свойства присущи только цифровым следам?
44. Какие свойства цифровых следов обусловливают необходимость использования криминалистических технологий при их выявлении, сохранении и изъятии, а также судебно-экспертном исследовании?
45. Назовите обстоятельства предусмотренные уголовно-процессуальным законом при которых применение технических средств является обязательным.
46. В соответствии со ст. 182 и 183 УПК РФ предусмотрено ли обязательное участие специалиста при изъятии и выемке электронных носителей информации?
47. Дайте определение понятию «заключение эксперта».
48. Какими признаками (как доказательство) обладает заключение эксперта?
49. Дайте определение понятию «косвенные доказательства».
50. Какие есть особенности использования косвенных доказательств?
51. На какие виды разделяются косвенные доказательства по А.А.Хмырову?
52. Исходя из положения: располагая косвенными доказательствами по делу, надо проверить их связь с доказываемым обстоятельством, чтобы исключить случайное стечение обстоятельств. Какие есть правила использования косвенных доказательств?
53. В чём отличие понятий «казус» и «преступная небрежность»?
54. Для достоверного установления фактических обстоятельств уголовного дела на
55. основе исключительно косвенных доказательств какими свойствами должна обладать их совокупность?
56. Перечислите новые актуальные уголовно-процессуальные проблемы следственных действий обусловленные широким внедрением облачных технологий обработки информации, применением технологий гиперконвергенции, виртуализации вычислений и инфраструктуры.
57. Приведите примеры когда изъятие машинных носителей информации или средств вычислительной техники в принципе невозможны.
58. Перечислите сущностные признаки преступлений, совершаемых с использованием информационно-коммуникационных технологий?

Следы – это ... (*Следы в русском языке.)*

...отпечаток (характерный отпечаток), оттиск чего-нибудь (ноги человека или животного, колёс или полозьев саней и т.п.) на земле или иной поверхности, а также полоса, оставшаяся после движения чего-нибудь. Фото полосы от самолёта.

Остаток или признак чего-нибудь. То, что осталось в результате чего-нибудь, последствие.

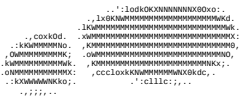
Идти по свежим следам. Идти по горячим следам. Собака взяла след. Напасть на чей-нибудь след. Следы ведут к...

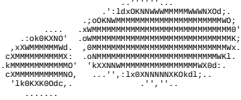
Идти след в след. Идти по чьим-нибудь следам. И след простыл...

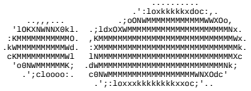
Следовать учению... Чтение данного учебного пособия прошло без следа.

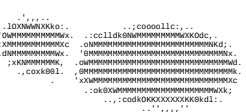
Следы в криминалистике, любые материальные последствия, возникающие в связи с совершённым преступлением (например, изменения в окружающей обстановке, материально-фиксированные отображения внешнего строения предметов, людей, подделки в документе). Изучение следов позволяет судить об обстановке и характере преступления, его орудиях, о самом преступнике.

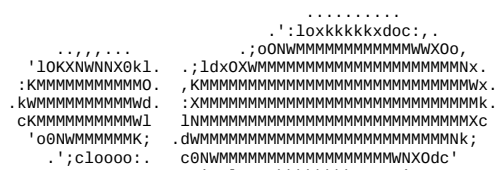
Трасология (*от франц. trace* ≈ следи, *греч. logos* ≈ *слово*, *учение*, буквально ≈ учение о следах), отрасль криминалистики, изучающая следы и разрабатывающая специальные приёмы, методы и научно-технические средства их обнаружения, фиксации, изъятия и исследования в целях идентификации человека или объекта. Различают следы: человека, орудий преступления, инструментов и производственных механизмов, транспортных средств, электронных устройств.











```
0003240 4d 4d 4d 4d 4d 4d 4d 4d 4d 4d 4d 4d 4d 4d 4d 4d
0003260 4d 4d 4d 4d 57 78 2e 20 20 20 20 20 20 20 20 20
0003280 20 20 20 20 20 20 20 20 20 20 2e 6c 4b 57 4d 4d
0003300 4d 4d 4d 4d 4d 4d 4f 2e 20 20 2e 6b 57 4d 4d 4d
0003320 4d 4d 4d 4d 4d 4d 4d 4d 4d 4d 4d 4d 4d 4d 4d 4d
0003340 4d 4d 4d 4d 4d 4d 4d 4d 4d 58 6f 2e 20 20 0a 20 20
0003360 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
```

Глава 2. Цифровые следы

В данной главе рассматриваются особенности идентификации, сбора, фиксации и представления доказательств в электронной форме.[66]

2.1. Принципиальные отличия и особенности

Принципиальные отличия и особенности тактик и способов сбора и фиксации доказательств, связанных с использованием информационных технологий.

Как отмечал Р. С. Белкин, «проблематика фиксации доказательственной информации – неотъемлемая часть комплекса проблем, связанного с изучением и использованием закономерностей собирания доказательств» [38].

Более того цифровизация всех значимых сфер деятельности человека, породила целый ряд теоретических, правовых и организационных проблем, связанных с методологией и методиками экспертного исследования и компетенцией судебных экспертов [115, 161, 169, 172, 179, 187, 191 и др.], т. к. в настоящее время практически любая судебная экспертиза, например, дактилоскопическая, фоноскопическая, видеотехническая, портретная, судебно-бухгалтерская, финансово-экономическая, судебно-техническая экспертиза документов и другие, в качестве своих объектов может иметь «цифровые следы».

Цифровые следы могут быть представлены для дальнейшего исследования с целью получения розыскной и доказательственной информации в различных видах и формах:

- находится на отдельных машинных носителях информации, например, на жёстком магнитном диске, твердотельном накопителе, USB-флеш-накопителе, оптическом компакт диске и др.;
- непосредственно содержаться в компьютерных системах и сетях (в том числе и на выключенном (обесточенном) оборудовании), мобильных коммуникаторах, планшетах, на серверах, в облачных хранилищах;
- в качестве цифровых следов можно рассматривать электронные документы;
- образы цифровых следов, отображаемые в цифровом виде с помощью различных программных продуктов, например изображения подписей, дактилоскопических отпечатков в графических или текстовых процессорах; снимки экранов с перепиской в социальных сетях и пр.;
- образы цифровых следов, отображаемые на бумажных носителях, например, распечатки снимков экрана, распечатки электронных документов и др.

Также, в отношении цифровых следов следует отметить следующее:

[66] В данной главе под электронной формой понимается такая форма при которых задействована вычислительные мощности (техника) в которой протекает электрический ток, т. е. если не оговорено особо, из рассмотрения исключаются пассивные накопители: на оптических дисках, бумажный QR-код, перфокарта и т.д.

Во-первых, выполняется критерий о специфике объектов исследования и, в то же время, их распространённости, частоте встречаемости в уголовном, административном и гражданском судопроизводстве. Действительно цифровизация привела к тому, весьма распространёнными объектами криминалистического исследования стали цифровые следы – не только электронные аналоги, аудио и видеозаписей, фотоизображений, подписей, документов, дактилоскопических следов и отпечатков и др. представленных в цифровом виде и фиксируемых на специфических компьютерных носителях, но и следы действий с использованием компьютерных систем и их сетей в виде структур компьютерной информации в оперативной памяти компьютера, на носителях информации различных типов, на линиях связи и в коммутаторах.

Во-вторых, налицо решение специфических криминалистических задач – диагностические и идентификационные исследования цифровых следов, в том числе воздействия вредоносных программ и изучение контрафактных информационно-компьютерных продуктов.

В-третьих, методологическая и методическая разработанность данного направления, несмотря на его новизну идёт уже давно в основном в русле судебно-экспертных исследований.[67]

К особенностям цифровых следов можно отнести двойственную природу информационно-компьютерных объектов[68], которая включает информационно-цифровую и материальную составляющие. Следовательно, наряду с цифровыми следами объектами криминалистического исследования компьютерных средств и систем будут являться носители цифровых следов, от правильного обнаружения, фиксации и изъятия которых, их судебно-экспертного исследования зависит целостность и полнота криминалистически значимой информации, имеющей доказательственное и ориентирующее значение.

2.1.1. Источники получения цифровых следов

На сегодня можно выделить следующие категории объектов, которые могут являться носителями криминалистически значимой компьютерной информации:

- устройства для хранения информации;
- устройства для ввода/вывода информации;
- устройства обработки информации;
- устройства для передачи информации по каналам связи;
- информационные комплексы и системы.

[67] 2001; Guidelines for best practice in the forensic examination of digital technology. IOCE, May 2002. <http://www.ioce.org/fileadmin/user_upload/2002/Guidelines for Best Practices in Examination of Digital Evid.pdf> (дата последнего посещения 20.12.2020); Нехорошев А.Б. Компьютерные преступления: квалификация, расследование, экспертиза. Часть 2. Расследование и экспертиза / А.Б. Нехорошев /Под ред. В.Н. Черкасова. Саратов, 2004; Россинская Е.Р. Судебная компьютерно-техническая экспертиза: проблемы становления и подготовки кадров экспертов / Е.Р. Россинская // Теория и практика судебной экспертизы, № 3, 2008, с.62–63.

[68] См. *Россинская Е. Р., Семикаленова А. И.* «Основы учения о криминалистическом исследовании компьютерных средств и систем как часть теории информационно-компьютерного обеспечения криминалистической деятельности» // Вестник Санкт-Петербургского университета. Право. 2020. Том 11. Вып. 3. С. 745–759.

Необходимо отметить, что все перечисленные виды объектов содержат цифровые следы, могут продуцировать собственные цифровые следы и участвуют в формировании криминалистически значимой компьютерной информации. В связи с этим рассмотрим их подробнее.

2.1.1.1. Устройства для хранения информации

Устройства предназначенные для хранения информации (носители информации), или, более коротко, – запоминающие устройства, могут быть классифицированы по различным основаниям.

Конечно, в традиционной криминалистике возможна классификация носителей информации, как физических объектов, по цвету (например, корпуса USB-флеш-накопителя), запаху (как у свежеотпечатанных купюр) или весу (более 500 г), но, с точки зрения «цифровой криминалистики», то есть исходя из специфики криминалистического исследования на сегодняшний день считают существенной классификацию объектов памяти определяющую, применяемые к ним технические средства.

При получении доступа к устройствам хранения и изъятия с них криминалистически значимой компьютерной информации наиболее важно определить порядок действий, позволяющий сохранить содержащиеся на устройствах цифровые следы в неизменном виде, а это, в первую очередь, зависит от отнесения устройства к тому или иному виду в соответствии с основаниями классификации, указанными ниже.

Запись информации (данных) – это процесс преобразования информационных сигналов в пространственное изменение физических характеристик (например, наличие или отсутствие заряда, ориентация вектора намагниченности и др.) или формы частей (ячеек памяти) носителя записи (например, следы от прожигания лазером одноразового оптического компакт диска) с целью сохранения и последующего воспроизведения записанной информации.

В процессе записи могут использоваться различные способы кодирования (помехоустойчивые коды, сопоставляемые уровни электрических сигналов, магнитных полей и т.д.) и организации записываемой информации (файловые системы, отказоустойчивые RAID-массивы, LVM-тома и т.д.), а также изменения физических или биологических свойств носителя.

Хранение является одной из основных операций, осуществляемых над информацией (данными) и служит главным способом для обеспечения её доступности в течение определённого промежутка времени (от долей секунды и до сотен лет).

Ещё буквально пару десятилетий назад устройства хранения информации принято было разделять на два вида по признаку расположения: в компьютерной системе или вне её, соответственно: внутренние и внешние.

К внутренним относились (и продолжают относиться): устройства, обеспечивающие работоспособность самой вычислительной системы (компьютера, ноутбука, планшета, телефона (смартфона), часов (смарт-часов) и т. п.) оперативная память, кэш-память, память микросхемы с BIOS, регистры внутри процессора и т. д. К внешним было принято относить большинство запоминающих устройств, известных как винчестер (жёсткий диск), твердотельный накопитель, USB-флеш-накопитель, карта памяти, оптический диск (CD, DVD, BD) и др.

Эта классификация условная и не совсем однозначная, если не написать прямо – не совсем нравится авторам, поскольку тот же жёсткий диск может оказаться как внутри компьютера, так подключаться к нему как внешний накопитель, но не в ней суть проблемы. На сегодняшний день существует (чётко обрисовавшись примерно лет 10 назад) ещё один вид устройства хранения информации – облачное хранилище, располагающееся в сети интернет. Данный вид хранения является гибридным, что вытекает из самой сути такого вида хранения. Данные, подготовленные и обработанные пользователем на своём компьютерном средстве и предназначенные для использования на нём или других компьютерных системах, хранятся на внутренних носителях информации серверов, расположенных за пределами системы пользователя.

При этом информация может как храниться явно на каком-то физическом носителе какого-то удалённого сетевого устройства, так и делиться на части, дублироваться, а также воссоздаваться на лету, появляясь «на свет» лишь как результат вычислений некоторого алгоритма или математической функции в отношении двух или более полученных частей из разных мест.

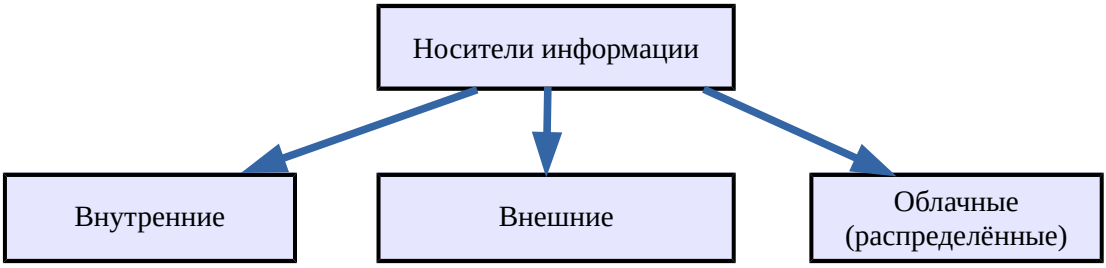


Рисунок 2. Классификация носителей информации

Следует отметить, что классификация устройств хранения информации, имеющая существенное криминалистическое значение, может осуществляться и по иным основаниям. Немаловажным является подразделение устройств хранения информации по принципу энергозависимости устройства, когда они могут быть разделены на два класса: энергозависимые (оперативная память) и энергонезависимые (жёсткие магнитные диски, флеш-память, оптические и магнитооптические диски и др.). Энергозависимые устройства требуют постоянного использования электропитания для возможности удержания записанной на них информации и очищаются при снятии электропитания, в то время как энергонезависимые запоминающие устройства сохраняют информацию при отключении электропитания.

Простой пример – выключили планшет, телефон или компьютер во время неправильного изъятия и потеряли какую-то важную информацию, которая могла бы служить доказательством.

2.1.1.2. Устройства ввода/вывода информации

Устройства ввода информации предназначены для преобразования поступающих от пользователя данных в доступную для обработки системой цифровую форму. К таковым относятся клавиатуры, манипуляторы (мыши, джойстики, трекболы), сенсорные

графические планшеты (не путать с мобильными устройствами), интерактивные доски, сканеры, веб-камеры, устройства видеозахвата, звуковые карты с аудиовходом, считыватели смарт-карт, акселерометры и гироскопы, приемники спутниковой навигации, сканеры папиллярных узоров и узоров сетчатки глаз, разного рода датчики и измерительное оборудование, а также иные устройства.

Устройства вывода информации предназначены для преобразования информации из цифровой формы в форму, доступную для восприятия человеком, а также техническими средствами. К ним относятся индикаторы, мониторы, проекторы, принтеры, звуковые карты, исполнительные механизмы и телемеханика (например, турникет или электронный замок) и т.д.

2.1.1.3. Устройства обработки информации

Устройства обработки информации предназначены для регистрации поступающей информации и формирования управляющих команд в соответствии с алгоритмом. Среди компонентов персонального компьютера примером устройства обработки информации являются центральный процессор, графический контроллер (видеокарта), звуковой процессор (звуковая карта). В устройствах обработки информации также обычно присутствует оперативная память, используемая для хранения обрабатываемых объёмов информации (кэш, буфер). Строго говоря, практически в каждом цифровом устройстве в том или ином виде имеется устройство обработки информации – микроконтроллер (преобразователь), осуществляющий обработку данных по алгоритму, заложенному в микропрограмме («прошивке», «микрокоде») и хранящемуся в постоянном запоминающем устройстве (ПЗУ), либо перепрограммируемом постоянном запоминающем устройстве (ППЗУ).

2.1.1.4. Устройства передачи информации

Устройства передачи информации по каналам связи по своей сути представляют собой устройства ввода/вывода информации, которые осуществляют преобразование поступающих данных в сигнал, пригодный для передачи по каналу связи (модуляцию, а точнее, манипуляцию), и его трансляцию, а также приём сигналов и их обратное преобразование в доступную для обработки форму (демодуляцию). К устройствам относятся коммутаторы (switch), маршрутизаторы (router), Wi-Fi-маршрутизаторы (точки доступа), модемы, сетевые карты, GSM/CDMA-модули, bluetooth-модули, модули ИК-связи, модули NFC и др.

Необходимо особо отметить, что передачу и хранение криминалистически значимой информации – цифровых следов следует рассматривать не только для компьютерных средств и систем, но и для мобильных телефонов сотовой связи, смартфонов, планшетов. Данные устройства в силу своего всеобщего использования являются одними из самых распространённых объектов криминалистического исследования компьютерных средств и систем, поскольку выступают не только как носители и средства передачи криминалистически значимой информации – цифровых следов, но нередко используются как орудия совершения преступлений. Подобные мобильные устройства в ряде случаев не могут классифицироваться как отдельные электронно-вычислительные машины (ЭВМ, компьютеры), поскольку отличительной особенно-

стью имеют постоянное соединение с сетью и являются её частью.[69] Они представляют собой интегрированные устройства, которые:

- содержат в своём составе вычислительный модуль (персональный компьютер, иногда с урезанными возможностями), устройство связи, коммутации;
- используют специфическое программное обеспечение (в том числе в составе микрокода отдельных компонентов устройства);
- содержат носители информации (SIM-карты, карты памяти, USB-накопители);
- осуществляют функции терминала глобальной системы позиционирования (ГЛОНАСС/GPS), оснащены фото- и видеокамерами.[70]

Современная компьютерная система (цифровое устройство) независимо от своих конструктивных особенностей (будь то сервер, ноутбук, смартфон или планшет) по сути является единым информационным комплексом. Управление данным информационным комплексом и взаимодействие его составных частей осуществляется посредством программного обеспечения, которое в свою очередь является как средством, продуцирующим цифровые следы, так и само представляет собой цифровой след (способно хранить цифровые следы от других устройств).

Отличительными чертами доказательственной информации, хранящейся в цифровом виде, являются следующие:

- неявный вид и необходимость использования специальных средств для обеспечения её восприятия (например человеку просмотреть типичный файл-картинку, например, цифровую фотографию в формате JPG, невооружённым взглядом не предоставляется возможным);
- возможность уничтожения или модификации информации в кратчайшие сроки и удалённо;
- наличие специальных средств, ограничивающих доступ к данной информации;
- постоянное изменение информации в ходе работы пользователя и выполнения различных операций;
- формирование взаимосвязанной информации на различных устройствах одновременно при передаче данных по каналам связи.

Перечисленные свойства цифровых данных обусловливают необходимость соблюдения определённых правил при фиксации и изъятии цифровых следов, а также их судебно-экспертном исследовании (ссылка).

Криминалистические технологии выявления, фиксации и изъятия криминалистически значимой доказательственной и ориентирующей информации при работе с компьютерными средствами и системами также должны быть отражены в рассматриваемом разделе криминалистической техники. Укажем основные принципы, которыми следует руководствоваться при проведении следственных действий, сопряжённых с изъятием компьютерных средств и систем:

- не должна изменяться никакая (в том числе и служебная, недоступная пользователю) информация, содержащаяся на изымаемых носителях компьютерной информации;

[69] Физическое извлечение SIM-карты, отсутствие положительного баланса или отключенный режим «передачи данных» существенно не меняют картины, поскольку у таких устройств невозможно отключить модуль связи, то есть разорвать связь с сетью. Наглядный пример, – осуществление связи с экстренной службой «112».

[70] *Семикаленова А. И., Сергеева К. А.* Мобильные телефоны сотовой связи – новые объекты судебной компьютерно-технической экспертизы. // Законы России, опыт, анализ, практика, № 12, 2011. – С. 89–94.

- любые манипуляции с компьютерными средствами и системами должны осуществляться только с участием специалиста;
- доступ к информации и исследование её на месте допустимы только когда невозможно изъять носитель для производства судебной экспертизы;
- все выполняемые действия должны подробно протоколироваться, чтобы обеспечить возможность использования результатов этих действий в доказывании.

Непосредственное восприятие цифровых следов невозможно, поэтому для выявления невозможна чувственно-рациональная форма восприятия. Выявление цифровых следов производится опосредованно с использованием специализированного криминалистического прикладного программного обеспечения, предназначенного для их поиска, сохранения и изъятия (консервирования на электронном носителе информации). Причём следует учитывать возможность безвозвратного уничтожения цифровых следов вследствие активного противодействия расследованию, оказываемого преступниками, заранее предусматривающими с целью сокрытия преступления в определённых условиях высокую скорость трансформации и возможности уничтожения либо фальсификации информации. Особенно это актуально при выявлении цифровых следов на работающей энергозависимой компьютерной системе.

Как указывалось выше, при собирании цифровых следов необходимо обеспечить их сохранение в неизменном виде. Если это невозможно, используются специальные средства криминалистической техники для создания копий, их верификации и документирования.[71]

2.1.1.5. Виртуальные компьютеры и сети, ЦОДы и др.

Отдельно необходимо отметить круглосуточно функционирующие системы, аттестованные по заданным требованиям информационной безопасности [23-24], [28-30], перезапуск или отключение, которых для осуществления идентификации, сбора и фиксации в электронной форме данных в качестве цифровых доказательств традиционными методами и средствами компьютерной криминалистики, затруднительны или не рациональны (например: федеральные электронные платёжные системы, системы управления инфраструктурой критически важных объектов и др.).

Более того значительный пласт автоматизированных и информационных систем, в том числе и информационные системы персональных данных, теперь разворачиваются в сторонних центрах обработки и хранения данных (далее – ЦОД). Подконтрольность ЦОД третьей стороне, применение технологий виртуализации и гиперконвергенции инфраструктуры несёт новые угрозы информационной безопасности (далее – ИБ) и затрудняет применение типовых методов и средств компьютерной криминалистики, рассчитанных на работу с обычными смартфонами, персональными электронно-вычислительными машинами (далее – ПЭВМ), машинными носителями информации (далее – МНИ) и в информационно-телекоммуникационных сетях (далее – ИТКС) вне виртуальной инфраструктуры ЦОД.

Ситуация усугубляется тем, что в рамках реализации государственных программ «Информационное общество» [15] и «Цифровая экономика Российской Федерации»

[71] Более подробно процессы выявления, фиксации и изъятия цифровых следов при производстве следственных действий описаны в главе 2.3 данного пособия.

[17], Министерством цифрового развития, массовых коммуникаций и связи Российской Федерации предложены и Правительством Российской Федерации одобрены концепции перевода государственных информационных ресурсов в ЦОДы [16] и развёртывания государственной единой облачной платформы [18], в 2019 г. начат соответствующий эксперимент [19].

Складывающиеся тенденции развития и практического применения информационных технологий требуют системного переосмысления достаточности имеющегося арсенала методов и средств компьютерной криминалистики: от поиска и апробации нового инструментария для компьютерно-технических экспертиз (далее – КТЭ) до новаций в тактике и средствах проведения оперативно-технических и оперативно-разыскных мероприятий в информационно-технической сфере.

2.2. Новые проблемы

Какие новые проблемы породили цифровые следы?

Большинство компьютерно-технических экспертиз проводится в подразделениях, где созданы соответствующие лабораторные условий для их осуществления. Такой подход по организации КТЭ и возможности использования имеющегося парка программно-технических средств компьютерной криминалистики вполне приемлем для исследования большинства образцов техники и носителей данных, полученных от физических или юридических лиц, в том числе и из государственных организаций и предприятий промышленности.

Вместе с тем бурный рост систем информатизации привёл к переводу на автоматизированную обработку многих процессов управления и обработки информации в организациях, на предприятиях промышленности и транспорта. Характерным примером могут служить локально-вычислительные сети оборонных предприятий и автоматизированные системы управления технологическим процессом (АСУТП), аттестованные в качестве автоматизированных систем в защищённом исполнении по требованиям ФСТЭК и ФСБ России для обработки и защиты сведений, составляющих государственную тайну.

Как можно догадаться, на таких предприятиях не всегда возможно изъятие ПЭВМ, МНИ и оборудования ИТКС для проведения выявления и разбора компьютерных инцидентов, проведения лабораторных исследований и экспертиз в полном объёме без остановки производственного процесса.

Например, остановка технологических процессов на нефтеперерабывающем заводе с целю изъятия и исследования машинных носителей компьютера управляющей системы в течении нескольких дней, может обернуться значительными финансовыми потерями, которые по своему объёму могут превысить нанесённый ущерб от той негативной деятельности в отношении которой заведено и расследуется уголовное дело.

2.2.1. Присутствует защищаемая законом информация

Если в обследуемых системах может присутствовать или присутствует защищаемая законом информация, то возникает ситуация, когда возможна её компрометация, то есть она может стать известной третьим лицам для которых она не предназначена.

В соответствии с нормами Российского законодательства выемка предметов и документов, содержащих государственную или иную охраняемую федеральным законом тайну, информацию о вкладах и счетах граждан в банках и иных кредитных организациях (для платёжных систем) производится на основании судебного решения, которое, как правило, получается только в рамках уголовного дела.

Вот это как раз тот случай, когда сам «инструмент» опертехника, цифрового криминалиста или ИТ-специалиста, участвующего в процессуальных мероприятиях, должен обеспечить защиту обрабатываемой информации, не влиять на саму защищённую систему, из который изымается информация. Именно поэтому необходимо применить сертифицированные ФСТЭК, МО или ФСБ России средства, позволяющие осуществлять идентификацию, сбор и фиксацию в электронной форме данных защищённых информационных и автоматизированных систем управления. Такие средства аудита, контроля защищённости, анализа носителей информации нетрудно найти в реестре[72] средств защиты ФСТЭК России и в перечне[73] ФСБ России.

А с позиции документирования инцидентов – большую практическую отдачу начинают приносить выполнение государственными организациями, предприятиями связи, промышленности и транспорта законодательных норм по предупреждению, выявлению и ликвидации последствий компьютерных инцидентов – ГосСОПКА [26-28] на критически важных объектах и в их информационной инфраструктуре, зачастую не связанной с обработкой сведений, составляющих государственную или иную охраняемую тайну.

Росту количества нейтрализованных инцидентов информационной безопасности в автоматизированных системах и существенному снижению ущерба от них способствует высокая результативность и популяризация стандартизации правоохранительными и контролирующими органами методов проверки режима защиты и аудита информационной безопасности с использованием инструментальных средств и методов [104-108, 160].

Здесь и далее рассмотрим более подробно применяемые методы и меры защиты от компрометации обрабатываемой информации в ходе разбора компьютерных инцидентов в защищённых информационных системах, не обрабатывающих сведения, составляющие государственную тайну.

К правовым и организационным мерам защиты информации следует отнести требования по наличию у привлекаемых сотрудников соответствующих допусков к сведениям по равному или более высокому уровню конфиденциальности, установленному для исследуемой системы, наличия специальных знаний (в области информационных технологий), а также принятию экспертом обязательств по неразглашению охраняемой законом тайны (тайны связи, тайны следствия, тайны о фактах личной жизни фигурантов и иных лиц, коммерческой тайны предприятия, врачебной тайны, налоговой и банковской тайны и т.п.).

[72] Государственный реестр сертифицированных средств защиты информации (ФСТЭК России), URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00

[73] Перечень средств защиты информации, сертифицированных ФСБ России (выписка). URL: http://clsz.fsb.ru/files/download/svedeniya_po_sertifikatam_04112022.doc (дата обращения: 12.11.2022).

2.2.1.1. Банковские системы

Для рассмотрения мер защиты от компрометации при идентификации, сборе и анализе технических данных защищённых автоматизированных систем в экономической отрасли: автоматизированные банковские и электронные платёжные системы, помимо требований к защите платёжных систем [29-30] и стандартов [100-105] следует использовать следующие отраслевые документы технического регулирования:

- СТО БР ИББС-1.3-2016 [106];
- РС БР ИББС-2.9-2016 [107];
- РС БР ИББС-2.5-2014 [108].

Для защиты от компрометации автоматизированных банковских систем в России установлены следующие правила идентификации и сбора цифровых криминалистических данных [106]:

- следует разделять содержательную (семантическую) информацию, защищаемую в соответствии с требованиями законодательства РФ, от не являющейся таковой методом группирования информации:
  - в отдельных постраничных разделах документов, а также путём помещения её в раздельные документы на бумажном носителе;
  - в различных файлах данных;
- следует обеспечить поиск (выделение) только той содержательной (семантической) информации, защищаемой в соответствии с требованиями законодательства РФ, которая имеет отношение к конкретному инциденту информационной безопасности (или их группе);
- следует использовать «доверенные» программно-технические средства;
- обработка содержательной (семантической) информации не должна приводить к формированию сводной информации обо всех клиентах организации Банковской системы Российской Федерации или информации о клиентах организации, не имеющих отношения к конкретному инциденту информационной безопасности (или их группе), в отношении которого осуществляется реагирование.

В случае отсутствия возможности разделить содержательную (семантическую) информацию, защищаемую в соответствии с требованиями законодательства РФ, от не являющейся таковой носители содержательной (семантической) информации, передаваемые в правоохранительные органы, должны быть классифицированы и маркированы в соответствии с правилами, установленными в организации Банковской системы Российской Федерации, и передаваться по акту, в котором среди прочего определяется обязанность принимающий стороны обеспечить конфиденциальность передаваемой информации (т. е. использование правовой меры защиты информации).

2.2.2. Необходима фиксация в электронной форме

Практически все легковые автомашины могут использоваться для перевозки пассажиров, но не все из них являются легальными такси, прошли технический осмотр, пассажиры застрахованы, а в конце поездки будет выдана электронная или бумажная квитанция о стоимости проезда. Так же и не все доступные и подходящие технические

средства «de facto» могут «de jure» применяться в ходе съёма, изъятия или осмотра компьютерной информации или компьютерно-технических экспертиз (о чём авторы и успели рассказать выше).

В случае исследования и документирования компьютерных инцидентов в защищённых информационных системах дополнительно необходимо уделять внимание приданию юридического значения показаниям программно-технических средств, что достигается за счёт:

1) законодательного установления «презумпции достоверности» информации, полученной с помощью доверенных программно-технических средств;

2) идентификации и аутентификации пользователей программно-технических средств;

3) применения определённых типов, видов или моделей программно-технических средств, прошедших сертификацию и/или поверку (для средств измерения);

4) обеспечения целостности и достоверности представленных в виде компьютерной информации показаний программно-технических средств на основе криптографических методов и средств, например, имитозащиты (криптографических контрольных сумм) или средств электронной подписи на базе отечественных стандартов.[74]

2.2.3. Примеры проблемных случаев

Бывают ситуации когда сложность исследуемой компьютерной системы накладывает свой отпечаток на то как в ней будет проводиться экспертиза. То есть обычный подход «в лоб», даже с учётом замечаний выше, не работает. Приведём пару подобных примеров сложных инцидентов в специальных системах.

Инцидент 1.[75]

Ключевым элементом успешной тактики проведения исследований методами компьютерной криминалистики по выявлению внутреннего нарушителя, обладающего привилегированными полномочиями в системе, являлось:

– логически продуманная последовательность действий, не нарушающая механизмов защиты информации технической системы и не позволившая её пользователям и администратору активно препятствовать исследованию системы, идентификации и сбору доказательств;

[74] Как обычно, есть исключения из правила, например, Банком России и российским сообществом FinCERT при фиксации цифровых доказательств инцидента в автоматизированных банковских и платёжных системах разрешается использование иностранных криптографических функций [106] серии MD5 и SHA, что вызвано необходимостью унификации методов контроля целостности с применяемыми за рубежом с целью возможности признания добытых в России цифровых доказательств при организации международного уголовного преследования и представления информации иностранным и международным организациям.

[75] См. новости от 29.11.2019: На Южном Урале два пограничника попались на взятках [Электронный ресурс]. – Режим доступа: https://uralpress.ru/news/proisshestviya/na-yuzhnom-urale-dva-pogranichnika-popalisna-vzyatkah. (Дата обращения: 09.01.2023); В Челябинске перед судом предстанут пограничники, обвиняемые в нарушении правил несения службы [Электронный ресурс]. – Режим доступа: http://gvsu.gov.ru/news/v-chelyabinske-pered-sudom-predstanut-pogranichniki-obvinyaemye-v-narushenii-pravil-neseniya-sluzhby/. (Дата обращения: 09.01.2023).

– привлечение сторонних по отношению к данному комплексу специалистов, обладающих специальными знаниями в области развёртывания и эксплуатации технических систем данного типа;

– создание условий минимизации вносимых изменений за счёт перенаправления основной части информационных потоков на резервные мощности;

– наличие, работоспособность и постоянный контроль подсистем журналирования событий, сопоставление данных из которых с последовательностью аналогичных событий в других системах позволило выявить и зафиксировать детали компьютерного инцидента.

Инцидент 2.[76]

Другим примером может служить ситуация с проблемой осуществления КТЭ средств управления вредоносным программным обеспечением, ранее предположительно располагавшемся на сервере сети интернет вне юрисдикции Российской Федерации.

2.2.4. Выводы по проблемам

В виду прихода в нашу жизнь повсеместно технологий 4-й промышленной революции[77] правоохранительные органы сталкиваются с широким разнообразием используемых в настоящее время различных автоматизированных систем и их спецификой. К сожалению, должное организационно-методическое обеспечение по большинству подобных систем отсутствует. Дополнительная проработка и внимание со стороны эксперта по цифровой и компьютерной криминалистике могут потребоваться для:

- систем автоматизированного управления инфраструктурой (например: в центре обработки и хранения данных, в т. ч. управления его инженерной инфраструктурой);
- автоматизированных систем управления сетями связи общего пользования (у операторов связи);
- автоматизированных систем исследований (научных, медицинских, химических, ядерных и т. п.);
- систем автоматизированного проектирования, технологической подготовки производства и его контроля.

Возможность идентификации и сбора данных в таких специализированных системах за счёт возможностей широко распространённых инструментальных средств существенно ограничена.[78] Общий подход по работе с такими системами, к сожалению, пока только опирается на следующие факторы:

[76] См. новость: В недоливе бензина обвинили вредоносную программу. Расследуется дело о хищениях на ставропольских АЗС. – Газета "Коммерсантъ" № 167 (6647) от 16.09.2019 [Электронный ресурс]. – Режим доступа: https://www.kommersant.ru/doc/4094388. (Дата обращения: 01.12.2022).

[77] См. *Шваб К., Дэвис Н.* Технологии четвёртой промышленной революции : [перевод с английского] / М.: Эксмо, 2018, ISBN 978-5-04-095268-7.

[78] Например. задайтесь относительно не сложными вопросами на эрудицию: А в каком формате хранятся изображения создаваемые медицинским оборудованием, например томографом, либо каким средством исследовать временные срезы файловой системы в слепке (гибернации) виртуальной машины?

- применение в специальных системах ранее встречавшихся типовых решений для обычных компьютеров (и иной техники бытового назначения), что позволит подобрать инструментальные средства;
- личная эрудиция и квалификация привлекаемого специалиста в данной предметной области, что позволит грамотно построить (как правило и перестроить) и реализовать тактику исследования системы, оказать реальную методическую помощь оперативникам и следователю (дознавателю) в постановках задач на такие исследования;
- возможность использования базы знаний о технологии обработки информации в системе из открытых источников или привлечения к работам второго узкоспециализированного специалиста, обладающего специальными знаниями по технологии работы такой специальной системы;
- создание возможности подключения дополнительных носителей и устройств к оборудованию системы для копирования значимой технологической информации.

2.3. Сбор и фиксация цифровых доказательств

2.3.1. В ходе производства осмотра

Тактика и особенности сбора и фиксации цифровых и вещественных доказательств по уголовным делам, связанным с информационными технологиями, в ходе производства осмотра.

В ходе осмотров и обысков обычно исследуются (обследуются) служебные и жилые помещения, салоны транспортных средств, средства вычислительной техники, носители машинной информации, документы, предметы и иные объекты.

Важно: Производя осмотр и обыск или выемку, необходимо учитывать, что компьютерное оборудование и компьютерная информация, как уже упоминалось, могут быть предметом посягательства, орудием преступления и хранилищем доказательств.

Как отмечают специалисты, осмотр является самым многогранным и сложным следственным действием, сложность которого, помимо прочего, обусловлена его неотложностью. То есть осмотр обычно производят по горячим следам совершённого преступления, что оставляет крайне мало времени для его подготовки.

Даже при наличии некоторого опыта (и внутреннего ощущения своей уверенности) подготовительные мероприятия провести всё же необходимо, иначе, прибыв на место происшествия для его осмотра с целью поиска, фиксации и изъятия следов преступления и других вещественных доказательств, выяснения обстановки и иных обстоятельств, имеющих значение для дела, следователь может столкнуться с проблемной ситуацией, поскольку, в отличие от «не компьютерных преступлений» не обнаружит каких-либо видимых материальных признаков совершённого деяния. При первом взгляде окажется, что в жилых или офисных помещениях порядок не нарушен, находящиеся в них средства вычислительной техники (компьютеры, мобильные устройства, серверы, маршрутизаторы), в ряде случаев связанные в локальную сеть и размещённые

в разных частях здания, работают без видимых внешних изменений, лампочки характерно мигают, материальные ценности на месте, следов присутствия посторонних лиц, борьбы, взлома замков, наличия пулевых отверстий, запахов и др., за что можно было бы зацепиться – нет.

Установление связи между преступлением и осматриваемым объектом (предполагаемым местом происшествия) при таких обстоятельствах возможно только с использованием специальных знаний и с применением криминалистических технических средств (специальных программных и технических средств).

По общему правилу при осмотре места происшествия в состав следственно-оперативной группы (далее – СОГ), в зависимости от конкретной следственной ситуации, помимо следователя (дознавателя), должны входить:

- специалист-криминалист, знающий особенности работы со следами по преступлениям данной категории;
- оперативные сотрудники;
- участковый инспектор, обслуживающий данную территорию;
- представитель Росгвардии или ведомственной охраны (ОАО «РЖД», Госкорпорации «Росатом» и др. – в случае, когда место происшествия или средство вычислительной техники (далее – СВТ), находящееся на нём, одновременно является охраняемым объектом);
- специалист-криминалист для проведения цветной фото- или видеосъёмки следственного действия.

Например, группа может быть такой:

- ведомственный следователь или дознаватель[79];
- дежурный кинолог с собакой или криминалист-дактилоскопист;
- ИТ-специалист, как правило, тоже ведомственный;[80]
- специалист узкой компетенции.[81]

При необходимости в ходе заблаговременного планирования в состав СОГ могут быть включены незаинтересованные в деле специалисты, знающие специфику работы осматриваемого объекта (инженеры-электрики, техник по системам сигнализации, видеорегистрации и пожаротушению, бухгалтеры со знанием СВТ, специалисты спутниковых систем связи, операторы компьютерных систем и техники сетей электросвязи, др.).

Целью осмотра места происшествия является установление конкретного СВТ и компьютерной информации, выступающей в качестве предмета и(или) орудия совер-

[79] Дознаватель может быть как штатным в органах внутренних дел, военной полиции, таможне, пограничной или противопожарной службе, так и внештатным — офицер-дознаватель войсковой части, уполномоченный по УПК РФ начальником органа дознания — командиром войсковой части.

[80] Как правило, в качестве основного ИТ-специалиста привлекают ведомственного специалиста технического профиля: инженера подразделения информационных технологий, связи и защиты информации РОВД, опертехника из подразделения специальных технических мероприятий УВД или дежурного специалиста из инженерно-технического подразделения экспертно-криминалистического центра (отдела) УВД ГУ МВД России по субъекту РФ, аналогично, и в СК или в ФСБ России.

[81] В экстраординарных случаях это может быть иной специалист, например, сотрудник подразделения Минюста, ФСТЭК, ФТС России и др. (например, при возможном наличии на месте происшествия конфиденциальной таможенной информации в электронном виде, машинных носителей с ней, специальных средств защиты от НСД и(или) специальных технических средств для обращения с компьютерной информацией).

шения преступления и несущих в себе следы преступной деятельности. Поэтому при производстве следственного действия целесообразнее всего использовать тактический приём «от центра – к периферии», где в качестве «центра» (отправной точки осмотра места происшествия) будет выступать конкретное СВТ и(или) компьютерная информация, обладающая вышеуказанными свойствами. Детальное описание данных предметов, их соединений (физических и логических) должно сопровождаться видеосъёмкой, фиксирующей последовательность действий следователя и специалистов, а также полученный при этом результат.

Замечание. Если при проведении осмотра места происшествия используются специализированные комплексы, СВТ и специальные поисковые технические устройства (материалы), об этом делается соответствующая отметка в протоколе следственного действия с указанием их индивидуальных признаков (тип, марка, название, заводской номер и т.д.). Кроме того, в обязательном порядке делается отметка о том, что данные СВТ перед началом следственного действия в присутствии понятых были тестированы антивирусным средством (указывают его тип, вид, название, версию, автора и другие реквизиты) на предмет отсутствия в них вредоносных программных средств (за исключением ранее сертифицированных систем и комплексов, неподверженных модификации).

Следователю необходимо знать, что к изменению или уничтожению компьютерной информации (следов преступника и преступления) может привести не только работа за пультом управления цифрового устройства (для СВТ это обычно клавиатура), но и одноразовое кратковременное включение-выключение СВТ или разрыв соединения между ними. Поэтому, если на момент проведения следственного действия какие-либо СВТ и иные электротехнические приборы и оборудование были включены или выключены, то они должны оставаться в таком положении до момента окончания осмотра их специалистом. По этой же причине подлежат обязательной охране все пункты отключения электропитания, находящиеся на месте происшествия.

Замечание. Для последующей однозначной идентификации нужно более подробно описывать средства СВТ, включая их форм-фактор, номера, наименования, фирмы производителя, другие идентифицирующие особенности. В этом случае исключается вопрос о подмене объектов-доказательств. В отношении цифровых следов также важна полнота данных, а именно: вид, наименование, объём, время создания, редактирования, местоположение, хэш, другая мета-информация.

При неполном копировании данных цифрового объекта необходимо описание его идентифицирующих признаков, иначе невозможно будет идентифицировать объект и адвокаты скажут, что объект исследовался другой.

Особенно тщательно должны быть описаны в протоколе следующие фактические данные:

- технические и конструктивные особенности местности, связанные с установкой и эксплуатацией СВТ, включая расположение и основные характеристики токонесущих коммуникаций;
- расположение СВТ относительно друг друга и оконечных устройств токонесущих коммуникаций;
- отсутствие или наличие соединений между ними (видимых и дистанционных);
- наличие или отсутствие соединений СВТ с оборудованием, в том числе находящемся вне территории осмотра (на это могут указывать кабели и провода, идущие от осматриваемого СВТ за границы места осмотра, либо к аппаратам элек-

тросвязи (в таком случае границы осмотра места происшествия значительно расширяются);

- наличие, внешнее состояние, расположение и вид охраны СВТ и компьютерной информации от НСД, их основные технические характеристики;
- расположение СВТ относительно вентиляционных и иных отверстий в строительных конструкциях, дверных и оконных проёмов, технических средств видеонаблюдения, а также относительно других рабочих мест;
- наличие в одном помещении со СВТ других электрических устройств и приборов (телефонных, селекторных и иных аппаратов электросвязи, электронных замков, домофонов, пейджеров, систем электрочасофикации, оргтехники – ксероксов, аудио-, видеомагнитофонов, автоответчиков, электрических пишущих машинок, приборов электроосвещения, громкоговорителей, телевизоров, радиоприёмников, электронных термометров, погодных станций, чайников, кофеварок и даже утюгов[82] с электронными модулями связи и т.д.).

Также особенно тщательно должны быть осмотрены и описаны в протоколе типичные вещественные доказательства в цифровой среде:

- вредоносные программы для ЭВМ и машинные носители с ними;
- программы для ЭВМ, заведомо приводящие к несанкционированным пользователем действиям (влияющие на конечные результаты технологического процесса), а также их носители;
- обнаруженные специальные технические средства (получения, уничтожения, блокирования компьютерной информации и магнитных носителей);
- специфические следы преступника и преступления.

Типичными вещественными («аналоговыми») следами являются:

- следы орудий взлома, повреждения, уничтожения и(или) модификации охранных и сигнальных устройств;
- показания регистрирующей аппаратуры (видеотехники, электронного журнала учёта операций с компьютерной информацией, доступа к ней и СВТ, др.);
- показания специальных мониторинговых (тестовых) программно-аппаратных средств, в том числе электронной подписи (далее – ЭП);[83]
- следы пальцев рук на СВТ, охранных и сигнальных устройствах, на их клавиатуре, соединительных и электропитающих проводах и разъёмах, на розетках и штепсильных вилках, тумблерах, кнопках и рубильниках, включающих и отключающих СВТ и электрооборудование; остатки соединительных проводов и изоляционных материалов; капли припоя, канифоли или флюса;

[82] Производители бытовой техники доукомплектовывают её модулем, который передаёт данные на зарубежный сервер через незащищенные wi-fi сети. См. новость от 22.10.2013 Китайские утюги и чайники следят за петербуржцами [Электронный ресурс] https://spb.mk.ru/article/2013/10/22/934460-kitayskie-utyugi-i-chayniki-sledyat-za-peterburzhtsami.html, (Дата обращения 22.10.2013).

[83] Электронная подпись – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе – (см.: Об электронной цифровой подписи: Федеральный закон от 10.01.2002 г. № 1-ФЗ. Ст. 3).

- следы вдавливания, проплавления, прокола, надреза изоляции токонесущих и соединительных (управляющих) проводов, приклеивания к ним сторонних предметов и устройств.

Важно:

Осмотру подлежат следующие документы и их носители, являющиеся доказательствами подготовки, совершения и сокрытия преступления:

а) учётно-справочная документация по работе с СВТ и компьютерной информацией (технический паспорт или документ его заменяющий; журнал оператора или протокол автоматической фиксации технологических операций, доступа к СВТ и конфиденциальной компьютерной информации; журналы (карточки) учёта машинных носителей информации, машинных документов, заказов (заданий или запросов), выдачи МНИ и машинных документов, массивов (участков, зон), программ, записанных на МНИ; журналы учёта уничтожения брака бумажных носителей, в том числе номерных бланков и бланков строгой отчётности (для конфиденциальных материалов – банки, производство, коммерция, адвокатура и нотариат и т. п.) и МНИ (диски, флэш-накопители, ноутбуки и т.п.); акты на стирание конфиденциальной информации и уничтожение машинных носителей с ней – особенно для ЦОД, предоставляющих сторонние услуги);

б) документация, отражающая санкционированность доступа (удостоверения личности, электронные ключи доступа, пароли, персональные идентификационные номера (ПИН-коды), ЭП (в т.ч. на носителях Jacarta, rutoken) и иные средства (предметы или устройства) идентификации и аутентификации санкционированного пользователя — proximty card и т.п.;

в) учётно-регистрационная и бухгалтерская документация (лицензии и лицензионные соглашения; сертификаты соответствия СВТ, программ для ЭВМ, средств защиты информации (в том числе и ЭП), протоколов обмена информацией и форматов электронных документов установленным требованиям; договора (соглашения) на пользование СВТ и доступ к компьютерной информации с соответствующим комплектом документов; расчётно-кассовые и иные бухгалтерские документы, отражающие факт оплаты пользователем предоставленной ему услуги, отпущенного товара или осуществлённой им кредитно-банковской операции);

г) учётно-контрольная документация (журналы (акты) пуско-наладочных, ремонтных и регламентных работ по техническому обслуживанию СВТ, программ для ЭВМ и средств защиты информации; журналы аварий и сбойных (нештатных) ситуаций; акты сбоев и ложных срабатываний охранных сигнализаций; акты контрольных проверок соблюдения режима безопасности информации, ревизий, служебных и иных документальных проверок; сводные отчёты и контрольные показатели по отдельным участкам работы, операциям и временным интервалам);

д) документация, регламентирующая действия обслуживающего персонала (должностные обязанности; инструкции по работе с СВТ, программами для ЭВМ, средствами защиты от НСД, действий оператора в нештатной (аварийной) ситуации; черновая рабочая документация оператора СВТ).

Их осмотр позволяет установить способ совершения преступления в сфере компьютерной информации, использованные для этого преступником материалы и

средства, наличие у субъекта специальных навыков и познаний; выдвинуть версии о причинно-следственных связях.

Более того осмотр и обыск должен иметь цель поиска, обнаружения, закрепления и изъятия всех возможных следов (в т. ч. «цифровых следов»), связанных или функциональным назначением технических (информационных) объектов (ЭВМ, сети ЭВМ, машинных залов), или с преобладающими гипотезами следствия (дознания).

Примеры того, на что стоит обращать внимание, где искать цифровые следы:

- информация о незаконных бухгалтерских и финансовых операциях, произведённых в кредитно-финансовой сфере;
- программы, отвечающие за проведение электронных платежей по сети интернет с использованием услуг интернет-магазинов и виртуальных фирм, а также списки произведенных перечислений с чужих счетов и кредитных карт;
- программы для осуществления операций с цифровыми активами (электронными монетами *Bitcoin*, *Etherium* и др., виртуальными товарами, виртуальной инфраструктурой, средствами майнинга и т.п.);
- переписка соучастников, касающаяся организации и исполнения преступления (в файлах-журналов программ-мессенжеров, на электронных информационных площадках – форумах);
- сведения, составляющие государственную, коммерческую, банковскую тайну;
- программное обеспечение и базы данных, правообладателями которых являются иные лица;
- личная переписка, компрометирующие материалы и порнографические изображения;
- вредоносные программы;
- файлы, содержащие конфиденциальную информацию, которой на законных основаниях не может обладать данный субъект;
- зашифрованные данные, связанные с совершением преступления.

Однако, несмотря важность «цифровых следов» для установления способа компьютерного преступления, в ходе осмотра места происшествия нельзя сосредотачиваться исключительно на средствах вычислительной техники, игнорируя иные предметы и документы, которые могут нести в себе криминалистически значимую информацию. Так, исходный код вредоносной программы может быть обнаружен в распечатанном либо даже рукописном виде, как и записи, подтверждающие неправомерный доступ к компьютерным системам, пароли к заблокированным компьютерным устройствам, реквизиты доступа к облачным сервисам, схемы сетевой инфраструктуры, используемой при совершении преступлений и т. п.[84] Поэтому немаловажное значение имеет обнаружение и изъятие в помещении, где установлено компьютерное оборудование, «традиционных» вещественных доказательств, например это могут быть:

1. бумажные носители информации (черновики, копии, распечатки с принтера, в том числе оставшиеся внутри его);
2. записи кодов и паролей доступа;
3. тексты программ и описание программного обеспечения;

[84] См. *Аверьянова Т. В., Белкин Р. С., Корухов Ю. Г., Россинская Е. Р.* Криминалистика. Учебник для вузов. Изд. 4-е перераб. и доп. – М.: Норма: ИНФРА-М, 2013. – С. 912.

4. записные книжки, в том числе и электронные, в которых могут находиться имена, клички хакеров и соучастников, номера телефонов, банковских счетов, ПИН-коды пластиковых карт;

5. кредитные карточки соучастников и третьих лиц, с помощью которых обналичивались и изымались денежные средства, похищенные с использованием компьютерных технологий;

6. вещи и ценности, приобретённые на похищенные деньги; телефонные счета за пользование провайдерскими услугами;

7. нестандартные периферийные устройства, устройства доступа в телефонные сети и сети ЭВМ, специальные технические средства (перехвата/снятия, имитации идентификационных номеров абонентов связи и т. п.;

8. документы, должностные инструкции, регламентирующие правила работы с данной компьютерной системой, сетью с пометками сотрудника, свидетельствующие о его ознакомлении с ними;

9. личные документы подозреваемых (предполагаемых преступников).

Если непосредственный доступ к ЭВМ осуществлялся посторонним лицом, целесообразно направить усилия на поиск следов рук на клавиатуре, мониторе, системном блоке, мебели, следов ног на полу, следов орудий взлома, сопровождавшего проникновение преступника в помещение, и пр.

2.3.1.1. Осмотр электронно-вычислительной техники и устройств

В большинстве случаев помимо осмотра места происшествия (объекта информатизации или транспорта) осмотр средства электронно-вычислительной техники является первоначальным следственным действием и проводится для обнаружения следов преступления; для решения вопросов о том, кем, с какой целью и при каких обстоятельствах было совершено преступление; выяснения обстановки происшедшего события; восстановления механизма совершения преступления. Проводить осмотр следует с участием специалиста.

Прежде всего нужно уяснить смысл и назначение СВТ; установить, включено оно или нет; проверить его работоспособность и наличие в его памяти компьютерной информации; установить наличие или отсутствие сопряжения с каналом электросвязи и другими техническими устройствами. После этого необходимо перейти к поиску материальных следов, содержащихся на его корпусе, отдельных деталях и проводных соединениях, в его постоянной и оперативной памяти (в виде компьютерной информации).

Тактические особенности осмотра места происшествия, сопряжённого с работой как с СВТ, так и с цифровыми устройствами и данными, зависят от конкретных обстоятельств дела. При наличии на месте происшествия одного компьютера следователь в полной мере может контролировать полноту, активность, методичность и последовательность осмотра, а роль специалиста носит технический характер и заключается в выполнении определённого набора действий, вариант которых обычно зависит от того, включен или выключен компьютер на момент проведения осмотра.

Возможные варианты:

Вариант № 1. В случае с неработающей системой сначала производится внешний осмотр компьютерной техники, отсоединение кабелей и внешних устройств, их упаковка (в случае изъятия взаимосвязанных объектов необходимо предварительно отметить, к какому порту что подключено) либо, при наличии оснований, может быть изъят не компьютер целиком, а создана побитовая копия его жёсткого диска, которая изымается и приобщается к уголовному делу.

Вариант № 2. Если же система активна, то дополнительно, перед её выключением и созданием копии диска, проводится проверка наличия активных сетевых подключений, осмотр компьютерной информации (установленных и использующихся приложений, файловой системы, запущенных процессов) и снятие копии содержимого оперативной памяти.

При осмотре СВТ недопустимо использование: магнитосодержащих материалов и инструментов; технических устройств, генерирующих и излучающих электромагнитные поля и наводки (магнитный порошок и кисточка, электромагнит, металлодетектор, мощные осветительные приборы, ультрафиолетовые (УФ) и инфракрасные (ИК) излучатели и т. п.); кислотно-щелочных материалов и нагревательных приборов во избежание уничтожения (повреждения) СВТ и компьютерной информации, следов преступника и преступления. Вышеуказанными материалами и оборудованием можно пользоваться с особой осторожностью на расстоянии более одного метра от СВТ и их соединительных проводов.

Таким образом, действия при осмотре средств вычислительной техники (ЭВМ, КПК, смартфона и т. п.) можно изложить в следующем порядке:

- внешний осмотр компьютерной техники;
- проверка наличия активных сетевых подключений;
- осмотр компьютерной информации (установленных и использующихся приложений, файловой системы, запущенных процессов);
- снятие копии (дампа) содержимого оперативной памяти;
- выключение компьютера и создание копии жёстких дисков;
- отсоединение кабелей и внешних устройств (в случае изъятия взаимосвязанных объектов необходимо промаркировать имеющиеся кабельные соединения);
- составление протокола и упаковка изъятого.

Замечание. В протоколе осмотра СВТ фиксируют: его тип (назначение), марку (название), конфигурацию, цвет и заводской номер (серийный, инвентарный или учётный номер изделия); тип (назначение), цвет и другие индивидуальные признаки соединительных и электропитающих проводов; состояние на момент осмотра (выключено или включено); техническое состояние – внешний вид, целостность корпуса, комплектность (наличие и работоспособность необходимых блоков, узлов, деталей, и правильность их соединения между собой), наличие расходных материалов, тип используемого машинного носителя информации; тип источника электропитания, его тактико-технические характеристики и техническое состояние (рабочее напряжение, частота тока, рабочая нагрузка, наличие предохранителя, стабилизатора, сетевого фильтра, количество подключенного к нему электрооборудования, количество питающих электроразъёмов-розеток и т.д.); наличие заземления («зануления») СВТ и его техническое состояние; на-

личие и техническая возможность подключения к СВТ периферийного оборудования и(или) самого СВТ к такому оборудованию, либо к каналу электросвязи; имеющиеся повреждения, непредусмотренные стандартом конструктивные изменения в архитектуре строения СВТ, его отдельных деталей (частей, блоков), особенно те, которые могли возникнуть в результате преступления, а равно могли спровоцировать возникновение происшествия; следы преступной деятельности (следы орудий взлома корпуса СВТ, проникновения внутрь корпуса, пальцев рук, несанкционированного подключения к СВТ сторонних технических устройств и др.); расположение СВТ в пространстве, относительно периферийного оборудования и других электротехнических устройств; точный порядок соединения СВТ с другими техническими устройствами; категорию обрабатываемой информации (общего пользования или конфиденциальная);

наличие или отсутствие индивидуальных средств защиты осматриваемого СВТ и обрабатываемой на нём информации от несанкционированного доступа и манипулирования. Если на момент осмотра СВТ находится в рабочем состоянии необходимо детально описать: расположение его рабочих механизмов и изображение на его видеоконтрольном устройстве (экране, мониторе, дисплее); основные действия, производимые специалистом при осмотре СВТ (порядок корректного приостановления работы и закрытия исполняемой операции или программы, выключения СВТ, отключения от источника электропитания, рассоединения (или соединения) СВТ, отсоединения проводов, результаты измерения технических параметров контрольно-измерительной или тестовой аппаратурой и т.п.).

Осмотр СВТ обычно приводит к необходимости их изъятия для последующего экспертного исследования и(или) приобщения к делу в качестве вещественного доказательства.

Здесь же следует отметить, что отличия в осмотре компьютерной системы, являющейся распределённой, даже в самом простом случае – корпоративной сети ЭВМ, которая включает рабочие станции сотрудников, серверы, в том числе почтовые серверы, прокси-серверы, серверы контроллеров доменов, маршрутизаторы, коммутаторы, кабельную систему. Элементы сети ЭВМ (кабельной и беспроводной, корпоративной или локальной сети и целые её сегменты) могут быть разнесены не только по разным помещениям в здании, но и по различным географическим регионам, например, если для организации сети используются технологии виртуальных (логических) каналов: *VLAN* (*от англ. Virtual Local Area Network* – виртуальная локально-вычислительная сеть), *MPLS* (*от англ. MultiProtocol Label Switching* – многопротокольная коммутация по меткам), *VPN* (*от англ. Virtual Private Network* – виртуальная частная сеть). Такая система может быть полностью программно определяемой (*англ. – Software Defined Everything: Network, Storage, Radio* и т. д.), трансграничной, облачной системой обработки информации, что представляет наибольшую трудность при организации и проведении осмотра, требует обязательного применения инструментальных средств и методов.

Замечание. Оставив за рамками настоящего описания процессуальные вопросы, что в таком случае считать местом осмотра, отметим очевидный факт, – границы места осмотра виртуально раздвигаются, предоставляя больше возможностей для поиска криминалистически значимой информации.

Сходная ситуация может возникнуть на месте происшествия в случаях, когда обнаруженные при осмотре цифровые устройства подключены к удаленным хранилищам информации, в том числе к облачным, либо в ходе осмотра помещения провайдера хостинговых услуг, предоставляющего в аренду вычислительные мощности, серверы которого физически размещены в ЦОД в различных регионах страны или зашифрованы [130].

В таких условиях многократно возрастает значение и квалификация специалиста, от него требуется уже не выполнение рутинных действий, а творческая вдумчивая работа на протяжении длительного времени, сопровождающаяся значительным психическим напряжением. Очевидно, что достижение результатов осмотра зависит от профессиональной и организационной подготовки специалиста и дознавателя (следователя), который вынужден самостоятельно выбирать тактические приемы осмотра места происшествия[85].

Учитывая огромный размер информации, хранящейся в локальной компьютерной сети [81], при её осмотре, например, в связи с проведенной сетевой атакой, тактически наиболее целесообразным движение по цифровым следам, оставленным в сети, начиная от выявленного цифрового устройства (телефона, компьютера), далее по цепочке других компьютеров и серверов до устройства, с которого началось проникновение, завершившееся получением НСД к системе.

Для поиска и документирования «цифровых следов» уместно применять не только криминалистический аппарат, но методы и стандарты[86] [87] [88] аудита информационной безопасности и технических мероприятий по реагированию на компьютерные инциденты[89], позволяющих выявлять различные информационные сущности и процессы в зависимости от типа осматриваемого объекта и имеющихся инструментальных средств: микропрограммное обеспечение и его настройки, процессы выполняемых программ; планировщики задач операционных систем ЭВМ; системные сервисы операционной системы; сетевой трафик; отдельные файлы; журналы регистрации событий операционной системы и программных систем мониторинга и защиты информации [131].

На основании собранных сведений формируется хронологическая последовательность событий в сети, связанных с получением несанкционированного доступа, и схемы развития сетевой атаки, затрагивающей различные элементы локальной сети. При составлении таких схем необходимо обязательно учитывать негативные обстоятельства[90], например изменения в файловой системе, ветках реестра, сведения из журналов событий, которые в силу своего наличия либо, напротив, отсутствия подтверждают или опровергают рассматриваемые гипотезы и следственные версии.

[85] См. *Коровин Н. К.* Тактические особенности следственного осмотра при расследовании неправомерного доступа к компьютерной информации. // Проблемы современной науки и образования, № 7 (89), 2017, С.92-94.

[86] ГОСТ Р ИСО/МЭК ТО 18044-2007. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. ISO/IEC TR 18044:2004 Information technology – Security techniques – Information security incident management (IDT). Дата введения 2008-07-01. Группа Т00. ОКС 01.040.01.

[87] ГОСТ Р ИСО/МЭК 27007-2014. Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности.

[88] проект ГОСТ Р «Управление инцидентами, связанными с безопасностью информации. Руководство по реагированию на инциденты в сфере информационных и компьютерных технологий. (ISO/IEC 27035-3:2020, NEQ)» URL: http://https://fstec.ru/en/component/attachments/download/3042 (дата обращения: 12.11.2022)

[89] РС БР ИББС-2.5-2014. Рекомендации в области стандартизации Банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности. Дата введения: 2014-06-01.

[90] См. *Белкин Р. С.* Курс криминалистики. 3-е изд., доп. – М.: ЮНИТИ-ДАНА, Закон и право, 2001. – С.796–799.

В случае невозможности изъятия средств вычислительной техники и изготовления посекторных копий их дисков вследствие большого размера или непрерывного производственного процесса следует рассмотреть следующие варианты сбора цифровых следов, имеющих значение для расследования уголовного дела:

1. Создание копии логического (а не физического) диска, если размер логического диска несопоставимо меньше неразмеченной области физического диска.[91]

2. Целевое копирование файлов, если известно, какие именно сведения представляют интерес и их расположение в файловой системе осматриваемого устройства.

3. Копирование файлов, содержащих в силу своего назначения достаточно сведений для анализа о возможной компрометации устройства, либо его использовании в противоправных целях.

Если по обстоятельствам дела необходимо производство судебной экспертизы всей компьютерной системы, изъятию подлежат взаимосвязанные объекты, включающие в себя аппаратное, программное и информационное обеспечение и являющиеся составными частями единого информационного технологического процесса.

2.3.1.2. Осмотр машинных носителей

Осмотр машинного носителя (МНИ) и компьютерной информации проводят по принципу «от общего к частному». Вначале описывают внешние индивидуальные признаки носителя: его цвет, размер, тип, вид, название, марка, заводской и индивидуальный номер, наличие наклейки и надписей на ней, наличие или отсутствие физических повреждений корпуса и следов на нём, положение элемента защиты от записи/стирания компьютерной информации. Затем переходят к осмотру компьютерной информации, содержащейся на МНИ.

Замечание. Для ОС Windows: копия (дамп) содержимого оперативной памяти; файл гибернации; страничный файл; ветви реестра операционной системы; журнальные файлы; файл $MFT (Master File Table); файл Prefetch; файл-листинг с хэш-суммами. Для ОС Linux это стандартный раздел (или файл) подкачки.

Если требуется по обстоятельствам дела копируются: файлы, содержащие копии веб-страниц, посещённых с помощью браузеров; файлы, содержащие историю посещения веб-страниц; архив электронной почты; настройки VPN; профили пользователей и т. п.[92]

Напомним, что перед началом осмотра необходимо указать в протоколе следственного действия: индивидуальные признаки используемого для осмотра средства электронно-вычислительной техники и основные реквизиты его программного обеспечения (тип, вид, марку, название, заводской или регистрационный номер, номер версии, юридический адрес и (или) автора программного продукта); юридические реквизиты программы, с помощью которой СВТ и его программное обеспечение в присутствии понятых было тестировано специалистом на предмет отсутствия вредоносных

[91] Например, с помощью системных программ fdisk в ОС Unix и ОС Windows, либо программы инженерного анализа из состава МКА-ИБИС [96] или иностранной специальной криминалистической программы – EnCase Forensic Imager и т.п.

[92] Имеются ввиду локальные копии, если же копирование данных сайтов идёт из сети, то подробнее об этом написано на стр. 98.

программно-аппаратных средств. После этого на указанный предмет проверяется и осматриваемая компьютерная информация.

Анализируя содержащуюся на осматриваемом носителе компьютерную информацию, надо установить сведения, имеющие отношение к расследуемому событию. Для оптимизации процесса осмотра большого объёма информации можно применять функции автоматизированного поиска по конкретному слову (реквизиту), входящие в состав стандартного программного обеспечения ЭВМ. Ход осмотра должен дополнительно фиксироваться на цветной фото- или видеокамере. При обнаружении следов преступления, необходимо сделать распечатку всей (как исключение, только для фото) или части компьютерной информации и приложить её к протоколу следственного действия с указанием в протоколе индивидуальных признаков использованного для этого печатающего устройства (тип, вид, марку, название, номер).

Замечание. В протоколе осмотра, помимо вышеуказанного, необходимо отразить: наличие, индивидуальные признаки защиты носителя от несанкционированного использования (голография, штрих-код, эмбоссинг, флуоресцирование, перфорация, ламинирование личной подписи и(или) фотографии владельца, их размеры, цвет, вид и т.п.); признаки материальной подделки МНИ и его защиты; внутреннюю спецификацию носителя – серийный номер и(или) метку тома, либо код, размер разметки (для дисков – по объёму записи информации, для лент – по продолжительности записи); размер области носителя свободной от записи и занятой под информацию; количество и номера сбойных зон, секторов, участков, кластеров, цилиндров; количество записанных программ, файлов, каталогов (структура их расположения на МНИ, название, имя и(или) расширение, размер (объём), в том числе тот, который занимают их названия, дата и время создания (или последнего изменения), а также специальная метка, флаг или тип, атрибуты (системный, архивный, скрытый, только для чтения или записи, и т.д., символическая ссылка, права пользователя, группы, списки доступа, контексты безопасности, зоны, уровни и т. п.); наличие скрытых или ранее стёртых файлов (программ) и их реквизиты (название, размер, временные метки (дата и время создания, доступа, изменения, модификации и (или) уничтожения)).

Разумеется, при собирании избыточных цифровых данных необходимо руководствоваться принципом разумности, отбор информационных объектов производить, исходя из предпосылок, что в них может содержаться криминалистически значимая информация.

Обнаруженные в ходе осмотра цифровые следы, которые характеризуются позволяющими их идентифицировать признаками: контрольной суммой (хэш-суммой), рассчитанной по криптографическому алгоритму, размером файла и другими его атрибутами, необходимо сохранить на электронных носителях информации.

Замечание. Сведения о рассчитанной хэш-сумме извлечённых данных и характерных признаках носителя информации, на который они были сохранены, вносятся в протокол. Также в протоколе должны полно и точно быть отражены ход и результаты проведённого осмотра и наименование применённых специалистом технических и программных средств.

Следует ещё раз подчеркнуть важность подготовительного этапа в проведении следственных действий по делам о компьютерных преступлениях. Формальный подход следователя к проверке необходимых компетенций у специалиста может привести к ситуации, при которой в отсутствие у последнего достаточных профессиональных знаний и навыков по работе с цифровыми следами будут упущены важные информационные объекты или не сохранены надлежащим образом цифровые следы преступле-

ния, что сделает непригодными такие доказательства для использования либо повлечёт их утрату.[93]

Расследуя неправомерный доступ к корпоративной компьютерной системе, как одну из версий следует рассматривать возможную причастность к преступлению сотрудника потерпевшей организации, а значит может потребоваться осмотр и изъятие записей с видеокамер наблюдения, исследование помещения, где размещены автоматизированные рабочие места, на предмет выявления признаков несанкционированного проникновения, поиск следов рук, оставленных сотрудниками, которым запрещён проход в осматриваемое помещение.

Замечание. Нельзя исключить из списка следственных версий и инсценировку применения вредоносных программ, когда сотрудники потерпевшей организации специально загружают в компьютерную систему вредоносное ПО, чтобы ввести следствие в заблуждение относительно истинных обстоятельств произошедшего и затруднить установление механизма и способа совершения компьютерного преступления.

В другом случае вредоносная программа может быть использована для сокрытия следов иного преступления, например налогового, когда, инсценируя сетевую атаку с использованием вредоносной программы – шифровальщика (иногда также называемой программой-«вымогателем»), преступники шифруют все данные, хранящиеся в компьютерной системе.

Помимо этого, для установления способа преступления и иных обстоятельств необходимо исследовать и изъять (или подготовить для последующей выемки – как отдельного процессуального мероприятия) документы, регламентирующие в компании процессы в сферах информационной безопасности и информационных технологий: правила разграничения доступа, политики информационной безопасности, инструкции по организации парольной защиты и т. д. Не помешает проверить автоматизированную систему доступа на объект (СКУД) и её журналы за несколько дней до произошедшего события.

В ходе выемки обязательно изымаются документы, необходимые для решения вопроса о нарушении правил эксплуатации ЭВМ:

- государственные контракты и/или договоры на оказание услуг, технического обслуживания и т. п. с техническими заданиями, регламентами, правилами и иными приложениями к ним;
- инструкции производителя по эксплуатации ЭВМ, системы или сети ЭВМ;
- правила работы на ЭВМ, установленные фирмой – собственником оборудования;
- журналы регистрации сбоев ЭВМ;
- журнал ремонта и профилактических осмотров компьютерного оборудования;
- материалы служебного расследования факта нарушения правил эксплуатации;
- приказ руководителя организации об отнесении сведений к разряду коммерческой тайны;
- приказ о назначении лица на должность; должностная инструкция работника; документы о соответствующей подготовке лица для работы с оборудованием;
- другие документы.

[93] Eoghan Casey. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press, 2011. – С. 228.

Весьма важно, чтобы следователь (дознаватель) осознавал, что из-за высокой волатильности[94] информации в компьютерных системах обнаружение цифровых следов преступления при повторном либо дополнительном осмотре по прошествии времени в большинстве случаев будет маловероятным. В отсутствие гарантий того, что компьютерные системы, изъятие которых невозможно по тем или иным причинам, будут оставаться выключенными в течение разумных сроков, цифровые данные из них должны быть извлечены в избыточном количестве. Хотя такой подход увеличивает нагрузку на специалистов и экспертов вследствие большего объёма данных, требующих исследования, его применение целесообразно, поскольку позволяет предотвратить потенциальную возможность утраты доказательств.

По окончании рабочего этапа осмотра места происшествия, осмотра СВТ (ЭВМ), сети ЭВМ или МНИ, оценки полноты и всесторонности его производства следователь составляет протокол, в котором, помимо прочего, подробно описывает действия специалиста, особенно если производилось исследование работающей компьютерной системы, сопровождающееся поиском и извлечением из неё цифровых следов, и примененное специалистом технико-криминалистическое и программное обеспечение.

Замечание. К протоколу должны прилагаться планы и схемы, например, план размещения средств вычислительной техники в помещениях либо схема локальной сети, а также, при их наличии, результаты применения средств технической фиксации хода следственного действия, которые могут быть представлены в виде фото и видеозаписей, файла-журнала использованных специалистом команд в исследуемой компьютерной системе и результатов их исполнения, сохранённого на электронный носитель информации, и т.п.

К упаковке электронных объектов, изъятых при осмотре места происшествия (средств вычислительной техники, электронных носителей информации и др.), необходимо отнестись с особой тщательностью в связи с тем, что возможное физическое повреждение может привести к утрате хранящихся на них цифровых следов. Следует исключить иные риски для сохранности изымаемых данных, например, разрушающее воздействие электромагнитного поля на определённые типы электронных носителей информации, такие как магнитные ленты (например, кассеты систем резервирования в серверных полках).

Современные средства вычислительной техники (смартфоны, планшеты, ноутбуки) используют различные технологии беспроводного обмена данными по радиоканалам, предоставляя пользователю альтернативу для подключения к сети интернет, например с помощью технологии Wi-Fi на основе стандартов IEEE 802.11 либо высокоскоростной передачи данных для мобильных телефонов, основанной на сетевых технологиях (GSM, UMTS, LTE, 4G, 5G и др.). При изъятии мобильных устройств с заблокированным экраном иногда бывает затруднительно определить, в каком состоянии они находятся – выключенном или энергосберегающем. В иных случаях выключение устройства может быть признано нецелесообразным, но при этом отсутствует возможность отключить адаптеры беспроводной связи, тогда устройства необходимо помещать в специальную изолирующую упаковку, чтобы исключить несанкционированное беспроводное подключение к ним посторонних лиц по протоколам удалённого управления и администрирования, в результате чего могут быть уничтожены или фальсифицированы цифровые следы.

[94] См. комментарий в сноске на стр. 6.

2.3.2. В ходе производства обыска

Тактика и особенности сбора и фиксации цифровых и вещественных доказательств по уголовным делам, связанным с информационными технологиями, в ходе производства обыска.

Тактические особенности производства обыска схожи с особенностями осмотра места происшествия, но имеют свою специфику. Кажущееся очевидным такое простое решение об изъятии без предварительного исследования обнаруженных в ходе обысков компьютеров или мобильных устройств, либо электронных носителей информации при определённых обстоятельствах приводит к утрате сведений, имеющих доказательственное значение, поскольку современные ноутбуки, планшеты, мобильные смартфоны и др. снабжены средствами защиты пользовательской информации, интегрированными производителями в свои продукты на программном или аппаратном уровнях. Помимо этого, преступники предпринимают меры к сокрытию следов преступления, устанавливая на используемое ими компьютерное оборудование программы для шифрования и уничтожения данных.

Одним из эффективных способов избежать утраты значимых для расследования сведений является осмотр работающих средств вычислительной техники, когда доступ к сохранённой на них информации не ограничен. В этом случае специалисту необходимо либо скопировать данные, относящиеся к делу, на отдельный накопитель информации либо обеспечить возможность повторного включения компьютерной техники без утраты хранящейся информации. Однако само наличие такой возможности зависит от подготовленности к производству обыска, от наличия детально разработанного плана следственного действия, предусматривающего возможные проблемные ситуации, прогнозирование таких ситуаций и рассмотрение вариантов их решений, а также от грамотной реализации разработанного плана.

Учитывая многообразие способов уничтожения либо шифрования данных, хранящихся в компьютерных системах и иных средствах вычислительной техники, а также изобретательность лиц, совершающих компьютерные преступления, что обусловлено их высоким образовательным уровнем, склонностью к нестандартному мышлению и творческим подходом к осуществляемой ими деятельности, трудно переоценить этап подготовки к проведению обыска.

В отличие от осмотра места происшествия обыск производится только по возбуждённому уголовному делу, проведение обыска по горячим следам по делам о компьютерных преступлениях – скорее исключение из правил, в связи с чем у следователя имеется возможность подготовиться должным образом к такому сложному следственному действию. Как и в случае с осмотром места происшествия необходимо заранее подобрать[95] специалиста, обладающего необходимыми компетенциями и совместно с ним разработать план обыска.

Готовясь к проведению обыска, следователь должен решить что и где он будет искать. Для этого необходимо тщательно изучить обстоятельства дела и собрать ориенти-

[95] К сожалению, на хороших специалистов существует кадровый голод, поэтому зачастую следователи, при наличии выбора, выбирают себе тех специалистов в глубине и широте профессиональных знаний которых они уверены, отказываясь сотрудничать с другими.

рующую информацию о предмете обыска, месте его проведения и личности обыскиваемого. По делам о преступлениях в сфере компьютерной информации предметом обыска могут быть не только разнообразные СВТ, машинные носители и содержащаяся на них компьютерная информация, но и документы, средства электросвязи, разработанные и приспособленные специальные технические устройства, бытовые электротехнические устройства и оборудование, материалы и инструменты.

Для составления плана следует предварительно собрать максимально полную информацию о месте производства обыска и находящемся там компьютерном оборудовании, о личности подозреваемого, используемых им средствах вычислительной техники, образе его жизни, графике бодрствования и сна, о времени, которое он проводит за компьютером и т. д.

Замечание. Значимую информацию можно получить путём проведения оперативно-разыскных мероприятий; из показаний лиц из окружения подозреваемого, сотрудничающих со следствием; посредством изучения статистических данных сетевых подключений, предоставленных провайдером, оказывающим подозреваемому услуги доступа в сеть интернет и/или оператором сотовой связи.

Проведение подготовительных мероприятий позволяет исключить ошибки, связанные с неправильным установлением места проведения обыска (например, когда квартира была установлена по выделенному для её владельца IP-адресу, а преступная деятельность осуществляется из соседнего помещения вследствие компрометации беспроводной точки доступа), а также минимизировать вредные последствия от несвоевременности производства обыска, когда подозреваемый отдыхает, средства вычислительной техники выключены, а вся хранящаяся в них информация надёжно зашифрована.

При проведении обыска в офисе, где преступную деятельность осуществляет группа лиц, следует выяснить планировку помещений, расположение рабочих мест, средств вычислительной техники, вспомогательного оборудования, необходимость привлечения дополнительно специалистов. После изучения собранной информации следователю надлежит убедиться в наличии специальных технико-криминалистических средств и программного обеспечения для предварительного исследования компьютерных устройств и цифровых следов с учётом возможного оказания подозреваемым противодействия, иного оборудования для поиска, обнаружения, копирования и фиксации компьютерной информации, в том числе электронных носителей для хранения на них цифровых следов либо изготовления побитовых копий дисков, а также кабелей, переходников, набора инструментов для разборки технического оборудования, упаковочного материала.

При проведении обыска по делам о компьютерных преступлениях крайне важно обеспечить своевременность и внезапность проникновения следственной группы в обыскиваемое помещение, что обусловлено той лёгкостью, с которой подозреваемый может уничтожить цифровые следы, имеющие криминалистическое значение.[96]

Главная задача на этом этапе – получить доступ к средствам вычислительной техники, находящимся во включённом состоянии, с подключенными внешними носителями информации. Затем, не сбавляя темпа, необходимо отстранить подозреваемого и

[96] При уничтожении физических доказательств «смыть» несколько килограмм порошка в канализацию или «прожевать» через бумагоуничтожитель несколько томов документов явно сложнее и дольше, чем несколько нажатий на кнопки.

иных лиц, находящихся в помещении, от компьютеров, силовых кабелей, электрических розеток и исключить их несанкционированное передвижение по помещению.

Грамотное использование следователем фактора внезапности, который, как правило, влечёт кратковременное психопатологическое состояние растерянности у подозреваемого, может помочь склонить последнего к сотрудничеству со следствием. В этом случае следует получить от подозреваемого и зафиксировать в протоколе реквизиты доступа к локальным учётным записям и аккаунтам на внешних ресурсах, пароли для разблокирования мобильных устройств, данные для доступа к зашифрованным дискам и т. п.

Вместе с тем, независимо от готовности подозреваемого сотрудничать со следствием, специалисту следует незамедлительно после проникновения в помещение начать работу по осмотру и предварительному исследованию средств вычислительной техники. В первую очередь необходимо используя различные способы исключить переход в режим энергосбережения или блокировки работающих компьютеров и мобильных устройств, например, путём периодического движения компьютерной мышью. Одновременно посредством фотосъёмки либо видеозаписи следует запечатлеть содержимое экранов компьютеров, тем самым возможно зафиксировать факт использования средств вычислительной техники (и программного обеспечения) в преступных целях на случай внезапного выключения питания и утраты возможностей для поиска цифровых следов преступления.

Крайне важная для расследования информация – машинный код, данные о сетевых подключениях, активных процессах, вычисленных хэш-функциях паролей, введённых пользователем как для локальных файловых томов, например, для подключения зашифрованной области диска, так и для авторизации на удалённых ресурсах и т. п., хранятся в энергозависимой оперативной памяти компьютера. Сведения, которые могут быть получены в результате исследования содержимого оперативной памяти, иными способами зачастую добыть невозможно, однако при этом они характеризуются высокой волатильностью[97] и уничтожаются при выключении питания. Для последующего поиска цифровых следов преступления в содержимом оперативного запоминающего устройства (ОЗУ) следует создать его копию с помощью специальной криминалистической программы, сохранённой на отдельном внешнем электронном носителе информации. Содержимое ОЗУ копируется в работающей системе путём подключения к ней электронного носителя со специальной программой. Извлечённые таким образом цифровые следы сохраняются на этом же, либо ином внешнем диске, который изымается и приобщается к протоколу следственного действия.

Исходя из конкретных обстоятельств дела и с учётом ранее собранных на этапе подготовки к обыску сведений о возможных средствах и методах, которые могут быть применены обыскиваемым для уничтожения цифровых следов преступления, перед копированием содержимого ОЗУ целесообразно произвести осмотр компьютерной информации, обрабатываемой компьютерной системой. Например, для противодействия следствию подозреваемый может настроить запуск программы уничтожения данных либо просто выключение компьютера на событие операционной системы – изменение аппаратного окружения. В этом случае при подключении внешнего электронного носителя с программой для снятия копии содержимого ОЗУ будет выполнено запрограммированное действие.

[97] См. комментарий в сноске на стр. 6.

Для выявления признаков, свидетельствующих о наличии в системе криминалистически значимых сведений, которые могут быть утрачены в результате противодействия подозреваемого, следует:

- провести поиск на предмет обнаружения программ, обеспечивающих шифрование файлов; программ для создания и использования шифруемых областей цифровых данных (криптоконтейнеров); программ, обеспечивающих функционирование виртуальных машин; программ-менеджеров паролей; программ-клиентов мгновенного обмена сообщениями, поддерживающих шифрование трафика; программ для написания приложений – среды разработки; специфических утилит (программ-спамеров и т. п.);
- изучить файловую систему с целью исследования логической структуры дисков на предмет выявления неразмеченной области большого размера и обнаружения файлов больших размеров, возможно являющихся криптоконтейнерами;
- исследовать запущенные на компьютере процессы, изучить аппаратное и сетевое окружение, проверить на наличие подключений к удалённым сетевым ресурсам, в том числе облачным хранилищам и т. п.

Информация, выводимая на монитор в ходе предварительного исследования компьютерной системы, должна быть зафиксирована посредством фотосъёмки либо видеозаписи.

В отсутствие уверенности, что после выключения средств вычислительной техники данные на них не будут зашифрованы либо доступ к ним не будет ограничен иными способами, необходимо скопировать все значимые для расследования данные на специально приготовленный электронный носитель информации. Такими сведениями могут быть архив электронной почты, контактные листы программ-клиентов обмена сообщениями, история переписки, исходные коды, среда разработки и скомпилированные образцы программного обеспечения, данные о доступе к серверам, веб-ресурсам и другой сетевой инфраструктуре, файлы, содержащие копии веб-страниц, посещённых с помощью браузеров, файлы, содержащие историю посещения веб-страниц, настройки VPN, профили пользователей, отсканированные изображения финансовых и регистрационных документов и т. п.

Кроме этого, обязательно следует скопировать файлы из доступных криптоконтейнеров в локальной системе, а при наличии активных подключений к сетевым ресурсам, в том числе облачным хранилищам, произвести удалённое копирование данных на внешний носитель информации, который приобщить к протоколу обыска.

Если непосредственное подключение через USB-интерфейс носителя информации к осматриваемой системе невозможно, в том числе из соображений обеспечения сохранности цифровых следов, следует рассмотреть иные способы для извлечения и сохранения криминалистически значимой информации, например, посредством копирования данных на сетевой диск с использованием протокола NFS, CIFS (SMB) и др.

При изъятии выключенной компьютерной системы, когда изучить её конфигурацию, аппаратное окружение и подключенные диски не представляется возможным, обыскиваемое помещение необходимо тщательно осмотреть и при необходимости исследовать с помощью специальной аппаратуры с целью проверки, не использует ли подозреваемый удалённые сетевые диски, которые физически могут быть скрыты в стенах, нишах мебельных гарнитуров, в подсобных помещениях.

Действия специалиста, направленные на осмотр и предварительное исследование средств вычислительной техники, извлечение и сохранение на внешний носитель информации цифровых данных, а также иные манипуляции, совершённые с целью поиска цифровых следов преступления, должны быть детально описаны в протоколе обыска, по возможности, запечатлены с помощью фотосъёмки либо видеозаписи или зарегистрированы иными средствами фиксации хода и результатов следственного действия. Использованные в ходе обыска специальные технические и программные средства должны быть указаны в протоколе. В протоколе обыска также подлежат фиксации действия подозреваемого, направленные на противодействие следственной группе, например, попытки уничтожить цифровые данные, обесточить средства вычислительной техники, заблокировать мобильное устройство.

Все компьютерные устройства, накопители информации и другие предметы, изъятые согласно протоколу обыска, должны быть соответствующим образом упакованы, чтобы исключить риски уничтожения либо повреждения цифровых следов и предотвратить несанкционированное удалённое подключение к ним с использованием сети интернет, о возможностях которого было упомянуто выше.

В ходе обыска следует обращать внимание на литературу, методические материалы и рекламные проспекты по компьютерной технике, обработке, защите, передаче и негласному получению компьютерной информации, а также на аудио-, видеокассеты, распечатки машинной информации и документы о соответствующем образовании.[98] Особое внимание нужно уделять предметам, содержащим коды, пароли доступа, идентификационные номера, названия, электронные адреса пользователей конкретных компьютерных систем и сетей, алгоритмы входа и работы в системах и сетях. Необходимо также перлюстрировать записные (телефонные) книжки, справочники и каталоги, в том числе электронные, находящиеся в памяти телефонных аппаратов, пейджеров и других компьютерных устройств.

Ценные доказательства могут быть обнаружены и при личных обысках подозреваемых (обвиняемых).

2.3.3. В ходе производства выемки

Тактика и особенности сбора и фиксации цифровых и вещественных доказательств по уголовным делам, связанным с информационными технологиями, в ходе производства выемки.

Выемка средств вычислительной техники и электронных носителей информации требует несколько меньше организационных усилий чем обыск. В большинстве случаев допущенные при её проведении ошибки технического характера не являются существенными. Тем не менее подготовительные мероприятия необходимы и заключаются в привлечении к производству следственного действия компетентного специалиста в соответствии с требованиями ч. 2 ст. 164.1 УПК РФ. Заметим, что участие специалиста при производстве выемки не должно носить формальный характер. При выемке средств вычислительной техники специалист может проверить их работоспособность, уточнить особенности функционирования, оказать содействие следователю в составлении протокола при описании технических аспектов.

[98] В том числе, сертификаты курсов повышения квалификации и т.п.

Предметом выемки по уголовным делам о преступлениях в сфере компьютерной информации, в подавляющем большинстве случаев, являются персональные компьютеры, машинные носители информации (включая распечатки на бумаге, аудио- и видеокассеты, пластиковые карты) и всевозможные документы (в том числе и электронные)[99], отражающие и регламентирующие различные операции (технологические процессы) использования ЭВМ, системы ЭВМ и их сети связанные с обработкой, накоплением, созданием, передачей и защитой компьютерной информации. Указанные предметы обычно, как правило, находятся по месту работы (учёбы) подозреваемого (обвиняемого), в рабочих кабинетах должностных лиц и других служебных (учебных) помещениях.

Помимо перечисленных предметов, также могут встречаться и быть изъяты специальные технические средства для получения, модификации и уничтожения информации, свободные образцы почерка, бланки и фрагменты документов, заготовки машинных носителей информации, исходные тексты программ для ЭВМ, черновики и иные образцы для сравнительного исследования.

Журнальные файлы доступа к ресурсам и копии содержимого серверов либо облачных хранилищ информации предоставляются провайдерами соответствующих услуг на электронных носителях информации, изъятие которых целесообразно производить в рамках выемки. Также в рамках выемки изымаются имеющие криминалистическое значение результаты внутреннего расследования, проведённого службой информационной безопасности пострадавшей организации. При выемке электронных носителей информации, содержащих криминалистически значимую информацию следует убедиться в её наличии, доступности на изымаемом диске и отразить тип и признаки изымаемой информации в протоколе.

Также в ходе выемки, как правило, изымаются и по протоколу выемки приобщаются к уголовному делу материалы и документы, сведения о которых получены ранее в ходе осмотра, обыска, проведения оперативно-разыскных мероприятий, показаний потерпевших и свидетелей или установлены путём переписки (запросов) следователя (дознавателя) или из анализа ранее приобщённых к делу доказательств.

Замечание. В случае когда уголовное дело возбуждается на основе заявления или сообщения полученного из СМИ или с технических материалов об обнаружении, предупреждении или ликвидации последствий компьютерных атак, либо актов (протоколов) аудита информационной безопасности в организации, либо результатов контроля эффективности защиты информации (или контрольно-технических мероприятий по оценке защищённости информации), содержащих объективные данные о признаках неправомерного доступа, применения вредоносного программного обеспечения или нарушения правил эксплуатации ЭВМ, сети ЭВМ или обеспечения безопасности объектов критической информационной инфраструктуры, такие материалы подлежат процедуре выемки (протокол выемки) и последующему осмотру с участием специалиста (протокол осмотра) для полноценного приобщения к уголовному делу и возможности использования в качестве доказательств по уголовному делу.

Если изымаемые МНИ являются накопителями на принципах магнитной записи (дискеты, ленты, жёсткие диски, магнито-оптика и др), то они должны быть в обязательном порядке упакованы в алюминиевый материал (алюминиевую фольгу или специальный контейнер), предохраняющий МНИ и их содержимое от внешнего электромагнитного и магнитного воздействия.

[99] Электронный документ – документ, в котором информация представлена в электронно-цифровой форме (см.: Об электронной цифровой подписи: Федеральный закон от 10.01.2002 г. № 1-ФЗ. Ст.3).

2.3.4. В ходе производства следственного эксперимента

Тактика и особенности сбора и фиксации цифровых и вещественных доказательств по уголовным делам, связанным с информационными технологиями, в ходе производства следственного эксперимента.

Отдельно в ряду следственных действий при расследовании компьютерных преступлений стоит следственный эксперимент. Его целью в большинстве случаев является установление возможностей использования определённых информационно-коммуникационных технологий, средств вычислительной техники, программного обеспечения, сетевых ресурсов и сервисов для осуществления данного способа преступления, деталей механизма преступного события.

Например, в процессе эксперимента может быть установлен факт взаимодействия вредоносной программы-бота с сервером управления, подтверждающий версию следствия, что проверяемые части программного обеспечения являются единым программным комплексом, разработанным с применением сетевой архитектуры «клиент-сервер». В другом случае с помощью следственного эксперимента может быть установлена фальсификация представленной в свою защиту подозреваемым электронной переписки, которая, якобы, была сохранена в результате резервного копирования в облачном хранилище данных.

К проведению эксперимента с использованием информационно-коммуникационных технологий, как и в случае с другими невербальными следственными действиями, в рамках которых подразумевается работа с «цифровыми следами», в обязательном порядке следует привлекать специалиста. Опытные действия с применением компьютерных устройств могут осуществляться как специалистом, так и непосредственно лицом, действия которого проверяются.

Если проверяются действия, производимые подозреваемым, предпочтительно, чтобы он лично демонстрировал их участникам следственного действия.

Замечание. Недопустимо, чтобы в опытных мероприятиях использовались изъятые по делу средства вычислительной техники и носители информации, так как это приведёт к модификации хранящихся на них цифровых следов. Для этих целей следует использовать аналогичное оборудование, возможности которого достаточны для проверки соответствующих фактов.

Помимо детального документирования проводимого опытного мероприятия в протоколе следственного действия, ход и результаты эксперимента могут быть зафиксированы посредством фотосъёмки и видеозаписи, с помощью журналирования действий в компьютерной системе, сохранения результатов эксперимента в файл, записи экрана и т. п.

Если в ходе следственного эксперимента получены новые данные, представленные в виде цифровых следов, они должны быть сохранены специалистом на специально приготовленном для этих целей электронном носителе информации. Идентифицирующие признаки полученных данных (хэш-сумма, размер и т. п.) следует внести в протокол, а электронный носитель приобщить к протоколу следственного эксперимента.

2.3.5. Особенности «облачных» систем

Особенности производства следственного осмотра (содержимого) удалённых («облачных») систем хранения, серверов и электронных носителей информации (на примере социальных сетей и мессенджеров).

Процедура фиксации и изъятия цифровых данных из «облачных» объектов, таких как социальные сети, мессенджеры и т.п. заслуживает отдельного внимания.

В гражданском праве и процессах имеются теоретические разработки и практика к организационно-правовому обеспечению фиксации цифровой информации, находящейся в сети интернет[100]. Вместе с тем, в арбитражном процессе определён статус «скриншотов», вместе с требованиями к их фиксации, что находит отражение в судебной практике.[101] Анализ судебной практики показывает[102], что устоявшимся механизмом обеспечения представляемых доказательств, полученных из сети интернет, является обращение одной из участвующих в деле сторон к нотариусу с целью проведения осмотра сайта в соответствии со статьями №№ 102–103 Основ законодательства о нотариате[103], и последующей фиксации цифровых данных, находящихся в сети интернет (так называемый «заверенный снимок экрана»).

Следует сказать о том, что в отношении специфики фиксации и изъятия цифровых данных – речевых продуктов, находящихся в цифровой среде, рядом авторов предпринимались попытки разрешения проблем, возникающих на практике, связанных с обеспечением достоверности зафиксированных на материальный носитель информации цифровых данных.[104] Однако единый унифицированный подход к фиксации и изъятию таких доказательств в уголовном процессе отсутствует.[105] В этой связи представляется целесообразным рассмотреть особенности фиксации и изъятия цифровых данных из страниц пользователей социальных сетей и мессенджеров в целях обеспечения их достоверности и возможности приобщения к вещественным доказательствам.

Как отмечает А. И. Семикаленова[106], цифровые следы несут в себе значимую для следствия информацию, которую можно разделить на основную, выражающуюся в виде звука, изображения, текста, рисунка и дополнительную – позволяющую судить о

[100] См. *Танимов О. В., Кудашкин Я. В.* О правовой природе и возможности правового регулирования отношений в сети Интернет // Информационное право. № 2. – 2012. – С. 17 – 21; *Бабкин С. А.* Право, применимое к отношениям, возникающим при использовании сети Интернет: основные проблемы. – М.: Центр ЮрИнфоР, 2003. – 68 с.

[101] Информационное письмо Президиума ВАС РФ от 7 июля 2004 г. № 78 «Обзор практики применения арбитражными судами предварительных обеспечительных мер» // Вестник ВАС РФ. – 2004. – № 8.

[102] См., например: Решение Арбитражного суда Саратовской области от 4 марта 2019 г. по делу № А57-15203/2018; Постановление Арбитражного суда Хабаровского края от 5 августа 2013 г. по делу № А73-14263/2012; Решение Арбитражного суда Курской области от 29 мая 2018 г. по делу № А35-5996/2017 [Электронный ресурс]. – Режим доступа: https://sudact.ru/. (Дата обращения: 21.07.2020).

[103] «Основы законодательства Российской Федерации о нотариате» (утв. ВС РФ 11.02.1993 № 4462-1), (ред. от 25.08.2021) // СПС «Консультант Плюс».

[104] См. *Никишин В. Д.* Особенности назначения судебной экспертизы материалов религиозного характера экстремистско-террористической направленности и оценки её результатов // Законы России: опыт, анализ, практика. № 4, 2019. – С. 95-101; *Никишин В. Д.* Цифровые и речевые следы в аспекте обеспечения информационной (мировоззренческой) безопасности в интернет-среде // Судебная экспертиза. № 1 (61), 2020. – С. 131-139.

[105] На момент написания данного учебного пособия.

[106] См. *Семикаленова А. И.* Цифровые следы: назначение и производство экспертиз // Вестник Университета имени О.Е. Кутафина. № 5, 2019. – С. 113-115.

способе и времени создания, распространения и редактирования основной информации. Исходя из этого, остановимся подробно на каждой из особенностей процедуры фиксации и изъятия цифровых данных, содержащихся на страницах пользователей в социальных сетях и мессенджерах.

Основополагающим фактором при работе с цифровыми данными выступает оперативность действий со стороны правоприменителя, связанная с фиксаций криминалистически значимой информации, интересующей следствие, после её обнаружения. Обусловлено это тем, что любой контент сайта поддерживается при помощи электронно-вычислительных мощностей, на которых хранится вся цифровая информация, отображающаяся на определённом контент-сайте (странице пользователя социальной сети), содержимое памяти которых, как было отмечено ранее, может быть крайне изменчивым во времени.

Риск утраты криминалистически значимой информации, содержащейся на определённом контенте, заключается в том, что, с одной стороны, сервер[107], при помощи которого поддерживается определённый контент-сайт, может быть уничтожен злоумышленниками или подвержен полному/частичному удалению с него информации, представляющей интерес для правоохранительных органов, вследствие чего воспроизводимость информации на контенте окажется в последующем невозможной, что будет означать безвозвратную утрату криминалистически значимой информации. Например, на сайте «Y» в течение суток содержались противозаконные и непристойные изображения «X», которые через время были удалены лицом, имеющим доступ к контенту сайта на правах администратора или загрузившим их пользователем. То, что они удалены сейчас (нарушения в данный момент нет), не означает что их не успели просмотреть/сохранить к себе другие пользователи и что нарушения не было в прошлом. Таким образом, если не осуществить оперативно фиксацию и изъятие интересующих следствия данных на облачных или сетевых ресурсах (сайтах), то в результате таких действий к моменту изъятия цифровых данных они могут уже быть подвергнуты удалению/изменению и, как следствие, не содержать криминалистически значимой информации, представляющей интерес для правоохранительных органов.

Исходя из вышеизложенного очевидно, что в зависимости от того, насколько оперативно правоприменителем будут предприняты действия по фиксации и изъятию криминалистически значимой информации с контента сайта в сети интернет, напрямую будет зависеть сохранность цифровых данных и дальнейшая возможность их приобщения к материалам дела в качестве вещественных доказательств.

Для эффективной работы в этом направлении видится целесообразным создание автоматизированных рабочих мест следователя или оперативного работника, являющихся терминалами к некоторой государственной системе регистрации и хранения цифровых данных, в том числе и улик.

Указанная система могла бы состоять из трёх компонентов: множества АРМ оперативного назначения (*frontend*'а, – см. параграф «*Применение автоматизированных рабочих мест*»на стр.102), хранилища (например, государственного) и модуля обращения («паука» – в терминологии поисковых систем), т. е. *backend*'а. При этом можно было бы сделать указанный сервис полезным не только для правоохранительных органов, но и для других целей. Например, как зарубежный сервис сайта «archive.org»,

[107] Аппаратный комплекс, настроенный на хранение данных или непрерывное решение определённых задач.

сохраняющий в истории содержимое множества web-страниц и предоставляющий их в общий доступ анонимно, без регистрации.

Подход по фиксации наблюдаемой информации на сетевых ресурсах в максимально короткие сроки в равной степени относится и к фиксации и изъятию цифровых данных, находящихся на электронных мобильных устройствах (мобильных телефонах, электронных планшетах и др.), так как в противном случае также велик риск утраты криминалистически значимой информации. Это связано с тем, что на электронных носителях информации зачастую содержится потенциально доказательственно релевантная информация, имеющая значение для расследования и раскрытия преступлений, которая в большинстве случаев бывает размещена и опубликована в закрытых группах в социальных сетях, блогах, пабликах, мессенджерах и т. д., в результате чего к данной информации имеет доступ ограниченный круг лиц.

Исходя из сказанного выше следует, что для того, чтобы получить доступ к криминалистически значимой информации, которая, например, опубликована в закрытых группах в социальных сетях, необходимо подписаться на определённую группу в конкретной социальной сети. В дальнейшем для получения доступа к информации закрытой группы необходимо одобрение администратора группы (Вконтакте, Одноклассники, Facebook и др.). Аналогичный порядок действий необходимо произвести и для получения доступа к информации в закрытых чатах мессенджеров (WhatsApp, Viber, Telegram). Однако, как и в социальных сетях, так и в мессенджерах далеко не во всех случаях возможно получение криминалистически значимой информации соответствующим способом.

Такие сложности возникают во многом из-за того, что, например, преступные экстремистские/террористические группировки, представляют собой закрытую субкультуру, внедрение в которую зачастую оказывается крайне сложным для сотрудников правоохранительных органов. Таким образом, может возникнуть необходимость в фиксации и изъятии цифровых данных, содержащихся на электронном носителе информации (мобильном телефоне, электронном планшете и др.). При этом важно понимать, что не всегда удаётся изъять и зафиксировать всю необходимую криминалистически значимую информацию, интересующую следствие, с электронного носителя информации.

В некоторых случаях цифровые следы могут содержаться только в «облачном» хранилище. Такое положение дел означает, что криминалистически значимая информация не имеет резервной копии на самом электронном устройстве, следовательно, её получение в этом случае возможно посредством авторизации через аккаунт пользователя электронного устройства (подозреваемого/обвиняемого) и последующей фиксации. Если цифровая информация выражена в виде письменных продуктов речевой деятельности, то по аналогии с утвердившейся практикой фиксации доказательств в гражданском праве и административных процессах, представляется целесообразным осуществлять снятие снимков образов экрана электронного устройства (мобильного телефона, ноутбука, электронного планшета и т. д.) используя имеющиеся функциональные возможности устройства («скриншоты»), либо применять внешнюю фото- или видеофиксацию. Однако при этом следует учитывать, что снимки образов экрана сделанные на устройствах отражают более качественно информацию, содержащуюся на сайте, чем внешние видео-, фотоснимки экрана электронного устройства, для которых

неизбежен «муаровый узор» и блики, которые могут привести к частичной утрате, фиксируемой криминалистически значимой информации.

Если осуществляется фиксация и изъятие аудио-/видеофайлов с содержимого сайтов (страниц пользователей социальных сетей), то целесообразно проводить трассировку[108], так как в результате таких действий представляется возможным отследить путь доступа от сервера, при помощи которого осуществлялся вход в информационно-коммуникационную сеть следователем, до сервера, на котором расположен осматриваемый информационный ресурс (контент сайта). Результаты трассировки, приобщаемые к протоколу осмотра, позволяют с достаточной вероятностью[109] верифицировать факт соединения сервера, используемого в ходе следственного осмотра, с контентом конкретного осматриваемого сайта, а также подтвердить отсутствие постороннего информационного влияния при осуществлении фиксации и изъятия текстовых, аудио-/видеофайлов, находящихся на странице пользователя, в частности, если подлежащие изъятию файлы, расположены в облачном хранилище, интересующего следствие идентификатора ID. Наряду с этим, данная процедура позволит также удостоверить факт, что в браузере были отображены страницы подлинного сайта, с которого была скопирована информация.

Отметим также, что относительно недавно для пользователей большинства социальных сетей и мессенджеров появилась функция, позволяющая проводить операцию по удалению письменного, аудио-/видеосообщения у другого(-их) пользователей. При этом одни из них устанавливают временные ограничения для выполнения данной операции (Вконтакте, WhatsApp, Viber), другие, напротив, не предусматривают таких ограничений (Telegram). В результате проведения соответствующих операций исходные текстовые или аудио-/видеосообщения, в которых, например, содержалась криминалистически значимая информация, не подлежит восстановлению, вследствие чего может произойти утрата криминалистически значимой информации, если не осуществить незамедлительно фиксацию и изъятие соответствующих цифровых данных.

Следует также учитывать, что, если у посторонних лиц имеются данные о реквизитах пользователя (логин и пароль) подозреваемого/обвиняемого в социальной сети (Вконтакте, Facebook, Одноклассники), то при помощи сети интернет возможно подключение к соответствующему профилю со стороны третьих лиц, которыми могут быть предприняты действия по удалению криминалистически значимой информации, находящейся в облачном хранилище.

Ещё одной не менее важной проблемой при получении информации с электронных устройств является возможность удалённого подключения к электронному устройству (смартфону, планшету) со стороны посторонних лиц. Как справедливо отмечают исследователи, «при изъятии автономных устройств (ноутбуков, смартфонов), экран которых заблокирован, но сами они находятся во включенном состоянии. При наличии доступа к сети интернет, например, по стандартам передачи данных в сото-

[108] Произвести трассировку маршрута до сервера с сайтом можно с использованием утилит «traceroute» или «tracert» из командной строки (в зависимости от используемой операционной системы) или с помощью любого их аналога.

[109] Вероятностность связана с относительной длительностью работы указанных утилит (секунды в сравнении со скоростями передачи 100/1000/10000 МБит/с), особенностями работы сетевой модели TCP/IP и непредсказуемо и быстро меняющейся маршрутизацией в сети интернет, которая на практике может отличаться в один и тот же момент времени для пакетов и дейтаграмм различных протоколов: ICMP, UDP, HTTP, HTTPS, используя которые работают утилиты трассировки и веб-сайты.

вых сетях, возможно удалённое подключение к ним посторонних лиц и внесение изменений в хранящуюся на них компьютерную информацию».[110]

Таким образом, оперативность в действиях дознавателя или следователя с момента обнаружения цифровых данных до момента их фиксации напрямую предопределяет сохранность криминалистически значимой информации, содержащейся на контенте сайта или на электронном устройстве подозреваемого/обвиняемого, потерпевшего.

Проблемы собирания цифровых доказательств из социальных сетей и мессенджеров, с одной стороны, связаны с отсутствием норм международного права, регулирующих вопросы взаимодействия между государствами в сфере противодействия информационной преступности, что на практике зачастую приводит органы следствия к невозможности сбора цифровых доказательств из социальных сетей и мессенджеров, представителями которых являются юридические лица, зарегистрированные в иностранных государствах (Facebook, Twitter, WhatsApp и др.). С другой стороны, стоит согласиться с Е. Р. Россинской и В. В. Крыловым, что теория информационно-компьютерного обеспечения криминалистической деятельности в России с 1991 г. находится пока на стадии своего формирования и развития [81], в связи с чем криминалистические технологии собирания (обнаружения, фиксации, изъятия) цифровых доказательств хоть и формализованы в 1996 г. [58], но не получили единого теоретического обобщения и систематизации, что, как следствие, приводит на практике к отсутствию единства в подходе к собиранию цифровых доказательств в новой антропогенной среде из социальных сетей и мессенджеров техногенной сферы.

Использование подхода по сохранению трафика на стороне провайдера[111] теоретически решает проблему фиксации передаваемого содержимого, однако специфика пакетной передачи данных по стеку протоколов «TCP/IP», использования шифрования, в том числе и на ключах сертификатов выданных зарубежными удостоверяющими центрами, многоуровневая вложенность данных делают на практике фиксацию передаваемого контента по сохранённому сетевому трафику на стороне провайдеров и использования данных материалов в судебной практике неосуществимой на сегодняшний день.

2.4. Документирование

Документирование доказательной базы, собранной в цифровом виде.

Общие криминалистические рекомендации по изъятию и фиксации доказательств содержат требования фиксировать в протоколе индивидуальные признаки, изъятых устройств и электронных носителей информации (размер, форму, номер и т. д.), позво-

[110] См. *Чекунов И. Г., Рядовский И. А., Пузарин А. В., Русскевич Е. А.* [и др.]. Методические рекомендации по расследованию преступлений в сфере компьютерной информации: учебное пособие, 2-е изд. – М.: Московский университет МВД России имени В. Я. Кикотя, 2019 г. – С. 195.

[111] «Закон Яровой», он же Федеральный закон от 6 июля 2016 г. № 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» обязывает операторов связи хранить звонки, сообщения и интернет-трафик пользователей (абонентов) за период, определяемый Правительством Российской Федерации (но не более, чем за 6 месяцев) в соответствии с 64-й статьёй федерального закона «О связи», а информацию о фактах приёма, передачи, доставки и обработки сообщений и звонков – 3 года. Следует отметить, что зарубежное законодательство в этом отношении более строгое, а сроки и объёмы хранения больше.

ляющие идентифицировать их и хранящуюся на них информацию; предъявляют требования к обеспечению их сохранности, механической целостности. Однако, как справедливо отмечает сводный коллектив авторов из АО «Лаборатория Касперского», Академии управления и Московского университета МВД России им. В.Я. Кикотя «Такие общие требования по отношению к компьютерной информации нельзя признать достаточными для обеспечения её сохранности и дальнейшей идентификации» [74].

Несмотря на то, что с процессуальной точки зрения доказательством будет протокол следственного действия и электронный носитель информации, на который копируется криминалистически значимая информация, содержащаяся на оригинале (содержимое сайта, файлы мобильного телефона, электронного планшета), наряду с этим также ещё необходимо верифицировать, зафиксированную на электронном носителе (CD-диске, USB-накопителе) информацию.

Верифицировать цифровые данные, полученные из социальных сетей или мессенджеров, вне зависимости от типа файла (текстовый, графический, аудио-/видео-) и их расширений (txt, docx, pdf, jpg, png, mp3, mp4, mkv, avi) возможно с помощью вычисления контрольной суммы (как правило, криптографической контрольной суммы – хэш-суммы[112]) файла по определённому алгоритму (хэш-значения по ГОСТ Р 34.11-2012, MD5, SHA-1, SHA-2[113] или электронная подпись ГОСТ Р 34.10.-2012). Именно с помощью хэш-суммы на любом из этапов расследования преступления становится возможным подтвердить идентичность изъятой и зафиксированной на электронном носителе информации. При этом сведения о хэш-сумме изъятого файла, должны быть занесены в протокол следственного действия. Необходимость в производстве расчёта контрольной суммы файла при фиксации и изъятии цифровых следов обусловливается тем, что:

- во-первых, исключается возможность внесения изменений в первоначальное содержание файла (снимков образов экрана, аудио-/видеофайлов). Так в случае, если, например, файл будет смонтирован при помощи современных программ обработки изображений (GIMP, Adobe Photoshop, PhotoEditor и др.), то хэш-сумма файла будет отличной от той, которая зафиксирована в протоколе следственного действия, что будет свидетельствовать о внесении каких-либо изменений в файл, содержащейся на электронном носителе информации;

[112] Расчёт контрольной суммы файла можно произвести с помощью встроенных в «Мобильный комплекс аудита ИБ ИС», в «Мобильный криминалист», сторонних программ: GOSTsum, filecalc, Arpoon Checksum, HashTab, Alternate HASH-Generator или иных аналогов, позволяющих рассчитать хэш-сумму файла по определённому алгоритму. Расчёт хэш-суммы файла позволяет в дальнейшем подтвердить его идентичность, исключить сомнения о внесении изменений в первоначальное содержание. Таким образом, при помощи расчёта контрольный суммы файла можно подтвердить достоверность цифровой информации.

[113] Отметим, что традиционно используемый в следственной практике расчёт хэш-суммы по алгоритму MD5 в настоящее время признан небезопасным. Например, рабочим информационным документом RFC 6151, выпускаемым под эгидой ISOC, и стандартом компьютерной безопасности правительства США FIPS 140-2 (ANNEX 2). Это связано с тем, что у двух разных файлов при расчёте по алгоритму MD5 не исключается возможность появления одинаковой хэш-суммы, следовательно, подтвердить идентичность изъятой и зафиксированной информации не представляется возможным. Безопасный алгоритм хэширования, версия SHA-2, включает в себя алгоритмы, наиболее часто используемые в следственной практике: SHA-512/256, именно расчёт по такому алгоритму позволяет подтвердить идентичность изъятой и зафиксированной на электронном носителе информации, поэтому с точки зрения обеспечения достоверности доказательств целесообразно использовать алгоритм расчёта контрольной сумм файла по SHA-2.

- во-вторых, в случае, если электронный носитель, на котором содержится изъятая информация, будет повреждён, то это не повлечет её утраты, если информация скопирована на другие электронные носители. Достоверность и идентичность содержащейся информации можно будет подтвердить при помощи расчёта хэш-суммы файла, содержащегося на другом электронном носителе информации, посредством соотношения контрольных сумм файлов, указанных в протоколе следственного действия и полученных с электронного носителя информации.

Специфика цифровых данных, содержащихся в сети интернет или на электронном носителе информации обусловливает и наличие специфических знаний у субъекта, осуществляющего её фиксацию и изъятие. По этому поводу Е. И. Галяшина справедливо отмечает: «если лицу необходимо получить доступ к оригинальному цифровому доказательству, лицо должно иметь соответствующую подготовку; вся деятельность по изъятию, доступу, хранению или передаче цифровых доказательств полностью задокументирована, защищена и доступна для анализа»[114]. Несоблюдение определённых этапов при работе с цифровыми доказательствами может привести впоследствии к признанию представленных доказательств недопустимыми.

Основываясь на вышеприведённых особенностях фиксации и изъятия цифровых следов, находящихся на страницах социальных сетей пользователей или мессенджеров, предлагаем сформулировать следующие рекомендации для дознавателей и следователей при работе с такими доказательствами для признания их надлежащими:

1. Оперативность фиксации и изъятия цифровых данных при их обнаружении.

2. Привлечение специалиста в области компьютерной безопасности или по информационным технологиям (ст. 168 УПК РФ) для оказания помощи в обнаружении, фиксации и изъятии цифровых данных, размещённых в сети интернет, при производстве такого следственного действия, как осмотр предметов (документов) в соответствии со ст. 177 УПК РФ.

3. Верификация того факта, что символьный адрес сайта соответствует его настоящему IP-адресу, что должно подтверждаться соответствующей записью в протоколе, посредством осуществления трассировки сайта.

4. Производство расчёта контрольной суммы файла(-ов) (хэш-суммы), зафиксированного на электронном носителе информации.

5. Производство копирования информации с оригинала (контента сайта, мобильного телефона) как минимум на два электронных носителя информации (оптических диска, USB-накопителя), в целях обеспечения сохранности криминалистически значимой информации.

6. Протокол следственного действия, приложением к которому является определённый файл(-ы) с «цифровыми следами» (данными), содержащейся на электронном носителе информации (pdf, docx, mp4, mkv, avi и др.) должен обязательно включать в себя:

- дату и время фиксации;
- данные о лице, которое производило фиксацию, его подпись;

[114] См. *Галяшина Е. И.* Проблемы криминалистической диагностики фальсификации фонограмм, получаемых при проведении оперативно-розыскных мероприятий // Научная школа уголовного процесса и криминалистики Санкт-Петербургского государственного университета и современная юридическая наука, СПб.: Издательский Дом СПбГУ, 2016. – С. 338.

- данные о специалисте, который был привлечён для участия в следственном действии;
- данные о соответствии символьного адреса сайта его настоящему IP-адресу, что должно подтверждаться соответствующей записью в протоколе;
- данные о хэш-сумме файла, зафиксированного на электронном носителе информации;
- данные об используемых технических средствах (программном обеспечении, компьютерной технике)[115].

Таким образом, процедура фиксации и изъятия цифровых следов из социальных сетей и мессенджеров требует определённого порядка, вызванного спецификой данных объектов, несоблюдение правил работы с такими доказательствами может привести к признанию полученных цифровых данных из сети интернет или электронных носителей информации недостоверными и, как следствие, недопустимыми доказательствами по делу.

2.5. Применение автоматизированных рабочих мест

Особенности применения автоматизированных рабочих мест (АРМ) при работе с цифровыми данными в оперативно-следственной деятельности.

Процедура документирования доказательной базы традиционными способами затруднительна, если речь идёт о цифровых данных. Зачастую данные просто не могут быть обработаны человеком без использования вспомогательных инструментов. Обработка большого числа абстрактных данных, т. е. не имеющих при первом взгляде семантической связи, трудно даётся человеку. Ошибка в одной букве длинной шестнадцатеричной записи того или иного идентификатора часто делает цифровые доказательства недействительными. Таким образом, необходимо применение вспомогательных технических средств, упрощающих работу человека, – автоматизированных рабочих мест (далее – АРМ).

Поскольку с исторической точки зрения понятие автоматизированного рабочего места обладает значительной изменчивостью, что отмечено в работе В.Е. Кадулина и В.С.Потехина[116], считаем необходимым ввести простое и понятное большинству понятие *«АРМ оперативно-следственного назначения» – это комплекс программных и технических средств, предназначенных для решения задач оперативной деятельности либо самостоятельно, либо в рамках более крупных автоматизированных информационных систем.*

[115] См. *Саркисян А. А.* Протокол работы с цифровыми следами / А. А. Саркисян // Социально-экономическое развитие и качество правовой среды : Сборник докладов VIII Московского юридического форума (XIX Международная научно-практическая конференция): в 5 ч., Москва, 08–10 апреля 2021 года. – Москва: Московский государственный юридический университет имени О.Е. Кутафина (МГЮА), 2021. – С. 336-338. – EDN ASRRVZ.

[116] См. *Кадулин В.Е., Потехин В.С.* Об уточнении понятия и классификации автоматизированных рабочих мест, используемых в информационных системах и компьютерных технологиях // Вестник Санкт-Петербургского университета МВД России № 4 (68) 2015 – стр. 208 «не во всех публикациях придерживаются терминологии, введённой ГОСТ 34.003-90 ... встречаются публикации, в которых АРМ рассматривают как разновидность автоматизированной системы, что тоже не совсем верно, поскольку такое понимание противоречит терминологии, введённой стандартами РД 50-680-88, ГОСТ 24.703-85 и ГОСТ 24.104-85, которые в состав АС включают пользователя (в то время как АРМ, согласно ГОСТ 34.003-90, – только программно-технический комплекс)».

Чтобы выполнять работу могли не только опытные работники, но и новички, функционал АРМ ОН должен включать в себя выполнение следующих трёх функций: информационной, документальной и аналитической.

Информационная часть должна обеспечивать следователя или оперативного работника всей необходимой ему информацией. Она должна включать компоненты системы поддержки принятия решений (выдачу советов, предложения шаблонов действий для начинающих специалистов, информирование об изменениях в законодательстве РФ) и системы поиска. Система поиска должна производить поиск по имеющимся нормативным документам (законам, постановлениям, разъяснениям, ведомственным приказам, инструкциям, методическим рекомендациям, информации в отношении судебного делопроизводства и т. п.), ресурсам сети интернет, справочным руководствам обследуемых систем, ведомственным и государственным базам данных (например, ГИБДД, ФНС РФ, ЦБ РФ), ресурсам ИСОДа МВД РФ и т. п. Интерфейс взаимодействия может быть через клавиатуру (традиционную или виртуальную на экране), либо голосовым, как при общении с голосовым помощником «*Алиса*», «*Алекса*», «*Google*» и др.

Документальная часть должна включать в себя сопровождение ведения требуемых форм отчётности. Заполнения нужного числа копий протоколов, запросов и т. п.

Аналитическая часть должна быть интеллектуальным продолжением системы поддержки принятия решений информационной части, но в отличие от неё она должна находить скрытые закономерности в уже собранных данных и наподобие системы подсказок для завершения набираемого текста при поиске предлагать возможные варианты переходов к документальной части.

Например, выстраивать цепочки «протокол следственного действия → приложенный к протоколу файла журнала с нарушением, полученным в результате осмотра → IP-адрес с которого было произведено обращение по сети (найдена запись в файле журнала) → провайдер, кому принадлежит указанный адрес (обращение к базе RIPE или др.) → пользователь, устройству которого был выдан адрес постоянно или через сессию трансляции адресов (*NAT* на момент времени *X*, соответствующий первоначальной записи времени и адреса из файла журнала) → Ф.И.О. подозреваемого физического лица → (1)данные из базы регистрации физических лиц → отображение информации на карте; → (2) движимое имущество, принадлежащее физическому лицу → определение номеров государственных регистрационных знаков транспортных средств → получение информации из ЦОД обрабатывающих видеоизображения камер дорожно-транспортной сети города *Y* о последних зафиксированных нарушениях в отношении указанного транспортного средства» и т. п.

При наличии (обработке) в какой-либо из частей защищаемой законом информации, указанная информация должна быть защищена.

К сожалению, указанные системы, обладающие полным потенциалом описанных возможностей сегодня скорее направление научного развития применения автоматизированных рабочих мест в оперативно-следственной и криминалистической деятельности. Авторы считают важным развивать данное научное направление в будущем, проводить НИОКРы, создавать прототипы систем и внедрять их в использование, поскольку на стыке информационных технологий и преступлений без них будет дальше обходится всё сложнее и сложнее.

2.6. Вопросы для самоконтроля

1. Что отмечал Р.С.Белкин в отношении проблематики фиксации доказательственной информации?
2. В каких формах и видах могут быть представлены цифровые следы?
3. Перечислите категории объектов, которые могут являться носителями криминалистически значимой компьютерной информации.
4. Дайте определение понятия "запись информации".
5. Чем отличаются внутренние и внешние носители информации?
6. Как Вы понимаете термин "распределённые (облачные) носители информации"?
7. Для компонентов персонального компьютера приведите примеры устройств обработки информации.
8. Для чего предназначены устройства обработки информации?
9. Что по своей сути представляют собой устройства передачи информации по каналам связи?
10. Приведите примеры устройств передачи информации.
11. Дайте криминалистическую оценку и классификацию для мобильных телефонов сотовой связи, смартфонов, планшетов.
12. Приведите отличительные черты доказательственной информации, хранящейся в цифровом виде.
13. Верно ли утверждение: современные цифровые устройства являются как средствами, продуцирующим цифровые следы, так и сами (или их части) представляют собой цифровой след (способны хранить цифровые следы от других устройств)?
14. Перечислите и раскройте основные принципы, которыми следует руководствоваться при проведении следственных действий, сопряжённых с изъятием компьютерных средств и систем.
15. При собирании цифровых следов необходимо обеспечить их сохранение в неизменном виде, что делать, если достичь выполнения указанного требования невозможно?
16. Какие появляются особенности (с точки зрения собирания доказательств) при использовании в современных условиях центров обработки и хранения данных?
17. Какие новые проблемы породили цифровые следы?
18. Расшифруйте аббревиатуру КТЭ.
19. Какие проблемы (в рамках получения цифровых следов, как доказательств) могут возникнуть в отношении предприятий использующих автоматизированные системы управления технологическим процессом?
20. Каким образом в соответствии с нормами Российского законодательства производится выемка предметов и документов, содержащих государственную или иную охраняемую федеральным законом тайну, информацию о вкладах и счетах граждан в банках и иных кредитных организациях (для платёжных систем)?
21. Для защиты от компрометации автоматизированных банковских систем какие правила идентификации и сбора цифровых криминалистических данных установлены в России?
22. За счёт чего достигается придание (обеспечение) юридического значения показаниям программно-технических средств?
23. Поясните, из-за наличия каких факторов в сложных специализированных системах возможность идентификации и сбора данных за счёт возможностей широко распространённых инструментальных средств существенно ограничена.
24. Чем обусловлена по мнению специалистов сложность осмотра?
25. Кто ещё, помимо следователя, должен входить в состав следственно-оперативной группы (СОГ) при осмотре места происшествия?

26. Приведите пример (состав) СОГ.
27. Могут ли быть в состав СОГ включены незаинтересованные в деле специалисты? (Ответ обоснуйте.)
28. Каковы цели осмотра места происшествия?
29. Поясните тактический приём осмотра «от центра – к периферии».
30. Если при проведении осмотра места происшествия используются специализированные комплексы, СВТ и специальные поисковые технические устройства (материалы), то в каком документе делается об этом соответствующая отметка и что в ней указывается?
31. Могут ли одноразовое кратковременное включение-выключение СВТ или разрыв соединения между ними привести к уничтожению компьютерной информации?
32. Какие фактические данные в протоколе должны быть описаны особенно тщательно?
33. Какие типичные вещественные доказательства в цифровой среде должны быть осмотрены и описаны в протоколе?
34. Приведите примеры типичных вещественных («аналоговых») следов.
35. Перечислите все документы и их носители, являющиеся доказательствами подготовки, совершения и сокрытия преступления, подлежащие осмотру.
36. Приведите примеры того, на что стоит обращать внимание, где искать цифровые следы.
37. Немаловажное значение имеет обнаружение и изъятие в помещении, где установлено компьютерное оборудование, «традиционных» вещественных доказательств, какие это могут быть предметы?
38. Какие методы и стандарты аудита информационной безопасности и технических мероприятий по реагированию на компьютерные инциденты уместно применять для поиска и документирования «цифровых следов»?
39. Что необходимо указать в протоколе следственного действия перед началом осмотра?
40. Какие документы, необходимые для решения вопроса о нарушении правил эксплуатации ЭВМ, обязательно изымаются ходе выемки?
41. В чём отличие осмотра места происшествия от обыска?
42. Готовясь к проведению обыска, что должен решить для себя следователь? (на какие вопросы ответить, что тщательно изучить, на что обратить внимание и т.д.)
43. Набросайте в черновом варианте пример плана предстоящего обыска.
44. Что в подавляющем большинстве случаев является предметом выемки по уголовным делам о преступлениях в сфере компьютерной информации?
45. На что следует обратить внимание в ходе выемки МНИ?
46. Если проверяются действия, производимые подозреваемым, то кто из лиц предпочтительнее для демонстрации проверяемых действий участникам следственного действия?
47. Как производится процедура фиксации и изъятия цифровых данных из «облачных» объектов?
48. При проведении следственных действий что предпочтительнее: делать статические снимки экрана из исследуемой системы или производить видеозапись самого процесса обследования? (Ответ обоснуйте.)
49. В чём заключается проблема, что при получении информации с электронных устройств имеется возможность удалённого подключения к этим устройствам по сети?
50. В чём заключается документирование доказательной базы?
51. Опишите возможное применение автоматизированных рабочих мест в будущем?

Глава 3. Особенности доказывания с использованием цифровых следов

Особенности доказывания по уголовном делам совершённым с использованием информационных технологий.

3.1. Возможные случаи

Вариативность тактики следствия и способов доказывания по уголовным делам по IT-преступлениям в зависимости от источника доказательств.

3.1.1. Ситуативность следственной тактики

Комплексность и вариативность следственной тактики по уголовным делам, связанным с информационными технологиями.

Рассмотрим вариативность тактики следствия и следственных действий на первоначальном этапе расследования.

Ситуация 1. Сведения о причинах возникновения общественно опасных деяний, способе их совершения и личности правонарушителя отсутствуют.

Ситуация 2. Имеются сведения о причинах возникновения преступления, способе его совершения, но нет сведений о личности преступника.

Ситуация 3. Известны причины возникновения преступления, способы его совершения и сокрытия, личность преступника и другие обстоятельства.

В первых двух следственных ситуациях обычно планируют и осуществляют следующие неотложные следственные действия, оперативно-разыскные, организационные и иные мероприятия:

1) получение объяснения (допрос) заявителя или лиц, на которых указано в исходной информации как на возможных свидетелей (очевидцев);

2) вызов и инструктаж необходимых специалистов для участия в осмотре места происшествия;

3) осмотр места происшествия (с осмотром, предварительным исследованием и изъятием машинных носителей и компьютерной информации, компьютерной техники (СВТ/АРМ, ноутбуки, смартфоны и т. п.), документов и т. п.);

4) проведение оперативно-разыскных мероприятий в целях установления причин совершения преступления, выявления лиц, виновных в его совершении, определения

рабочего места преступника, обнаружения следов и других вещественных доказательств;

5) изучение справочной литературы, ведомственных нормативных актов, положений, инструкций, правил эксплуатации конкретного СВТ и порядка работы с компьютерной информацией, а также консультации с соответствующими специалистами;

6) наведение справок в контролирующих, инспектирующих и лицензирующих организациях и их структурных подразделениях (территориальных органах Ростехнадзора, Росатомнадзора, ФСТЭК, Росгвардии, ФСБ, ФНС, ФТС, ФССП России и др., ТПП, Россанэпидемнадзоре, Роскомнадзоре, Росреестре, КРУ (региональной счетной палате), торговой инспекции и т. п., а также операторах связи или интеграторах услуг [61];

7) истребование материалов контрольных проверок, инвентаризаций и ревизий (соблюдения правил обработки информации, системы защиты конфиденциальной информации, оборота электронных документов и др.) за интересующий следствие период, в случае необходимости – организовать их производство (в том числе повторно);

8) выемку и последующий осмотр недостающих документов (в том числе находящихся в электронной форме на машинных носителях информации), характеризующих производственную операцию, в ходе которой по имеющимся данным совершены преступные действия, а также орудий (СВТ, программ для ЭВМ, компьютерной информации, предметов, материалов и др.), с помощью которых они, возможно, были изготовлены;

9) допросы подозреваемых и (или) свидетелей, ответственных за данный участок работы, конкретную производственную операцию и защиту конфиденциальной информации;

10) обыски на рабочих местах и по месту проживания подозреваемых;

11) назначение судебных экспертиз – компьютерно-технической, радиотехнической, технической, бухгалтерской, полимерных материалов и изделий из них и иных.

Дальнейшие действия планируются с учётом дополнительной информации, полученной при производстве вышеуказанных действий.

При наличии третьей следственной ситуации необходимо:

1) изучить поступившие материалы с позиций их полноты, соблюдения норм уголовно-процессуального законодательства и порядка их передачи в органы предварительного следствия. При необходимости – принять меры к получению недостающей процессуальной информации;

2) решить вопрос о возможности задержания преступника с поличным и о необходимых в связи с этим мероприятиях;

3) провести личный обыск задержанного;

4) провести осмотр места происшествия с участием соответствующих заранее приглашённых специалистов;

5) допросить задержанного;

6) провести обыски на рабочем месте и по месту проживания задержанного;

7) установить связи задержанного и лиц, причастных к совершению преступления;

8) допросить свидетелей (очевидцев);

9) допросить подозреваемого;

10) провести выемку и осмотр следующих вещественных доказательств и документов: подлинных документов, удостоверяющих личность преступника и наличие у него соответствующих специальных познаний, характеризующих те производственные операции, в процессе которых допущены нарушения и преступные действия (в том числе документов, находящихся в электронной форме на машинных носителях информации); орудий подготовки, совершения и сокрытия преступления; предмета преступления;

11) провести допросы лиц, названных в документах, переданных в следственные органы, как допустивших нарушения, ответственных за конкретный участок работы по фактам установленных нарушений;

12) истребовать, а при необходимости – провести выемки нормативных актов и документов, характеризующих порядок и организацию работы в данном подразделении с конфиденциальной информацией, с бланками строгой отчётности, компьютерной информацией, ЭВМ, системой ЭВМ, их сетью и т. п.;

13) допросить свидетелей, причастных к соответствующим производственным операциям или подозреваемых в связях с преступником;

14) проанализировать полученную информацию и решить вопрос о необходимости назначения судебных экспертиз, проведения ревизии, инвентаризации или контрольной проверки (в том числе повторной).

В очерёдность перечисленных следственных действий, оперативных и организационных мероприятий могут быть внесены коррективы в зависимости от изменения ситуации.

3.1.2. Назначение и задачи экспертиз

Назначение и задачи компьютерно-технических и иных экспертиз по уголовным делам, связанным с информационными технологиями.

При расследовании преступления в сфере компьютерной информации наиболее характерна компьютерно-техническая экспертиза. Её проводят в целях:

- воспроизведения и распечатки всей или части компьютерной информации (по определённым темам, ключевым словам и т.д.), содержащейся на машинных носителях, в том числе находящейся в нетекстовой форме (в сложных форматах: в форме языков программирования, электронных таблиц, баз данных и т.д.);
- восстановления компьютерной информации, ранее содержавшейся на машинных носителях, но впоследствии стертой (уничтоженной) или измененной (модифицированной) по различным причинам;
- установления даты и времени создания, изменения (модификации), уничтожения, либо копирования информации (документов, файлов, программ);
- расшифровки закодированной информации, подбора паролей и раскрытия системы защиты от НСД;
- исследования СВТ и компьютерной информации на предмет наличия программно-аппаратных модулей и модификаций, приводящих к несанкциониро-

ванному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети;

- установления авторства, места (средства) подготовки и способа изготовления документов (файлов, программ), находящихся на МНИ; выяснения возможных каналов утечки информации из компьютерной сети, конкретных СВТ и помещений;
- установления возможных несанкционированных способов доступа к охраняемой законом компьютерной информации и её носителям; выяснения технического состояния, исправности СВТ, оценки их износа, а также индивидуальных признаков адаптации СВТ под конкретного пользователя;
- установления уровня профессиональной подготовки отдельных лиц, проходящих по делу, в области программирования и в качестве пользователя конкретного СВТ;
- установления конкретных лиц[117], нарушивших правила эксплуатации ЭВМ, системы ЭВМ или их сети; установления причин и условий, способствующих совершению преступления в сфере компьютерной информации.

Признав необходимым назначение судебной экспертизы, следователь (дознаватель) выносит об этом постановление в соответствии со ст. 195 «*Порядок назначения судебной экспертизы*» УПК РФ , как правило при участии специалиста:

- обосновывает основания назначения судебной экспертизы;
- формулирует вопросы перед экспертом;
- группирует материалы (предметы, документы и носители с информацией), предоставляемые в распоряжение эксперта;
- определяет (подбирает) экспертное учреждение, в котором должна быть произведена судебная экспертиза или конкретного эксперта, обладающего специальными знаниями.[118]

Важно. Даже если следователь имеет подготовку в сфере информационных технологий, всегда рекомендуется до вынесения постановления о назначении экспертизы ещё раз проконсультироваться со специалистом по поводу её целей, формулировки вопросов, характера предоставляемых материалов.

Может быть назначена идентификационная и/или диагностическая компьютерно-техническая экспертиза.

По делам рассматриваемой категории из криминалистических экспертиз наиболее часто назначают дактилоскопическую, одорологическую, трасологическую, почерковедческую, фоноскопическую, автороведческую, радиотехническую и технико-криминалистическую экспертизу документов, экспертизу полимерных материалов и изделий из них.

[117] Следует иметь ввиду, что полученные идентификационные данные учётной записи, IP-адрес и т.п. не устанавливают конкретных лиц. Для этого потребуется или использование данных биометрии (если она есть), либо свидетельские показания с синхронизацией (однозначным соотнесением) моментов времени полученных из различных источников.

[118] См. *Саркисян А. А.* Сертификация судебных экспертов в условиях цифровизации / А. А. Саркисян // Законы России: опыт, анализ, практика. – 2021. – № 3. – С. 65-67. – EDN CMEAQD.

3.1.3. Типовая процедура подготовки к процессуальным действиям

Типовая процедура подготовки к процессуальным действиям следователя (дознавателя) для сбора доказательств по уголовным делам, связанным с IT-преступлениями.

Если у следствия есть основания полагать, что цифровая информация может являться доказательством по уголовному делу, то она должна изыматься только процессуальными способами, предусмотренными законом: в процессе производства осмотра, обыска, выемки. Выбор конкретного следственного действия зависит от решения следователя, которое, как правило, обусловлено конкретной ситуацией расследования на момент необходимости изъятия цифровой информации.

Все следственные действия по делам о преступлениях в сфере компьютерной информации проводятся в строгом соответствии с правилами, регламентированными действующим уголовно-процессуальным законодательством, но с учётом следующих основных особенностей:

- следственное действие должно быть заблаговременно подготовлено и детально спланировано;
- в каждом следственном действии должны принимать участие специалисты чётко представляющие свои задачи, права и обязанности;
- понятые должны обладать минимально необходимыми специальными познаниями в области обработки компьютерной информации (на уровне бытовых пользователей ПЭВМ), следователь и специалисты – познаниями в части полной сохранности (неизменяемости) компьютерной информации, содержащейся на осматриваемом (изымаемом) средстве электронно-вычислительной техники;
- для осмотра, обыска и выемки компьютерной информации и её носителей заранее должны быть подготовлены необходимые СВТ и материалы.

В бесконфликтной ситуации с собственником или владельцем цифровой информации, когда гражданин или организация потерпели от правонарушения и готовы оказать помощь в установлении истины, целесообразно проводить выемку или осмотр. Такая ситуация чаще всего складывается с организациями, подвергшимися неправомерному доступу к компьютерной информации.

В конфликтной ситуации, особенно при расследовании преступлений в сфере экономики, целесообразно проводить обыск, поскольку гражданин и организация могут оказывать явное или скрытое противодействие, вплоть до преграждения доступа и уничтожения информации и её носителей.

Задачи подготовительной стадии [59]:

1. получить наиболее полное представление о характере деятельности объекта, где могут находиться следы преступления и другие объекты, относящиеся к расследуемому делу, изучить обстановку в организации: отрасль хозяйствования, порядок учёта, документооборот, структуру, особенности используемых технологий;

2. изучить коммуникативные и иные тактико-технические характеристики используемой компьютерной техники и программного обеспечения;

3. изучить организацию охраны объекта информатизации и конкретной компьютерной информации;

4. выяснить служебные обязанности лиц, имеющих санкционированный доступ к охраняемой законом компьютерной информации, а также их прямое или косвенное отношение к ценностям (имуществу), которые стали предметом правонарушения.

Для полного, объективного и всестороннего исследования всех обстоятельств совершения преступления следует получить ответы на целый ряд вопросов, касающихся обстановки в организации:

1. Сколько компьютеров в организации, в каких подразделениях они находятся (отделах, службах, филиалах, подразделениях и пр.)?

2. Известно ли конкретное СВТ, носитель информации, которое было использовано в качестве орудия или средств совершения преступления, объекта посягательств или источника доказательств о преступлении?

3. Имеется ли локальная сеть (одна или несколько)? Какова размерность сети (сколько ПЭВМ объединены сетью и в каких помещениях они находятся)? Имеются ли у организации филиалы и представительства, по каким адресам, соединены ли в локальную сеть их компьютеры? Связаны ли их сети с сетью основного предприятия?

4. Есть ли в организации компьютеры, имеющие выход в глобальную сеть интернет? В каких помещениях они находятся? Посредством какого провайдера осуществляется выход в глобальную сеть?

5. Какие средства связи и телекоммуникаций используются для работы средств вычислительной техники и информационного обмена (какого типа, общедоступные или конфиденциальные, абонентские номера, позывные, ключи (коды) доступа)?

6. Каков режим и система охраны объекта? Какая организация осуществляет охрану?

7. К какой категории относится обрабатываемая информация (имеются ли данные, составляющие государственную тайну, конфиденциальная информация, персональные данные)?

8. Какие источники электропитания используются (электросеть, автономные, бесперебойные, комбинированные)?

9. Какая операционная система и какое программное обеспечение используется на компьютерах в сети?

10. Какие средства защиты доступа используются в локальной сети (коды, пароли, шифры, программные средства и др.)?

11. Какая документация по функционированию локальной сети ведётся в организации? Кто ответственен за её ведение?

12. Другие вопросы в зависимости от контекста IT-преступления, например: «Какая часть бухгалтерского учёта (какие именно учётно-хозяйственные операции) фиксируется через локальную сеть и где хранятся итоги обработки?».

Для выяснения перечисленных выше вопросов проводится ряд следственных действий и иных мероприятий, в частности:

- запрос и изучение схемы документооборота организации, утверждённой приказом руководителя на текущий год или интересующий следствие период;
- выемка и изучение документов по локальной сети (технический проект и сопроводительные документы, в которых указываются: количество помещений, охваченных сетью; количество ПЭВМ в каждом помещении, подключенных к

сети; схемы мест подключения в каждом помещении; место нахождения сервера; тип машины, которая будет использоваться в качестве сервера, и её технические характеристики);

- анализ показаний свидетелей, потерпевших, подозреваемых, обвиняемых, допрошенных по перечисленным выше вопросам. Свидетельская база должна быть расширена и представлена следующими группами свидетелей: заказчики локальной сети, проектировщики, менеджер сети, операторы и лица, работающие непосредственно с сервером и рабочими станциями, и другие;
- выемка и исследование актов проверок независимых контролирующих органов: налоговых, финансовых, экологических, санитарных, пожарных, а также аварийных, аудиторских проверок и других документов.

В этот период тактически правильно должны быть определены не только места проведения следственных действий, но и время с учётом возможного доступа к средствам компьютерной информации, оказания противодействия следственной группе со стороны правонарушителей, полноты загрузки мощностей действующего компьютерного оборудования или, наоборот, его отключения и т. д.

План

Обязательно должен составляться план предстоящего следственного действия, в котором учитываются и тактически обоснованно используются полученные данные об обстановке в заподозренной организации. Именно на основе результатов, как правило, мероприятий оперативно-разыскной деятельности, следователь (дознаватель) определяет место, время проведения следственного действия, его участников, материально-техническое обеспечение и др. Важно иметь информацию о схеме локальной вычислительной сети или схеме межсетевого взаимодействия, в том числе беспроводного (такую информацию целесообразно добыть заблаговременно путём поручения следователя органу дознания негласных ОРД и ОТМ в соответствии с законом об ОРД).

Планирование состава оперативно-следственной группы зависит от обстановки в организации. Кроме следователя, осуществляющего руководство производством следственного действия, в следственно-оперативную группу дополнительно включаются для МВД России или СК РФ (наименования подразделений могут отличаться в зависимости от организационно-штатного строения территориального органа внутренних дел (безопасности), или иного органа (службы), осуществляющего обеспечение процессуальных действий):

- оперуполномоченный отдела «К» ПСТМ ТОВД;
- специалист-криминалист (от ЭКЦ ТОВД или подразделения криминалистики управления СК РФ по субъекту РФ)
- специалист (инженер) подразделения ИТ, связи и защиты информации ТОВД;
- иные специалисты (при необходимости, в зависимости от вида и функций носителей цифровой информации, подлежащей осмотру).

Замечание. При необходимости, СОГ дополняется представителями оперативно-боевого подразделения ТОВД, Росгвардии для защиты участников процессуальных мероприятий, обеспечения правопорядка и охраны следственно-оперативной группы.

При производстве следственного действия могут присутствовать:

- собственник жилья и проживающее лицо (если следственное действие проводится в жилище);
- представители организации, в которой проводится следственное действие: администрации; службы безопасности; персонал, обслуживающий носители цифровой информации; специалисты (операторы ЭВМ, бухгалтеры, контролёры, технологи и другие, в зависимости от задач следственного действия и обстановки) и др.

Техническая подготовка включает обеспечение: транспортом, упаковочными материалами, научно-техническими средствами различного назначения, достаточным количеством съёмных МНИ для копирования информации.

Рекомендация

В качестве рекомендации, целесообразно иметь при себе:

- носимый (мобильный) инженерный комплекс типа «Мобильный криминалист», «Мобильный комплекс аудита информационной безопасности информационных систем» [96] или аналогичный, как правило, включающий в себя:
  1. портативный компьютер типа «Notebook» с соединительными кабелями с различными разъёмами или с комбинированным разъёмом;
  2. сертифицированное программное средство однонаправленного копирования информации [97] (и\или аппаратное устройство однонаправленного чтения информации, т. н. блокиратор записи), при их отсутствии, программное обеспечение для копирования информации на месте производства следственного действия;
  3. набор сервисных программ для определения технических характеристик исследуемых компьютеров, исправности отдельных устройств и внешней памяти, а также антивирусные программы;
- при необходимости копирования фрагментов информации – комплект сторонних твердотельных накопителей (USB/SATA-Flash/SSD, чистых компакт-дисков (BD/DVD/CD-R или -RW) для записи информации.
- при необходимости, МФУ со сканером или принтер для вывода в бумажную (твёрдую) копию и распечатки протокола следственного действия.

Необходимый набор таких программ следователь или специалист формирует по своему усмотрению в зависимости от категории расследуемых дел, используемого программного обеспечения и оборудования в данном регионе в данный момент времени, либо использует типовой, входящий в состав носимого (мобильного) комплекса.

Изъятые в ходе осмотра места происшествия, обыска или выемки средства вычислительной техники и электронные носители информации, а равно содержащиеся на них цифровые следы нуждаются в последующем исследовании.

Предварительное исследование, предшествующее назначению судебной экспертизы, возможно провести в рамках осмотра предметов с привлечением специалиста с использованием многофункциональных возможностей универсальных криминалистических комплексов с высоким уровнем автоматизации, например отечественных мобильных комплексов МКА-ИБИС, Belkasoft Evidence или Мобильный криминалист. Интерфейс таких систем во многом оптимизирован для работы пользователей без углублённых специальных знаний, в связи с чем их применение часто называют исследованием с помощью одной кнопки – «PBF» (аббревиатура *от англ. – push-button forensics*). С другой стороны, упрощённый интерфейс несёт в себе риск утраты цифровых следов поскольку такие комплексы не в состоянии обработать нестандартные ситуации.[119]

При осмотре средств вычислительной техники и накопителей информации важно следовать общим правилам по работе с цифровыми данными. Для обеспечения неизменности информации подключение электронных носителей, в том числе копий дисков, следует производить исключительно с использованием специальных устройств-блокираторов, либо программно-технических комплексов, имеющих сертификат соответствия в качестве средств аудита информационной безопасности, средств контрольно-технически мероприятий оценки защищённости или средств (устройств) однонаправленного доступа. Включение осматриваемого компьютерного устройства допускается исключительных случаях, когда иным образом извлечь криминалистически значимую информацию невозможно, о чём специалист (эксперт), как правило, информирует следователя (дознавателя). В этом случае все манипуляции с устройством и цифровыми следами должны быть детально отражены в протоколе осмотра предмета и, по возможности, зафиксированы посредством фотосъёмки либо видеозаписи или зарегистрированы иным техническим способом.

Как отмечалось выше, место совершения компьютерного преступления неоднозначно, поэтому поиск и фиксация компьютерной информации осуществляется на различных объектах, а именно в местах:

- непосредственной обработки и постоянного хранения компьютерной информации, ставшей предметом преступного посягательства;
- непосредственного использования компьютерного оборудования с целью неправомерного доступа к охраняемым базам и банкам данных или создания, использования и распространения вредоносных программ для ЭВМ;
- хранения добытой преступным путём из других компьютеров, компьютерных систем и сетей информации на машинном носителе, в ЭВМ, системе ЭВМ или их сети;
- непосредственного нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети;
- наступления вредных последствий; задержания подозреваемого (личный обыск).

Грамотно проведённые осмотры, обыски и выемки дают следователю (дознавателю) богатый, но к сожалению, избыточно обширный материал для дальнейшего расследования. Его дополняют показания заявителей о совершённом преступлении, а так-

[119] Joshua I. James, Pavel Gladyshev. Challenges with Automation in Digital Forensic Investigations // URL: https://arxiv.org/pdf/1303.4498 (дата обращения 11.07.2021).

же свидетелей, как правило, из числа участвовавших в подготовке деяния лиц или из круга их общения.

3.1.4. Специфика организации проведения опросов и допросов

Специфика организации проведения опросов и допросов по уголовным делам, связанным с информационными технологиями.

Если заявление поступило от лиц, которым причинён материальный, моральный или иной вред действиями преступников, они признаются потерпевшими по делу. В ходе их допроса выясняется обстановка в организации, способы защиты компьютерной информации и доступа к ЭВМ и локальной сети организации, обстоятельства выявления преступления, последствия преступного посягательства, оценка причинённого вреда.

После таких допросов легко определить свидетельскую базу, т. е. тех лиц, которые причастны к работе вычислительных систем и сетей. Начинать допросы, безусловно, следует с очевидцев совершённого преступления, т. е. тех, кто непосредственно может свидетельствовать о неправомерном доступе к информации, создании, использовании или распространении вредоносных программ или нарушении правил эксплуатации компьютерного оборудования либо о тех последствиях, которые возникли в результате этих действий.

В качестве свидетелей допрашиваются сотрудники потерпевшей организации по обстоятельствам неправомерного доступа: операторы; администраторы сети; работники бухгалтерии и финансового отдела; руководители отделов, где обрабатывается информация, подвергшаяся «нападению»; инженеры-программисты, разработавшие программное обеспечение и осуществляющие его отладку и обслуживание; специалисты, занимающиеся эксплуатацией и ремонтом компьютерной техники; системные программисты; инженеры по средствам связи и телекоммуникационному оборудованию; специалисты, обеспечивающие информационную безопасность; работники охраны и службы безопасности и другие.

Целью их допросов является получение показаний об обстоятельствах, предшествовавших совершению преступления, для установления круга подозреваемых лиц; об обстоятельствах обнаружения факта преступления и наступивших негативных последствиях. Уточняется наличие и функционирование защиты информации, например, программы шифрования, её недостатки, иные причины и условия, которые могли быть использованы для совершения противоправных действий.[120]

[120] Фактически уточняется объективная сторона преступления, которая в уголовном праве представляется собой внешнее, доступное восприятию проявление преступления, поскольку она, более, чем другие элементы преступления, даёт ответы на вопросы: что, где, когда и как (каким образом) произошло или было совершено? Возможно, вам помогут традиционно выделяемые признаки объективной стороны:

1. собственно преступное проявление (чьего-либо деяния);
2. последствия этого деяния;
3. причинная связь между деянием и последствием;
4. пространственно-временная характеристика совершения преступления;
5. способ совершения преступления;
6. орудия и средства, используемые преступником для совершения преступления;
7. обстановка, в которой совершено преступление.

В результате складывается одна из двух ситуаций: подозреваемые (возможные преступники) установлены или не установлены.

Если «преступник»[121] не установлен, целесообразно в ходе допроса попытаться выяснить некоторые криминалистические признаки, позволяющие получить сведения о правонарушителе. Например, как часто менялись коды и пароли доступа к информации, на ком лежала ответственность за их смену, имелись ли факты осуществления сотрудниками сверхурочных работ без видимых на то причин, немотивированные отказы от отпусков сотрудников, обслуживающих компьютерные системы или сети, чрезмерный интерес некоторых сотрудников к работе других отделов, к документам или работе компьютеров, появление дискет или лазерных дисков для копирования компьютерной информации, другие случаи подозрительного поведения сотрудников, обслуживающего персонала или по-сторонних лиц, кто из посторонних лиц проявлял интерес к оборудованию, программному обеспечению и компьютерной информации.

Если «преступник» установлен, проводится его задержание[122], личный обыск, допрос в качестве подозреваемого, обыск по месту жительства и работы, другие следственные действия. Готовиться к допросу подозреваемого и обвиняемого в ряде случаев целесообразно, заранее получив консультацию специалиста, поскольку совершение компьютерных преступлений по плечу не каждому субъекту, а лишь тем, кто имеет специальную подготовку, соответствующие знания, навыки, оборудование. Знания следователя не всегда могут соответствовать необходимому уровню, поэтому он должен восполнять пробелы за счёт привлечения специалиста. Лучше всего получить предварительную консультацию, а затем пригласить специалиста для участия непосредственно в допросе.

В ходе допроса подозреваемого и обвиняемого выясняются следующие вопросы:

- какое образование имеет подозреваемый или обвиняемый, имеет ли навыки обращения с компьютером, где, когда и при каких обстоятельствах он освоил работу с компьютерной техникой и с конкретным программным обеспечением;
- каково место его учёбы или работы, должность, работает ли он на компьютере по месту работы, имеет ли правомерный доступ к компьютерной технике и к определённым видам программного обеспечения;
- какие операции с компьютерной информацией выполняет на рабочем месте;
- имеет ли правомерный доступ к глобальной сети интернет или иной, работает ли в них;
- закреплены ли за ним по месту работы идентификационные коды и пароли для работы в компьютерной сети, кто их устанавливает, как часто они меняются;
- если не работает, то какие операции выполняет на своём персональном компьютере либо персональных компьютерах других лиц из своего ближайшего окружения, где и у кого приобрёл программы для своей ЭВМ.

[121] Отнесение подозреваемого к категории преступников осуществляет суд, поэтому слово «преступник» здесь и далее взято в кавычки, под «преступником» понимается подозреваемый или обвиняемый, либо лицо, реально совершившее противоправное деяние .

[122]Если подозреваемый целенаправленно скрывается или находится вне России, например, за рубежом, то обвинение при наличии доказательств можно вынести и заочно, а в розыск объявить при наличии постановления об изменении статуса – объявлении подозреваемым.

При адекватном психологическом подходе следователя, на такие вопросы подозреваемые отвечают охотно и даже немного бравируют, стараясь показать своё превосходство над следователем в области знания компьютерного оборудования. Если подозреваемый или обвиняемый пожелает далее отвечать на вопросы, то следует выяснить у него обстоятельства совершённого преступления:

- как и кто высказал идею совершения преступления;
- как осуществлялась подготовка, выбирался объект «атаки»;
- каковы мотивы и цель совершения преступления;
- как осуществлён неправомерный доступ к информации, создана вредоносная программа, использовалась ли или распространялась ли она, знает ли создателя вредоносной программы;
- знает ли о наступивших вредных последствиях;
- другие вопросы.

Несколько отличается тактика допросов подозреваемых в нарушении правил эксплуатации ЭВМ, системы ЭВМ или их сети. Ими могут быть только лица, имеющие правомерный доступ к компьютерному оборудованию и сети, компьютерной информации. Это может быть как любой сотрудник-пользователь корпоративной или ведомственной сети организации, но чаще всего это сотрудники инженерно-технических подразделений, техперсонал центра обработки данных или обслуживающей организации: операторы, программисты, техники-наладчики, дежурные машзалов ЦОД. Они зачастую и сами понимают объём и меру своей ответственности, поэтому при опросе и допросе этих лиц следует выяснять:

- когда назначен на должность, какое получил образование, какими навыками обладает;
- был ли ознакомлен с установленными режимом работы и правилами эксплуатации; в каком документе такое ознакомление отражено, проводился ли официальный инструктаж, кем и как часто, в каких документах фиксировался;
- каковы место и время факта нарушения правил эксплуатации, в какой период времени подобным образом эксплуатировалось оборудование;
- чем конкретно выразилось нарушение правил эксплуатации, каковы технические аспекты способа и механизма нарушения правил: совершены действия, не предусмотренные инструкциями; не выполнены предписанные действия; нарушены технологии соответствующих операций;
- каковы последствия допущенных нарушений: возникновение нештатной ситуации с компьютером и его устройствами, повлекшей уничтожение, модификацию или копирование информации; выведение из строя компьютерной системы, вызвавшее блокирование информации и нарушение работы организации, учреждения, предприятия, систем управления и связи; вывод из строя оборудования организации, управляемого компьютерными программами; иное;
- место наступления вредных последствий.

Также в отношении субъектов преступления устанавливаются:

- персональные данные; занимаемая должность;
- функциональные обязанности, связанные с ответственностью за информационную безопасность и надёжность работы компьютерного оборудования, за обес-

печение выполнения правил эксплуатации данной компьютерной системы или сети;

- нормативные акты, устанавливающие функциональные обязанности субъекта: инструкции и правила по эксплуатации, приказы, распоряжения руководителей, трудовой договор или контракт, дополнительные соглашения и пр.;
- образование и специальность;
- стаж работы по специальности и на данной должности; уровень профессиональной квалификации; данные, характеризующие лицо по месту работы.

Указанная информация устанавливается посредством допросов свидетелей, самого подозреваемого, истребования соответствующих документов из кадрового органа, осмотра эксплуатационных документов на данную компьютерную систему, осмотра компьютера, оборудования к нему, машинных носителей информации, распечаток.

3.2. В ходе предварительного расследования

Доказывание с использованием результатов оперативно-разыскной деятельности и возможность переквалификации деяний в ходе предварительного расследования.

3.2.1. Использование результатов ОРД в процессе доказывания

Особое значение использования результатов оперативно-разыскной деятельности в процессе доказывания по уголовным делам о преступлениях, совершённых с использованием информационных технологий.

Уголовно-процессуальный закон запретил использовать в процессе доказывания результаты оперативно-разыскной деятельности, если они не отвечают требованиям, предъявляемым УПК РФ к доказательствам (ст. 89 УПК РФ). Они, как и все доказательства по делу, должны быть относимыми и допустимыми.

Согласно ст. 11 Федерального закона «*Об оперативно-розыскной деятельности*» результаты этой деятельности могут быть использованы, в частности, для подготовки и осуществления следственных действий, представляться в орган дознания, следователю или в суд, в производстве которого находится уголовное дело, а также использоваться в доказывании по уголовным делам в соответствии с положениями уголовно-процессуального законодательства Российской Федерации, регламентирующими собирание, проверку и оценку доказательств.

Добывание фактической оперативной информации, значимой для выявления, предупреждения, пресечения и раскрытия преступной деятельности, представляет собой главную цель любого оперативно-разыскного мероприятия (далее – ОРМ). Однако результаты ОРМ могут стать доказательствами по уголовному делу в том случае, когда они могут быть легализованы путём приобщения к материалам уголовного дела в процессуальном порядке.

Использование результатов ОРД способно существенно обогатить доказательственную базу, в том числе за счёт того, что:

1) могут быть использованы специальные технические средства, применение которых не требует решения суда;

2) существует возможность одновременного проведения нескольких ОРМ;

3) допускается использование помощи при проведении ОРМ должностных лиц и специалистов, обладающих научными, техническими и иными специальными знаниями, а также отдельных граждан.

Ввиду прямого запрета в Федеральном законе от 12.08.1995 № 144-ФЗ «*Об оперативно-розыскной деятельности*» использования специальных и иных технических средств, предназначенных для негласного получения информации, не уполномоченными на то законодательством физическими и юридическими лицами, такие действия являются нарушением закона. Однако указанный запрет достаточно часто обходится на практике, т. к. граждане, участвующие на добровольной основе в ОРМ, используют предоставленные им оперативными сотрудниками специальные технические средства в целях фиксации ОРМ.

Для решения этих проблем представляется необходимым протоколирование не только процесса изъятия документов, предметов и материалов в ходе ОРМ, но и в целом документирование (протоколирование) всех результатов и хода ОРМ в тех случаях, когда оно возможно. Это обусловлено необходимостью наличия такой информации, как время, место и обстоятельства изъятия предметов, материалов и документов, сообщений, видео- и аудиозаписей, копий, слепков и т. п., которые были получены в ходе ОРМ.

Перечисленные данные, в свою очередь, необходимы для проверки подлинности результатов ОРМ и должны содержаться в едином протоколе.

В случае представления третьим лицом сведений, полученных с помощью технических средств, для их «введения» в уголовный процесс необходимо учитывать следующие особенности:

1) качество полученных сведений, полнота информации часто напрямую зависит от наличия или отсутствия у лица специальных знаний, навыков;

2) сведения, полученные и представленные третьими лицами, не всегда могут отвечать требованиям достоверности. Препятствием будет являться возможность внесения изменений в представленные в электронном виде фотоснимки, аудио- и видеозаписи;[123]

3) на практике процессуальное введение информации от третьих лиц в уголовное дело, полученной за рамками уголовного процесса, осуществляется посредством выемки. В случае представления предметов и документов до возбуждения уголовного дела осуществляется истребование.

В соответствии со ст. 11 Федерального закона от 12.08.1995 № 144-ФЗ «*Об оперативно-розыскной деятельности*» её результаты могут служить поводом и основанием для возбуждения уголовного дела и использоваться в доказывании по уголовным делам в соответствии с положениями уголовно-процессуального законодательства, регламентирующими собирание, проверку и оценку доказательств.

[123] Т. е., вопрос, чем обеспечивается гарантия объективности представленных материалов, что они не были ошибочно (случайно) искажены, либо умышленно сфабрикованы?

Результаты оперативно-разыскной деятельности, оформленные надлежащим образом, могут стать полноценными доказательствами по уголовному делу в совокупности с другими доказательствами могут быть положены в основу обвинения. Для этого уголовно-процессуальное право предусматривает соответствующие способы реализации результатов оперативно-разыскной деятельности. В зависимости от конкретного оперативно-розыскного мероприятия они приобретают свой итоговый статус.

Представление доказательств является одним из способов собирания доказательств и включает в себя действия следователя (дознавателя), направленные на приобщение к материалам уголовного дела результатов ОРМ и административной деятельности, а также предметов и документов, представленных иными лицами, в качестве вещественных доказательств или иных документов.

Общим принципом остается постулат, что результаты ОРД, полученные с соблюдением требований Федерального закона от 12.08.1995 № 144-ФЗ «*Об оперативно-розыскной деятельности*», в том числе с помощью специальных программных и технических средств, могут стать доказательствами по уголовному делу, связанному с информационными технологиями, после их закрепления и проверки следственным путём в соответствии с уголовно-процессуальным законодательством.

По общей практике [22] приобщения к уголовному делу результатов оперативно-розыскных мероприятий, в том числе оперативно-технических мероприятий, осуществляется на основании постановления о представлении результатов оперативно-розыскной деятельности органу дознания, следователю или в суд для использования в доказывании по уголовным делам. При получении таких данных в электронном виде следователь или дознаватель с участием специалиста с использованием инструментальных средств может осмотреть такие материалы и составить протокол осмотра [51], в котором отражаются сведения о том, в каком виде представлены материалы, содержащаяся в них информация [62], содержит сведения о следах преступления (в т.ч. «виртуальных», цифровых), проясняет другие обстоятельства, имеющих значение для уголовного дела. Фактические данные, полученные в ходе оперативно-технических мероприятий ОРД сами по себе могут приобрести доказательное значение в соответствии со ст. 89 УПК РФ, если в результат таких ОРД содержит не только сведения об источниках фактов [50], но и конкретные материалы [86], которые соответствуют требованиям, предъявляемым к доказательствам по УПК РФ [76, 81].

В спорных ситуациях, в большинстве случаев результаты ОРД, в том числе оперативно-технических мероприятий предъявляются для проверки надзирающему прокурору. Это позволяет проверить полноту материалов, легитимность их получения, позволит использовать их органу предварительного расследования в качестве доказательной базы, и в последующем, как правило, ускорит рассмотрение дела и утверждение обвинения прокурором.

С учётом специфики компьютерных преступлений [99] в направляемых для возбуждения уголовного дела или в качестве результатов ОРД следователю (дознавателю) материалов должны содержаться:

1. сопроводительное письмо руководителя органа дознания (оперативной службы);

2. рапорт сотрудника, проводившего оперативно-розыскные и иные мероприятия;

3. документы, фиксирующие этапы проведения оперативно-розыскных мероприятий (за исключением сведений, составляющих государственную тайну);

4. протоколы наблюдений и контрольных закупок (при продаже, распространении компакт-дисков с вредоносными компьютерными программами);

5. протоколы и стенограммы прослушивания телефонных переговоров и иных сообщений (радиообмена, пейджинговых, модемных, иных), перехвата информации с иных каналов связи, свидетельствующие о неправомерной деятельности подозреваемых лиц (необходимо иметь в виду, что согласно действующему законодательству указанные оперативно-розыскные мероприятия могут проводиться только на основании судебного решения и только в отношении преступлений особо тяжких, тяжких и средней тяжести);

6. протоколы перехвата и регистрации информации электронной почты лиц, причастных к преступлению;

7. протоколы оперативного наблюдения с приобщёнными фото- и видео- кадрами;

8. материалы оперативных экспериментов;

9. протоколы изъятия образцов для сравнительного исследования с участием специалистов;

10. протоколы (акты) изъятия компьютерной техники (машинных носителей) либо отражение такого изъятия непосредственно в протоколах оперативно-розыскных мероприятий (следует обратить внимание на тот факт, что доказательства, изъятые в ходе проведения оперативно-розыскных мероприятий, в соответствии со ст. 89 УПК РФ должны отвечать требованиям, предъявляемым к доказательствам, указанным Кодексом (разъяснение соответствующих прав лицам, присутствующим при изъятии, присутствие общественных наблюдателей и т.п.);[124]

11. бумажные распечатки «тематической» информации с изъятых машинных носителей информации и информации, находившейся на жёстком диске переносного компьютера подозреваемого (при негласном снятии информации или при добровольной выдаче компьютерного оборудования);

12. материалы лабораторных исследований содержимого системных блоков и машинных носителей, изъятых у подозреваемого;

13. протоколы изъятия и осмотров финансовых документов, кассовых чеков, свидетельствующих о внесенных изменениях в базы данных компьютеров, некоторых видов кассовых аппаратов, являющихся разновидностью компьютеров;

14. протоколы использования специальных химических средств (химловушек) при фиксации использования компьютерного оборудования в целях неправомерного доступа, краж машинных носителей информации;

15. объяснения должностных и иных лиц;

16. инструкции, справки, другие документы и материалы.

Как и сказано выше авторами одним из способов процессуального закрепления доказательств может быть истребование и последующий осмотр следователем (дознавателем) материалов ОРД с последующим приобщением к уголовному делу в качестве приложения к протоколу осмотра (выемки).

[124] В противном случае доказательства, полученные таким образом не будут легитимными и не могут быть положены в основу приговора. Соответственно, теряется какая-либо целесообразность проведения судебных экспертиз по изъятым объектам.

Таким образом, можно констатировать, что возможность использования результатов оперативно-разыскной деятельности в качестве доказательств по уголовному делу, связанному с информационными технологиями, очень значима, но всегда находится в прямой зависимости от того, насколько точно эта деятельность[125] соответствует требованиям соответствующих законов (Конституции Российской Федерации, федеральному закону «Об ОРД», УПК РФ) и подзаконных актов. В этом смысле гласную и негласную оперативно-разыскную деятельность, как и её составляющие - оперативно-технические мероприятия, можно и нужно рассматривать как систему добывания и собирания уголовно-процессуальных доказательств.

3.2.2. Изменение квалификации преступлений

Некоторые вопросы изменения квалификации преступлений при получении (изучении) цифровых доказательств.

Отметим, что по результатам выявления следователем и специалистом, а также исследования экспертом доказательств в электронной форме, в том числе цифровых доказательств, а также при анализе результатов ОРД и ОТМ, опросом и допросов может возникнуть проблема выявления новых эпизодов иных преступных деяний или вопрос переквалификации преступлений в сфере компьютерной информации (компьютерных преступлений), возникающих в ходе следствия (дознания) по уголовным делам, связанным с информационными технологиями.

Юридический и фактический моменты окончания неправомерного доступа к компьютерной информации (ст. 272 УК РФ) могут не совпадать. Копирование и модификация информации, как правило, не осуществляются одномоментно. При копировании значительных объёмов компьютерных данных процесс может потребовать нескольких минут, а иногда и часов.[126] Вместе с тем, в случае, когда лицо, по независящим обстоятельствам не смогло скопировать или модифицировать заранее определённый объём информации (например, целиком заполучить интересующую его базу данных), содеянное образует оконченное преступление. Более того, даже наличие у потерпевшего системы архивного копирования данных не исключает возможности привлечения лица к уголовной ответственности за неправомерный доступ к компьютерной информации по ст. 272 УК РФ.

Несмотря на то, что умысел лица не был реализован в полном объёме, это свидетельствует лишь о фактической незавершённости деяния, в юридическом же смысле оно было окончено с момента копирования или модификации первого файла.

Неправомерный доступ к охраняемой законом компьютерной информации, осуществляемый под скрытым контролем сотрудников правоохранительных органов, следует квалифицировать как покушение на преступление, предусмотренное ст. 272 УК РФ. Критически оценим распространённую в теории уголовного права позицию, со-

[125] Её результаты, зафиксированные на материальных носителях.

[126] Поделите, например, объём в 2 ТБ = 1024*2 ГБ = 1024*1024*2 МБ ~ 2000000 МБ на характерную скорость записи обычного жёсктого диска – 80-150 Мбайт/с. Также отметим, что у большинства современных твердотельных накопителей хотя и первоначальная и пиковая скорость записи выше – до 450-800 МБ/с, после копирования относительно небольшого объёма она быстро асимтотически падает, в зависимости от модели диска, до 30 МБ/с, что оказывается даже ниже чем у обычных жёстких дисков с магнитным принципом записи.

гласно которой как оконченное преступление – создание вредоносной компьютерной программы – следует оценивать, в том числе, действия по её описанию в рукописном или машинописном виде. Отмечается, что определение целей программы, разработка её алгоритма и последующие действия по программированию правильнее оценивать как покушение на создание вредоносной программы. Создание вредоносной компьютерной программы следует считать оконченным с момента придания ей такого состояния, при котором она уже обладает соответствующим деструктивным функционалом (вредоносными свойствами) и пригодна для использования.

Распространение вредоносных компьютерных программ либо вредоносной компьютерной информации при проведении проверочной закупки образует признаки оконченного преступления, предусмотренного ст. 273 УК РФ.

В отечественной доктрине уголовного права и правоприменительной практике встречаются попытки расширительного толкования подстрекательских и пособнических действий по делам о компьютерных преступлениях имеют свое объяснение – публичное размещение информации, склоняющей или облегчающей их совершение, объективно является общественно опасным и требует надлежащей оценки. Вместе с тем, что даже при решении самых злободневных проблем нельзя законность приносить в жертву социальной необходимости, произвольно расширяя пределы действия уголовного закона. В связи с этим отечественному законодателю необходимо обратить более пристальное внимание на опыт других государств, которые пошли по пути выделения специальных норм об ответственности за подобное поведение. [75]

Верной квалификацией неправомерного доступа к компьютерной информации, совершаемого с использованием специального оборудования и (или) вредоносного компьютерного обеспечения, будет вменение сложного единичного преступления с множественностью потерпевших, характеризующегося следующими отличительными чертами:

1) направленностью посягательства на двух или более лиц;

2) причинением вреда нескольким потерпевшим в результате одного преступного деяния;

3) причинной связью нескольких последствий (в виде копирования, блокирования или уничтожения охраняемой законом компьютерной информации) с одним преступным деянием;

4) единством умысла виновного, направленного на неправомерный доступ к охраняемой законом компьютерной информации в отношении двух или более лиц. При этом специально оговаривается, что в случае сложного единичного неправомерного доступа к охраняемой законом компьютерной информации с множеством потерпевших деяние необходимо квалифицировать по ч. 4 ст. 272 УК РФ, как повлекшее тяжкие последствия.

Помимо компьютерных преступлений, рассмотрим вопросы квалификации компьютеризированных преступлений. В ряде уголовно-правовых норм (ст. 1853 УК РФ, ст. 205^2 УК РФ, ст. 228^1 УК РФ, ст. 258^1 УК РФ, ст. 280^1 УК РФ) имеется указание на совершение соответствующих общественно опасных деяний с использованием «электронных сетей». Понятие электронной сети не только не раскрывается, но и не используется Федеральным законом Российской Федерации от 27 июля 2006 г. № 149-ФЗ «*Об информации, информационных технологиях и о защите информации*». Обзор судебно-следственной практики не позволил выявить и случаи применения дан-

ного признака при квалификации конкретных преступлений, таким образом специальное указание на электронную сеть в ряду квалифицирующих признаков статей Особенной части УК РФ является следствием ситуативного и необдуманного законотворчества.

Необходимо отказаться как от формулировки «электронной сети», так и от аналога – «информационно-телекоммуникационной сети», заменив их более общей, признанной на международном уровне конструкцией «информационно-коммуникационная технология».

Нарушение неприкосновенности частной жизни по ст. 137 УК РФ следует квалифицировать действия лица, которое осуществило распространение сведений об активности другого пользователя в сети интернет без его согласия (например, распространило снимки экранов с историей браузера).

Хищения автотранспортных средств с использованием специальных радиоприёмников автосигнализаций, т. н. «код-грабберов» должны квалифицироваться по совокупности со ст. 138^1 УК РФ.

Умышленное создание на территории Российской Федерации необходимых условий для заключения соглашений о выигрыше между гражданами и субъектами (организациями), осуществляющими проведение азартных игр в сети интернет, необходимо квалифицировать по ст. 171^2 УК РФ. Юридическая оценка подобного рода действий как незаконных организации и проведения азартных игр, является возможной только при условии признания, что заключённый между сторонами субагентский договор обладает признаками притворной сделки, которая хотя формально и не нарушает закон, но на самом деле прикрывает собой сделку, совершаемую с целью, противной основам правопорядка и нравственности, – проведения азартных игр с использованием сети интернет.

Уголовно-правовая норма об ответственности за неправомерное вмешательство в работу Государственной автоматизированной системы Российской Федерации «Выборы» (ч. 3 ст. 141 УК РФ) имеет очевидные пересечения с положениями ч. 2 ст. 274^1 УК РФ. Преодоление данной конкуренции в сложившихся условиях представляется довольно проблематичным, поскольку, сопоставление санкций указанных норм позволяет сделать вывод, что общая норма об ответственности за вмешательство в работу объектов критической информационной инфраструктуры Российской Федерации должна быть замещена специальной нормой об ответственности за вмешательство в функционирование ГАС РФ «Выборы», хотя последняя предусматривает более мягкое наказание и не содержит каких-либо привилегирующих признаков. С другой стороны правила разрешения конкуренции между общей и специальной нормой предельно чётко закреплены в ч. 3 ст. 17 УК РФ. Пренебрежение требованием о преимуществе специальной нормы и квалификация содеянного как идеальной совокупности объективно породит ситуацию двойного вменения, что не допускается положениями ч. 2 ст. 6 УК РФ, именно так и должна строиться практика по делам о совершении компьютерных атак на ГАС РФ «Выборы».

Из-за массовости и гиперлатентности отдельно необходимо рассматривать проблемы квалификации мошенничества в сфере компьютерной информации (ст. 159^6 УК РФ).

Обращаясь к проблеме отграничения мошенничества в сфере компьютерной информации от мошенничества, предусмотренного ст. 159 УК РФ, введение в заблужде-

ние потерпевшего может быть следствием работы вредоносного программного обеспечения, что само по себе не обосновывает необходимость квалификации содеянного по ст. 159^6 УК РФ. Если денежные средства списывались вредоносной программой не автоматически, а перечислялись потерпевшими самостоятельно, например, в качестве оплаты несуществующих административных штрафов за просмотр порнографических материалов, содеянное подпадает под действие общей нормы о мошенничестве (ст. 159 УК РФ).

В научных кругах и у практиков включение в ч. 3 ст. 159^6 УК РФ особо квалифицирующего признака, связанного с совершением компьютерного мошенничества в отношении электронных денежных средств и средств, которые находятся на банковском счёте потерпевшего, считается в научных правовых кругах [52, 67, 68, 72] весьма дискуссионным и противоречащим теоретико-правовым основам дифференциации уголовной ответственности, т. к. из-за специфического способа мошенничество в сфере компьютерной информации изначально не предполагало возможности его осуществления в отношении обычных (бумажных) денежных средств. Таким образом, изменив редакцию статьи 159^6 УК РФ, законодатель фактически сузил действие её первой и второй части статьи 159^6 УК РФ, поэтому более перспективным направлением является установление повышенной ответственности за совершение мошенничества в сфере компьютерной информации с неправомерным сокрытием либо изменением идентификаторов оконечного оборудования пользователя информационно-коммуникационными технологиями.

Замечание. Толкование мошенничества с использованием электронных средств платежа по-прежнему должно основываться на разъяснениях, сформулированных в п. 17 постановления Пленума Верховного Суда Российской Федерации от 30.11.2017 г. № 48 «*О судебной практике по делам о мошенничестве, присвоении и растрате*», согласно которым признаки ст. 159^3 УК РФ имеют место только в случаях, когда хищение имущества осуществлялось путём сообщения уполномоченному работнику кредитной, торговой или иной организации заведомо ложных сведений о принадлежности лицу карты (с учётом изменений – электронного средства платежа) на законных основаниях, либо путём умолчания о незаконном владении им такой картой (с учётом изменений – электронным средством платежа).

Современная редакция ст. 159^3 УК РФ позволяет предположить и другой подход разрешения конкуренции уголовно-правовых норм об ответственности за хищения с банковского счёта потерпевшего, а равно в отношении электронных денежных средств.

Принимая во внимание, что модифицированная диспозиция мошенничества с использованием электронных средств платежа не содержит специального указания о способе его совершения, можно сделать вывод, что все посягательства на денежные средства граждан по-средством использования современных продуктов и систем дистанционного банковского обслуживания (электронных средств платежа) без признаков деструктивного вмешательства в их функционирование охватываются данной уголовно-правовой нормой.

При подобном толковании, хищения денежных средств граждан путём использования злоумышленниками поддельных сайтов популярных интернет-магазинов, компаний-перевозчиков, благотворительных организаций и т. п., а равно при введении потерпевших в заблуждение дистанционно (например, по телефону), следует квалифицировать уже не как общеуголовное мошенничество (как указывает о том Пленум Верховного Суда Российской Федерации в постановлении от 30.11.2017 г. № 48), а как мошенничество с использованием электронных средств платежа.

Авторы надеются, что обладая должной эрудицией и хотя бы предварительными знаниями особенной части УК РФ и комментариями к нему, наши читатели смогут достойно и самостоятельно продолжить данный параграф по другим статьям уголовного кодекса, исходя из содержания компьютерной информации и результатов процессуальных действий следователя (дознавателя) и оперативно-розыскной деятельности органа дознания.

3.2.2.1. Криптовалюты

Квалификация преступлений, совершаемых с использованием, в отношении и по поводу цифровых финансовых активов (криптовалют).

Современные исследователи [62, 124, 134-138] выделяют следующие основные группы преступлений, сопряжённых с использованием в той или иной форме цифровых финансовых активов (криптовалют):

а) преступления, в которых криптовалюта выступает средством их совершения;

б) преступления, в которых криптовалюта выступает предметом посягательства;

в) преступления, совершаемые в целях генерации (майнинга) криптовалюты.

Из общего количества изученных приговоров и обвинительных заключений по конкретным делам 2017-2021 гг. (всего 73) подавляющее большинство составляет первая группа – 64 (преимущественно по эпизодам, связанным с незаконным оборотом наркотических средств, оружия и легализацией денежных средств). Значительно меньше было выявлено дел, где криптовалюта выступала предметом посягательства – 7. Всего 2 материла были связаны с преступлениями, совершаемыми в целях майнинга криптовалюты.

В судебной практике существуют проблемы при квалификации таких преступлений. Использование лицом криптовалюты не может априорно свидетельствовать о том, что имела место легализация денежных средств. Простое распоряжение «виртуальной валютой» (в целях оплаты товаров или услуг) без намерения придания правомерного вида преступным доходам не содержит признаков состава преступления, предусмотренного ст. 174^1 УК РФ.

Замечание. Как незаконное предпринимательство (ст. 171 УК РФ) можно было бы квалифицировать осуществление лицом деятельности, связанной с обменом криптовалюты на фиатные денежные средства и наоборот, направленной на получение прибыли за счёт взимания комиссии по каждой операции. Учитывая, что получение лицензии на оказание таких услуг является невозможным по действующему законодательству, логично придти к выводу, что лицо будет нести ответственность за незаконное предпринимательство при условии, если оно осуществляло указанную деятельность без регистрации в качестве такового.

Квалификация подобных действий по ст. 172 УК РФ является ошибочной, поскольку криптовалюта не считается официально признанным в Российской Федерации денежным средством, поэтому операции с ней не могут быть квалифицированы как банковские.

Официальное отношение к цифровым деньгам в нашей стране было озвучено 27 января 2014 года Банком России, заявившим[127], что в последнее время в мире получили определённое распространение так называемые «виртуальные валюты», в частности, Биткойн. То есть, ука-

[127] Об использовании при совершении сделок «виртуальных валют», в частности, Биткойн, 27 января 2014 года, http://www.cbr.ru/press/PR.aspx?file=27012014_1825052.htm.

занные валюты, несмотря на научный интерес, были отнесены к суррогатным, а это означает, что согласно статье 27 Федерального закона «О Центральном банке Российской Федерации (Банке России)» выпуск на территории Российской Федерации денежных суррогатов запрещается.

06 февраля 2014 года в Генеральной прокуратуре Российской Федерации состоялось совещание[128] по вопросу правомерности использования анонимных платёжных систем и криптовалют на котором было всесторонне изучено положение дел и подтверждено официальное мнение: «*Получившие определённое распространение анонимные платёжные системы и криптовалюты, в том числе наиболее известная из них – Биткойн, являются денежными суррогатами и не могут быть использованы гражданами и юридическими лицами.*» А использование указанных платёжных средств со стороны юридических лиц на территории России «*будет рассматриваться как потенциальная вовлечённость в осуществление сомнительных операций в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма.*»

Статьи 128 и 141[1] Гражданского кодекса Российской Федерации в своём единстве позволяют криптовалюту относить к иному имуществу и тем самым снимают проблему квалификации деяний, в которых она выступает предметом преступления.

При квалификации посягательств на криптовалюту правоприменительные органы в качестве системной проблемы отмечают отсутствие на территории Российской Федерации органа, уполномоченного дать оценку её стоимости на конкретную дату. В настоящее время при расследовании уголовных дел установление размера причинённого ущерба потерпевшему основывается либо на заключении специалиста, либо посредством получения информации о курсе криптовалюты на время совершения преступления непосредственно через данные торговой площадки (криптобиржи).

Действия работников организации, использовавших её вычислительные мощности для вычисления (майнинга) криптовалюты, следует оценивать по ст. 274 УК РФ, как преступное нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

В июле 2022 г. Госдума приняла Федеральный закон от 14.07.2022 № 292-ФЗ о внесении изменений в отдельные законодательные акты Российской Федерации, в том числе и в Федеральный закон от 31 июля 2020 года № 259-ФЗ «*О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации*» (в быту «*О цифровых финансовых активах*»). После изменений последний вводит понятие цифровой валюты, но запрещает её оборот на территории России и запрещает чиновникам владеть ею.

В ноябре 2022 г.[129] группа депутатов, среди которых были председатель думского комитета по финрынку Анатолий Аксаков и член комитета Госдумы по экономической политике Сергей Алтухов, внесла в Думу законопроект «*О правовом регулировании деятельности по майнингу*». После чего Центральный Банк (ЦБ) России подтвердил свою позицию «В целом мы придерживаемся позиции о недопустимости оборота цифровой валюты на территории РФ», но концептуально поддержал законопроект о правовом регулировании майнинга. ЦБ считает, что в рамках экспериментально правовых режимов при условии совершения сделок с криптовалютой через уполномоченную ор-

[128] См. http://www.genproc.gov.ru/smi/news/genproc/news-86432/.

[129] См. новость от 07 декабря 2022 г. Центробанк поддержал легализацию криптовалюты в России. Но на своих условиях. [Электронный ресурс], https://www.cnews.ru/news/top/2022-12-07_tsentrobank_podderzhal_legalizatsiyu. (Дата обращения: 10.01.2023).

ганизацию, «допускается возможность снятия таких ограничений», также полученная цифровая валюта должна продаваться исключительно на иностранных биржах и только нерезидентам.

3.2.2.2. Нейросетевые аудио- и видео-фильтры

Узнай врага в лицо.
Кто предупреждён, тот вооружён!

Квалификация преступлений, совершённых (совершаемых) с использованием нейросетевых (нейронных) аудио- и видео-фильтров реального времени.

Для осуществления правильной квалификации преступлений, совершённых с использованием указанной в заголовке данного параграфа «новомодной» информационной технологии, рассмотрим подробнее её саму, а также возникшие предпосылки к её преступному применению.

Исторически в вопросах, связанных с информационной безопасностью, в общем случае выделяют три основных вида угроз [49, стр. 444], которые существуют в компьютерных и информационных системах, прослеживаются в большинстве нормативных документов и от которых создают и используют средства защиты:

угроза целостности	,	угроза конфиденциальности	и	угроза доступности.

Все другие существующие угрозы (как считалось ранее) есть комбинации этих трёх. Все рассматриваемые модели нарушителей в системах также ориентированы на использование различных комбинаций указанных трёх видов угроз.

Пример угрозы целостности: мошенники на вашем счету в банке взяли и вместо 100 рублей каким-то образом записали 0. Нарушена целостность данных, хранящихся в банковском компьютере.

Пример угрозы конфиденциальности: вы приготовили сюрприз жене и сделали заказ в службе доставки подарков. База заказов стала доступной через интернет, и ваша супруга узнала о готовящемся сюрпризе.

Пример угрозы доступности: перед Новым годом, 31 декабря, Вы решили заказать букет цветов по телефону в интернет-магазине, но не смогли туда дозвониться по причине большого числа желающих и занятости телефонных линий. Необходимый вам сервис оказался недоступен.

Однако, жизненное применение информационных технологий мошенниками, и, как следствие, возбуждаемые уголовные дела против них, показали, что пустующая и не описанная в теории область на практике быстро заполнилась четвёртым видом угроз:

угроза авторства цифровых данных (репутационные риски, угроза достоверности)

Это довольно новый тип угроз серьёзно не воспринимаемый большинством специалистов, поскольку реализуется вне компьютера жертвы. Например, в сети выкладывается какой-либо документ, якобы от автора X, при этом подписанный его электронной подписью. В случае нарушения авторских прав X будет тратить силы и время на доказательство своей непричастности. Также данный вид угроз легко применим к различным цифровым деньгам с распределённым механизмом подтверждения транзакций, например на основе технологии *block chain*. Естественно, что операционные системы компьютеров и мобильных устройств защищать пользователей от угрозы авторства пока не могут, но с течением времени вопрос будет становиться более актуальным.

На момент подготовки к изданию данного учебного пособия усилились предпосылки к использованию вариаций угрозы авторства, связанные с тем, что в полной мере при хранении данных в распределённых системах (как и по отношению к передаваемой информации или находящейся на отчуждаемых машинных носителях) средства имитозащиты не применяются вовсе, так как не предусмотрены разработчиками, либо используемые алгоритмы криптографически слабы, либо содержат ошибки в реализациях. Также срабатывает эффект новизны проблемы в купе с ригидностью людей, проживших много лет в «аналоговом» мире и системах без дополнительной проверки авторства.

В обществе за последнее столетие сформировалось устойчивое мнение, что подделывать аудио и видео (фото, кино) записи невозможно, а если и возможно (например в радиостудиях при создании передач или киностудиях при создании художественных фильмов), то это очень сложно, долго и затратно, то есть не под силу ни отдельным преступникам, ни большим преступным группам.

Развитие аппаратной составляющей компьютерной техники и науки в области программных реализаций различных видов нейронных сетей создало новые возможности, например, просмотр видеофильмов с одновременным (т. е. выполняемым «на лету», в режиме реального времени) синхронным машинным переводом (дублированием) на другой язык. Технология на основе специальной созданной нейросети распознаёт произносимую в фильме речь, переводит на другой язык и воспроизводит, укладываясь при этом в неуловимую ухом человека задержку до 250 мс.

Далее, указанную технологию применяют не в отношении записанного и статичного фильма (видеофрагмента), а в отношении живой видеотрансляции. Если у видео отключить картинку, то останется только симплексный аудиоканал. С помощью другой нейросети заранее определяется тембр и звуковой окрас требуемого голоса (достаточно нескольких секунд), перенастраивается звук на выходе аудиофильтра первой сети. Таким образом, получается нейронный аудиофильтр, подстраиваемых под голос любого человека. Далее, мошенники определяют пары из знакомых и узнающих друг друга по голосу абонентов и действуют как известные пранкеры «Вован и Лексус», только вместо безобидных розыгрышей «С Новым годом!» совершают действия подпадающие, например под ст. 128.1 «Клевета», ст. 159 «Мошенничество» и др. УК РФ.

Подобные фильтры могут использоваться не только в отношении обмана людей, но и в отношении обмана систем с удалённой биометрической идентификацией.

При сочетании указанной технологии с уязвимостями технологий связи, в том числе и закрытых (офисных, местных) АТС открывается широкое поле для возможных преступлений.

В сочетании с возможностями других искусственных нейронных сетей (по ведению голосовой беседы) возможно совершение десятков тысяч звонков, если не миллионов за короткий период времени. Звучит как фантастика, но одна программа запросто сможет за несколько минут позвонить сразу всем учащимся школьникам одной школы и голосом их родителей сказать разными словами и в разных формах, что надо срочно уйти с уроков и пойти домой.

Применение видеофильтров происходит не менее эффектно. Вспоминается прошлогодний (2022 г.) случай, когда в эфире известного телеканала был произведён online-видеозвонок через учётную запись мессенджера пресс секретарю одного из политиков, где ему были заданы относительно безобидные вопросы. После завершения связи внимание зрителей было обращено не на ответы на вопросы, а на тот факт, что цвет рубашки и галстука были выбраны собеседником под тона флага страны «X», а не «Y». В действительности цвета рубашки и галстука были совсем другие, а о том, что зарубежное средство видеосвязи использовало специальный нейросетевой видеофильтр сообщено не было.

Фактически, технология Vall-E[130] [131] способна сделать прорыв в синтезе аудио и видеофильтров, сродни тому, как в 2001 году опубликованный алгоритм Виолы-Джонса[132] качественно и навсегда изменил индустрию распознавания лиц на изображениях.

В будущей судебной практике наверняка будут сложности при квалификации деяний связанных с использованием нейросетевых аудио- и видеофильтров при совершении преступлений, поэтому правоохранительные органы, в упреждающем порядке, в соответствии с Указами Президента Российской Федерации от 09 мая 2017 года № 203 «*О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы*» и от 10 октября 2019 года № 490 «*О развитии искусственного интеллекта в Российской Федерации*», должны среди первых быть готовы к тому, что подобные технологии служат инструментом совершения преступлений, а также быть готовыми к применению ответных мер, например разрабатывать встречные методы применения искусственного интеллекта для обнаружения подобных обманов (fake'ов).

[130] См. новость от 10 января 2023 г. Microsoft создала инструмент для подделки голоса любого человека, включая эмоции и тон. [Электронный ресурс], https://www.cnews.ru/news/top/2023-01-10_microsoft_sozdala_ii-sistemu. (Дата обращения: 10.01.2023).

[131] См. *C.Wang, S.Chen, Y.Wu* и др. Neural Codec Language Models are Zero-Shot Text to Speech Synthesizers [Электронный ресурс], https://arxiv.org/pdf/2301.02111.pdf. (Дата обращения: 10.01.2023). Для выполнения синтеза человеческого голоса функции Vall-E достаточно трёхсекундного образца речи, особенности которой необходимо имитировать, а также текстового сообщения, которое будет преобразовано в аудиоформат. Также исследователям с разным успехом удалось имитировать эмоции: злость, сонливость, изумление и отвращение.

[132] См. Viola, P.; Jones, M. (2001). "Rapid object detection using a boosted cascade of simple features" [Электронный ресурс], https://web.archive.org/web/20210125234726/http://www.hpl.hp.com/techreports/Compaq-DEC/CRL-2001-1.pdf, (Дата обращения: 10.01.2023).

3.3. Особенности допросов экспертов и специалистов в суде

3.3.1. Не было бы так смешно, если не было бы так грустно

Вопросы опровержения доводов специалиста и эксперта в суде при использовании цифровых доказательств.

Всё большее количество преступлений совершается и, соответственно, раскрывается с использованием компьютерной техники, поэтому компьютерная экспертиза, исследование и осмотр материалов, полученных в ходе проведения оперативных и следственных действий, являются неотъемлемой частью доказательственной базы, представляемой затем в судебных заседаниях.

Практический опыт показывает, что наличие у специалиста знаний и навыков проведения компьютерных экспертиз должно сочетаться с умением быть убедительным при выступлении в суде[133]. Зачастую эксперты (специалисты), впервые попадая на судебные слушания, испытывают стресс и растерянность, так как оказываются в незнакомой для них обстановке. Вместе с тем от их показаний может зависеть исход уголовного дела. Поэтому, на наш взгляд, практикующим подразделениям необходимо регулярно направлять своих сотрудников[134] в качестве слушателей на открытые судебные заседания (особенно при заслушивании экспертов и специалистов в области компьютерных технологий) с целью изучения возможной стратегии поведения стороны защиты, а также слабых и сильных сторон в выступлениях экспертов (специалистов). Полученную информацию в последствии следует доводить до всего личного состава подразделения, проводящего компьютерные экспертизы, исследования и осмотры.

Рассмотрим несколько конкретных ситуаций, произошедших в ходе судебных слушаний, о которых авторам рассказали сами их участники. Во избежание всевозможных нарушений прав граждан, общества и государства стенограммы и рассказы специалистов и иных участников судопроизводства приведены в литературной обработке авторов пособия.

[133] Бывают случаи, как в поговорке: не важно что говориться, важно каким тоном.

[134] Это также в полной мере относится и к студентам (слушателям) старших курсов профильных высших учебных заведений.

3.3.1.1. Сплетни и разговоры ни о чём

В ожидании начала судебных слушаний представители стороны обвинения и защиты, обвиняемый и его родственники, а также эксперт находились в холле перед залом, в котором должно было проводиться судебное заседание. Прокурор и эксперт, как оказалось ранее по службе знакомые между собой, разговаривали на отвлечённые темы (например, шутили или «вспоминали былое»), не имевшие отношения непосредственно к судебному заседанию. Спустя некоторое время адвокат, обвиняемый и его родственники стали демонстративно утверждать, что прокурор оказывает давление на эксперта. При этом производилась видеосъёмка. Адвокат требовал немедленного составления протокола. Порядок удалось восстановить только после прибытия в холл группы судебных приставов.

Данный инцидент имел, скорее, психологический эффект, так как доказательств давления на эксперта представлено не было, но если бы, например, адвокату удалось зафиксировать разговор прокурора и эксперта, непосредственно касающийся проведённой им экспертизы, или какой-либо обмен бумагами, то последствия как для прокурора, так и для эксперта были бы значительно тяжелее.

Мораль. Важно уяснить, что прокурор и эксперт (специалист) не должны разговаривать, обмениваться чем-либо хоть фотографиями с пляжа, хоть документами и бумагами на глазах у стороны защиты, обвиняемого и посторонних людей.

3.3.1.2. Кто ясно мыслит, тот ясно излагает свои мысли

Во время судебного слушания проводился допрос специалиста, участвовавшего в осмотре компьютерных носителей информации. В ходе повествования он последовательно приближался к одному из ключевых моментов – описанию признаков загрузки информации с использованием регистрационной записи обвиняемого в один из интернет-сервисов. Адвокат, в свою очередь, начал утверждать, что все пользователи обладают регистрационными записями и различными наборами приложений, поэтому доводы специалиста не имеют непосредственного отношения к описываемой ситуации.

В результате адвокату удалось воспрепятствовать последовательному изложению специалистом выявленных им признаков. В то же время прокурор и судья в силу отсутствия у них соответствующих знаний не смогли уяснить истинную причину совершённых специалистом действий.

Мораль. В ходе судебных заседаний необходимо чётко придерживаться линии повествования и внимательно относиться к ключевым моментам.

3.3.1.3. А была ли инструкция от прокурора?

Во время судебного заседания заслушивались показания специалиста. При этом адвокат, ссылаясь на плохое качество имеющейся у него копии материалов дела, попросил дать ему возможность ознакомиться с оригиналом, находившимся на кафедре, за которой стоял специалист. Увидев лист бумаги с записями специалиста, он потребовал разъяснить, не является ли это инструкцией от прокурора по поводу ответов на поставленные вопросы. В результате стало очевидным, что единственной целью прибли-

жения адвоката к кафедре была проверка содержимого листа бумаги с надписями, который он заметил у специалиста.

Специалист пояснил, что его записи носят личный характер и что иметь при себе подобные материалы допустимо.

Мораль. Из приведённого примера следует, что в суде эксперт (специалист) не должен иметь при себе бумаги, написанные не им, а уж тем более «тезисы» прокурора, особенно с планируемыми вопросами и заготовленными ответами на них.

3.3.1.4. Лучше тупой карандаш, чем острая память

Во время судебного слушания сторона защиты попросила специалиста подтвердить присутствие при осмотре понятых и указать, видел ли он их. Специалист ответил утвердительно на оба вопроса. Далее адвокат, заметив, что фамилия одного из понятых не склоняется (например, заканчивается на «-ко», как Порошенко), попросил специалиста уточнить пол свидетеля (имя и отчество которого заведомо не произносились). Отвечая на этот вопрос специалист допустил ошибку, тем самым дал основания усомниться в законности проведения процессуальных действий.

Мораль. Эксперту (специалисту) необходимо по возможности заранее прорабатывать подготовленные им в рамках соответствующего уголовного дела заключения и протоколы осмотра, в которых он принимал участие, не утверждать, что хорошо запомнил понятых, а затем ошибаться, ссылаясь на давность события, плохую память на лица, высокую загруженность и т. д.

3.3.1.5. Говорите правду и только правду...

... но, не обязательно всю.

Во время судебного слушания сторона защиты поинтересовалась у специалиста, насколько тщательно им просматривались обнаруженные графические файлы и осуществлялось ли это действие в отношении каждого файла в отдельности (всего было обнаружено более 6000 графических файлов). Специалист сказал, что каждый файл просматривался тщательно. Тогда адвокат заметил, что согласно протоколу осмотр проводился в течение приблизительно 3-х часов и подробный просмотр 6000 графических файлов и подготовка протокола за это время невозможны. В результате правильность составления протокола осмотра была поставлена под сомнение.

Мораль. Эксперту (специалисту) необходимо обращать существенное внимание на проставляемые в заключениях (протоколах осмотра) даты и время проведения экспертиз/исследований/осмотров. Важно, чтобы они соответствовали реальным трудозатратам на выполненные действия. В описанном же выше примере целесообразно было сразу пояснить, что специалистом был обеспечен доступ к графическим файлам, однако их непосредственным осмотром занимался следователь, качество работы которого специалистом не оценивалось.

3.3.1.6. Гладко было на бумаге, да забыли про овраги

«Чисто писано в бумаге, да забыли про овраги, как по ним ходить.» Л.Н. Толстой

Во время судебного слушания сторона защиты поинтересовалась у специалиста, с помощью какой аппаратуры производилась распечатка прилагаемых материалов, и, получив в качестве ответа указание на служебный принтер, спросила, почему последний не указан среди использованной в ходе осмотра техники. В результате возникла угроза признания протокола осмотра неправильно оформленным.

Мораль. Эксперту (специалисту) в подготавливаемых документах следует приводить весь использованный им инструментарий (если это не приведет к разглашению сведений, составляющих государственную тайну, в таком случае, необходимо устанавливать соответствующий гриф секретности на протокол и требовать закрытого судебного заседания).

3.3.1.7. В своём глазу бревна не увидел

Во время судебного слушания сторона защиты спросила эксперта, кто инструктировал его об ответственности за дачу заведомо ложного заключения, правах и обязанностях. Эксперт ответил неверно, в результате чего заключение эксперта было признано недействительным.

Мораль. Эксперту (специалисту) нужно чётко знать положения нормативно-правовых актов, регулирующих его деятельность в качестве эксперта или специалиста.

3.3.1.8. Внимание к мелочам рождает совершенство...

..., а вот совершенство уже не мелочь. (Микеланджело Буонарроти)

Во время судебного слушания сторона защиты поинтересовалась у специалиста, почему время, зафиксированное в отчёте использованной программы (например, «Мобильный криминалист»), не укладывается во временной промежуток проведения осмотра, указанный в протоколе, поставив тем самым под сомнение правильность проведения осмотра. Специалисту пришлось разъяснять, что это связано с настройками конкретной программно-аппаратной среды, примененной для запуска программы, и в этом случае заданное время не соответствует действительному. Настоящее же время может быть подтверждено понятыми.

Мораль. Эксперту (специалисту) нужно добиваться отсутствия противоречий во всех подготавливаемых им документах.

Важно. Во время судебных слушаний может возникнуть также и обратная ситуация, когда сторона защиты на коммерческой основе привлекает сторонних специалистов в области информационных технологий, которые подготавливают «нужные» ей заключения.

В этом случае необходимо проверить легальность использования такими специалистами программного обеспечения (ПО) для проведения компьютерных экспертиз (обычно оно являет-

ся дорогостоящим, а его нелегальное использование представляет собой уголовное преступление).

Так, например, специалист коммерческой организации указал, что для проведения исследования применялось дорогостоящее программное обеспечение.

Сторона обвинения запросила у официальных дилеров этого ПО информацию о легальности его использования конкретным специалистом. Оказалось, что прав на применение данной программы у коммерческой организации не было. Письмо с соответствующим ответом официального дилера прокурор представил в суде. В результате специалист коммерческой организации больше на слушаниях не присутствовал, и сторона защиты потеряла возможность проводить с ним консультации в это время.

3.3.1.9. Мораль всех ~~басен~~ случаев такова

Негативное влияние на исход судебных слушаний для стороны обвинения оказывает зачастую полная неграмотность (или её умелая имитация) судей и прокуроров в области информационных технологий. Например, в ходе одного из слушаний судья был готов принять решение в пользу стороны защиты, которая утверждала, что преступные действия не могли быть совершены с использованием компьютера, так как на нём обнаружены файлы с именами, отличающимися от имени обвиняемого. Именно это «доказательство» невиновности последнего использовала сторона защиты. Только разъяснения специалиста помогли не допустить развития столь абсурдной ситуации.

Зачастую прокуроры не могут грамотно сформулировать вопросы во время допроса эксперта (специалиста), из-за чего возникает потребность в присутствии лица с соответствующим образованием для их консультирования.

В большинстве правоохранительных органов и специальных служб России имеется опыт использования сотрудников для «сопровождения» судебных слушаний в качестве консультантов прокурорских и следственных работников, но из-за высокой загруженности сотрудников-специалистов по информационным технологиям широкое её применение практически затруднительно.

Всё изложенное выше только подчёркивает необходимость усиления подготовки экспертов и специалистов для участия в судебных слушаниях. При этом одним из наиболее простых и в то же время плодотворных способов является их регулярное присутствие на открытых заседаниях в качестве слушателей, в т. ч. по разнарядке.

3.3.2. Использование видеоконференцсвязи

Особенности производства допроса эксперта посредством использования видеоконференцсвязи.

Допрос, связанный с внедрением результатов науки и техники в деятельность правоохранительных органов с учётом их адаптации под цели раскрытия и расследования преступлений в условиях цифровизации и информатизации современного общества сохраняет перманентную актуальность. Сжатые сроки предварительного расследования, предусмотренные ныне действующим УПК РФ, предопределяют необходимость оптимизации деятельности следователя по производству тех или иных следственных

действий. Одним из самых распространённых и в то же время наиболее сложных вербальных следственных действий является допрос.[135]

В свою очередь, допрос эксперта в отличие от допроса подозреваемого, обвиняемого, свидетеля или потерпевшего характеризуется особой сложностью, обусловленной тем, что следователю, не обладающему, как правило, специальными знаниями в области конкретной науки, техники, искусства или ремесла, необходимо допросить эксперта по существу проведённого им исследования. В этой связи тактика планирования и производства такого следственного действия как допрос эксперта заслуживает особого внимания, о чём свидетельствуют многочисленные публикации учёных, посвящённые данной проблематике.[136]

Однако в настоящей работе нами будут рассматриваться преимущественно пути оптимизации производства допроса эксперта, которые могут быть реализованы посредством проведения данного следственного действия в виде видеоконференцсвязи (далее – ВКС) между участниками допроса, а также тактические особенности, обусловленные спецификой использования ВКС при производстве рассматриваемого следственного действия.

На сегодня в УПК РФ отсутствуют нормы, предусматривающие возможность проведение допроса при помощи ВКС тех или иных участников уголовного судопроизводства, в том числе эксперта. Вместе с тем, в июне 2021 года сенаторами Российской Федерации А. В. Кутеповым и В. А. Пономарёвым на основании ст. 104 Конституции Российской Федерации была проявлена законодательная инициатива, заключающаяся в предложении внесения изменений в УПК РФ[137], позволяющих осуществлять допрос различных участников уголовного судопроизводства при помощи использования ВКС. В свою очередь, указанный законопроект за исключением небольших замечаний был поддержан Правительством Российской Федерации.[138]

Следует отметить, что в следственной практике на протяжении нескольких лет успешно используются возможности предъявления для опознания по видеоизображениям, а также при помощи ВКС, особенно это становится актуальным, если опознающий находится в удалённом от места проведения следственного действия регионе Российской Федерации.[139]

Таким образом, несмотря на большое количество вопросов, которые будут возникать в ходе проведения данного следственного действия, проводимого посредством ВКС, целесообразность и необходимость введения вышеуказанных изменений в УПК РФ для соблюдения разумных сроков предварительного расследования и оптимизации

[135] Тактика допроса по делам о компьютерных преступлениях является слишком сложной и малоизученной проблемой и планируется к изучению в дальнейшем.

[136] См., например: *Захарова В. А.* Допрос эксперта: рекомендации и ошибки // Российский следователь, № 5, 2021. – С. 2-24; *Ахмедшин Р. Л.* Актуальные аспекты тактики допроса эксперта // Вестник Том. гос. ун-та. – Право. 2014, № 4 (14) – С. 15-21; *Гришин А. В.* Особенности допроса эксперта в суде // Евразийская адвокатура, 2015, № 1 (14). – С. 26-30.

[137] Официальный сайт Системы обеспечения законодательной деятельности [Электронный ресурс]. – Режим доступа: https://sozd.duma.gov.ru/bill/1184595-7 (дата обращения: 07.11.2021)

[138] См. *Саркисян А. А.* Правовое регулирование цифровизации судебно-экспертной деятельности / А. А. Саркисян // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2022. – № 2(90). – С. 157-160. – DOI 10.17803/2311-5998.2022.90.2.157-160. – EDN EOAWOY.

[139] См. *Ильин Н. Н.* К вопросу о предъявлении лица для опознания по видеоизображениям // Вестник дальневосточного юридического института МВД России, № 1 (38), 2017. – С. 119–126.

производства такого следственного действия как допрос, по нашему мнению, не вызывает сомнения.

Как известно, допрос – это следственное действие, в процессе которого следователь получает показания от лица, обладающего сведениями, имеющими значение для расследуемого дела. Допрос представляет собой наиболее распространённый способ получения ориентирующей и доказательственной информации, когда речь заходит о таких процессуальных фигурах как подозреваемый, обвиняемый, свидетель или потерпевший. Однако при допросе эксперта следователь преследует иные цели, кардинально отличающиеся от целей допроса других участников уголовного судопроизводства. Во многом такое положение вещей объясняется кругом обстоятельств, которые следователь может установить путём допроса эксперта и которые в криминалистической литературе получили называние – предмет допроса.

Предметом допроса эксперта, исходя из смысла ст. ст. 205, 282 УПК РФ могут служить выводы эксперта по поставленным перед ним вопросам, а также методика проведённого им исследования. В ходе допроса эксперта, согласно ч. 2 ст. 80 УПК РФ могут быть выяснены только сведения, разъясняющие или уточняющие данное им заключение. Однако зачастую именно во время допроса эксперта выясняются обстоятельства, свидетельствующие о некомпетентности эксперта, что служит основанием назначения повторной экспертизы. Наиболее распространённые случаи встречаются при производстве компьютерно-технической экспертизы, что объясняется сложностью выбора соответствующего эксперта, обусловленного многогранностью специализаций в области информационных технологий.

Целью допроса эксперта, исходя из положений ч. 2 ст. 80, ч. 1 ст. 86, ст. 87 и 88 УПК РФ, является получение новых доказательств в виде показаний эксперта, а также оценка относимости, допустимости и достоверности данного ранее экспертом заключения, проверка не противоречит ли заключение эксперта иным имеющимися по уголовному делу доказательствам.

В ходе предварительного расследования допрос эксперта проводится по правилам, установленным ст. 164, 166, 167, 187–190, 205 УПК РФ, также допрос эксперта может быть осуществлен на стадии судебного разбирательства в соответствии со ст. ст. 282, 283 УПК РФ. Инициатором проведения данного процессуального действия могут быть следователь или суд.

Нужно отметить, что передача экспертом заключения в следственные или судебные органы и необходимость в проведении допроса эксперта часто значительно разнятся во времени. Зачастую немаловажную роль играет расположение органа, назначившего экспертизу, и эксперта в различных субъектах Российской Федерации, что в ряде случаев приводит к значительным потерям во времени и финансовым трудностям, связанным с прибытием эксперта в место расположения следственного или судебного органа. Особенно это стало актуальным с успешным развитием института частных экспертов, проводящих экспертизы не только для гражданского, но и для уголовного судопроизводства. Наиболее ощутимо это для наукоёмких видов экспертиз, таких как судебная компьютерно-техническая, основные кадровые и технологические ресурсы для производства которой в основном расположены в крупных городах Российской Федерации с развитой научной и технологической базой.

Представляется, что возможность проведения допроса при помощи ВКС в таких случаях позволяет существенно снизить значительные временные и экономические за-

траты. Однако, как отмечалось нами ранее, ни в рамках предварительного расследования, ни в рамках судебного разбирательства в соответствии с ныне действующими нормами УПК РФ не предусмотрено проведение допроса эксперта при помощи использования ВКС. Полагаем, что проведение допроса эксперта при помощи использования ВКС не только бы позволило избежать излишних финансовых затрат, связанных с расходами на командировку и проживание эксперта по месту пребывания, но и позволило бы:

- во-первых, соблюсти сроки разумного уголовного судопроизводства, так как в продлении сроков предварительного расследования по рассматриваемому основанию отпала бы необходимость;
- во-вторых, оптимизировать в первую очередь деятельность государственных судебно-экспертных учреждений, имеющих высокую загруженность, увеличивающуюся в виду дальних и длительных командировок экспертов, вызванных на допрос следователем или судом для дачи показаний.

Конечно же, в случае проведения допроса посредством ВКС возникает ряд проблем, основной из которых становится идентификация допрашиваемого и обеспечение информационной безопасности, исключающей несанкционированный доступ третьих лиц во время допроса, проводимого посредством ВКС. Как полагаем, здесь существует несколько решений, взаимодополняющими друг друга:

- создание информационно-компьютерной системы, аналогичной автоматизированным информационным системам федеральных арбитражных судов (www.arbitr.ru[140]), в которой идентификация допрашиваемого лица будет проводиться через систему «Госуслуги»;
- контроль личности допрашиваемого и обеспечение его подключения к внутренней системе ВКС поручить местному следственному органу в соответствии со ст. 38 УПК РФ;
- двойной контроль личности допрашиваемого по двум вышеприведённым основаниям.

В случае поручения местному следственному органу проведения контроля личности допрашиваемого останется вопрос целесообразности данного действия, которое по мнению наших оппонентов, не будет отличаться от поручения для проведения допроса эксперта. Мы же считаем, что в данном случае с тактической точки зрения преимущества на стороне предложенной нами схемы. Это связанно с имеющейся в такой ситуации возможностью для следователя, ведущего расследование, имея перед глазами экспертное заключение и владея уже собранной доказательственной базой, скорректировать заранее подготовленные вопросы и сформулировать новые, появившиеся в процессе допроса. Более того, заключение эксперта по ряду составов преступлений, предусмотренных УК РФ, выступает чуть ли не единственным источником криминалистически значимой информации, позволяющим следователю принять решение о возбуждении или отказе в возбуждении уголовного дела.

Например, по делам, связанным с проявлением словесного экстремизма или терроризма в соответствии п. 2.3. Приказа СК России «*О мерах по противодействию экстремистской деятельности*» указывается необходимость назначения судебной экспертизы: «*при установлении в*

[140] Официальный сайт Федеральных арбитражных судов Российской Федерации. [Электронный ресурс] – Режим доступа: http://www.arbitr.ru (дата обращения: 08.11.2021).

ходе процессуальной проверки очевидных признаков преступления принимать решение о возбуждении уголовного дела с последующим получением заключения эксперта»[141].

Ввиду сложности и особой концептосферы, в частности религиозного дискурса, следователю фактически невозможно без результатов производства лингвистической экспертизы оценить имеющиеся у него материалы и дать им правовую квалификацию. Наряду с этим как свидетельствуют результаты обобщения следственной практики[142] ввиду многочисленного использования в тексте заключения специальных филологических терминов и определений следователю очень сложно оценить полученное по результатам экспертизы заключение, вследствие чего возникает потребность в допросе эксперта в целях устранения неточностей. При этом в соответствии с ч.3. ст. 144 УПК РФ сроки рассмотрения сообщения о преступлении не могут превышать 30 суток. Наряду с этим, по указанной выше категории дел, очень сложно найти компетентного эксперта ввиду незначительного количества сведущих лиц, способных полно, всесторонне, научно-обоснованно и объективно осуществить исследование материалов религиозного дискурса в целях установления факта наличия/отсутствия в них лингвистических признаков призывов, оправдания терроризма, вербовки и т. д.

Зачастую эксперт, осуществлявший производство данной экспертизы, территориально расположен в отдалённом от дислокации следователя субъекте Российской Федерации, вследствие чего его допрос в вышеприведённой ситуации в установленные в ст. 144 УПК РФ сроки в большинстве случаев невозможен, что оказывает негативное влияние на оценку имеющего у следствия заключения, а также на принятие решения о правовой квалификации соответствующих материалов.

Говоря о преимуществах допроса эксперта при помощи ВКС, считаем необходимым уделить особое внимание возникновению причин допроса эксперта и предложить следующие тактические приёмы, делающие его более приоритетным.

В соответствии со статьями 205 и 282 УПК РФ причинами допроса эксперта могут выступать в первую очередь недостаточная ясность заключения в целом или его частей (формулировок, терминов, структурных частей и др.) как следователю и суду, так и участвующим в деле лицам, ознакомленным с заключением эксперта. Часто это связано со сложностью понимания языка эксперта, наличием большого числа специфических терминов и логических выкладок, поддержанных формулами.[143] Такое положение вещей влечёт за собой невозможность оценки логической структуры заключения и обоснованности выводов.

В случае допроса при помощи ВКС у следователя или суда появится возможность не только перечитывать повторно вместе с экспертом заключение, а использовать средства визуального отображения, демонстрируя конкретные части этого заключения в которых возникли у правоприменителя сомнения. При этом у эксперта также появляется возможность не просто отвечать на поставленные вопросы, а сопровождать ответы схемами, чертежами, формулами и делать их визуально доступными сразу для всех лиц, участвующих в уголовном процессе.

[141] Приказ Следственного комитета России от 12.07.2011 № 109 (ред. от 27.03.2013) «О мерах по противодействию экстремистской деятельности» // СПС «Консультант Плюс».

[142] Материалы из архивов 2015-2020 гг. Следственных управлений и отделов Следственного комитета России.

[143] См. например: *Россинская Е. Р.* Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе. Изд. 4 перераб. и доп. – М.: Норма, 2019. – С. 288-292. Помните народную мудрость: «Каждая встречающаяся в книге формула уменьшает вдвое число её читателей.»

В результате могут быть сняты многие вопросы и не возникнет необходимость в назначении дополнительной экспертизы по причине недостаточной ясности заключения эксперта в соответствии ч.1 ст. 207 УПК РФ, что, несомненно, сэкономит и временные и финансовые ресурсы. Считаем также необходимым отметить, что при проведении допроса в режиме ВКС может отпасть необходимость назначения повторной экспертизы. Поскольку в практике нередки случаи, когда во многом подобное назначение обусловлено тем, что следователь, не обладая специальными знаниями, далеко не всегда способен полно и всесторонне оценить научную обоснованность, полноту, объективность заключения эксперта.

Допрос эксперта посредством ВКС, проведённый до назначения повторной экспертизы с участием специалиста, позволяет путём соответствующих разъяснений и визуализации логических связей, предоставления на обозрение экспертной методики и иных научных материалов, решающих промежуточных выводов, которые легли в основу сделанного им итогового вывода, устранить заблуждения следователя относительно наличия оснований назначения повторной экспертизы, а, следовательно, избежать неоправданных затрат времени, сил и средств, связанных с её производством.

С другой стороны, в случаях, когда возникает потребность в допросе экспертов, осуществлявших производство комплексной или комиссионной экспертизы, как правило, на допрос является один из экспертов, осуществлявших производство конкретной экспертизы. Однако в литературе ранее было высказано мнение о возможности привлечения эксперта другой специальности к допросу данного эксперта.[144] Подобная тактика в процессе допроса позволяет всем участвующим в допросе экспертам указать, например, на неправильное толкование своих выводов. Для подобных вопросов нет необходимости вызывать экспертов в суд или в место дислокации следователя. Эксперты могут находиться в различных регионах и принимать участие в допросе, практически не отрываясь на длительный срок от выполнения других профессиональных обязанностей.

Ещё одним неоспоримым достоинством допроса, проводимого при помощи ВКС, является возможность его записи в режиме реального времени с использованием функциональных возможностей компьютерно-цифровых технологий с дальнейшим приобщением данных материалов к уголовному делу. В этом случае будет решена проблема надлежащего толкования допрашивающим слов эксперта. У следователя или суда всегда будет оставаться возможность просмотреть запись в полном объёме и провести анализ полученной информации в совокупности с другими материалами дела. В отличие от аудио-/видеозаписи допроса, все слова эксперта сразу будут подтверждаться текстовыми и графическими материалами, являющимися частью методики или пояснений с выдержками и научными обоснованиями.[145] В созданном таким образом протоколе допроса будут учтены все требования к такого рода процессуальным документам.[146]

Как видим, у допроса, проведённого посредством ВКС, существует достаточное количество положительных факторов, которые ведут к оптимизации предварительного

[144] См. *Дулов А. В.* Права и обязанности участников судебной экспертизы // Минск: изд-во Мин-ва высшего, сред. спец. и проф. обр-ния БССР, 1962. – С. 310.

[145] Главное, чтобы форма не заменила содержание и готовиться эксперту к предстоящему сеансу ВКС не пришлось больше, чем если бы он на несколько минут вживую посетил зал судебных заседаний и ответил на вопросы.

[146] См. *Зинин А. М.* Криминалист в следственных действиях: учебно-практическое пособие. – М.: Экзамен, Право и закон, 2004. – 144 с.

расследования и судебного разбирательства. Однако, существуют и сложности, сопровождающие данное следственное/судебной действие.

Приняв решение о производстве допроса эксперта, следователь приступает к его подготовке, которая включает: собирание исходных данных для допроса и его тактическое обеспечение. При подготовке к ВКС допросу, так же, как и к обычному, основу составляет исследование заключения эксперта и определение его соответствия имеющимся в материалах дела доказательствам. В случае выявления каких-либо противоречий, следователю целесообразно сделать соответствующие выписки, указав в них местонахождение тех или иных данных (том и лист дела), но это применимо для очного допроса, когда эксперт оказывается непосредственно в кабинете следователя. На допросе это позволяет следователю оперативно отыскать необходимые материалы и предложить эксперту объяснить выявленные противоречия (если таковые, действительно, имеют место) с точки зрения его специальных знаний.

Совсем иначе обстоят дела в случае ВКС допроса. В этом случае недостаточно «сделать закладки» в материалах дела. Необходимо интересующие и спорные моменты перевести в цифровой формат. С помощью сканеров, плат захвата звука и изображения создать файлы, содержащие необходимую информацию, представленную в избранной следователем последовательности. Таким образом, возникает проблема в доступности такого рода техники и наличия навыков и умений её применения следователями. Другая проблема заключается в том, что в процессе допроса зачастую возникают ситуации, когда необходимо предоставить допрашиваемому информацию, которая изначально не была подготовлена, но в процессе проведения допроса стала актуальной. В этом случае для следователя, проводящего допрос при помощи ВКС, необходимо в режиме реального времени создать цифровую копию требуемых материалов. Следовательно, становится очевидной проблема обеспечения следователей соответствующей техникой и умением её применять.

В заключение следует отметить, что несмотря на некоторые сложности, указанные выше, связанные с допросом эксперта, проводимым посредством ВКС, следует отметить, что в условиях сложившейся следственно-судебной и экспертной практики возможность производства допроса эксперта при помощи ВКС, по мнению авторов, будет способствовать оптимизации деятельности следователя/суда при производстве рассматриваемых процессуальных действий.

3.4. Вопросы для самоконтроля

1. Что есть вариативность тактики следствия и способов доказывания по уголовным делам?
2. На первоначальном этапе расследования какие возможны следственные ситуации и какие обычно в связи с этим планируют и осуществляют неотложные следственные действия?
3. Какие обычно осуществляют (планируют возможные) неотложные следственные действия?
4. Каковы задачи проведения компьютерно-технических и иных экспертиз по уголовным делам, связанным с информационными технологиями?

5. С какими возможными целями обычно проводят компьютерно-технические экспертизы?
6. Какой статьёй УПК РФ определяется порядок назначения судебной экспертизы?
7. Как выглядит типовая процедура подготовки к процессуальным действиям следователя (дознавателя) для сбора доказательств по уголовным делам, связанным с IT-преступлениями?
8. Приведите пример плана предстоящего следственного действия.
9. Какие рекомендации (что не забыть, что целесообразно иметь при себе) можно дать начинающим следователям?
10. В чём заключается специфика организации проведения опросов и допросов?
11. Какие вопросы выясняются в ходе допроса подозреваемого (обвиняемого)?
12. В чём заключается отличие тактики допроса подозреваемых в нарушении правил эксплуатации ЭВМ, системы ЭВМ или их сети?
13. Что дополнительно устанавливается в отношении субъектов преступления?
14. Должный ли результаты ОРД удовлетворять ст. 89 УПК РФ?
15. За счёт чего использование результатов ОРД способно существенно обогатить доказательственную базу?
16. С учётом специфики компьютерных преступлений что должно содержаться в материалах направляемых для возбуждения уголовного дела или в качестве результатов ОРД следователю (дознавателю)?
17. В каком случае производится переквалификация преступления?
18. Каких преступлений по статистике больше: а) преступления, в которых криптовалюта выступает средством их совершения; б) преступления, в которых криптовалюта выступает предметом посягательства; в) преступления, совершаемые в целях генерации (майнинга) криптовалюты?
19. В чём опасность использования нейросетевых аудио- и видео-фильтров?
20. В чём опасность использования нейросетевых аудио- и видео-фильтров?
21. Поясните почему специалистам (экспертам) желательно быть ораторами?
22. Зачем практикующим подразделениям необходимо регулярно направлять своих сотрудников в качестве слушателей на открытые судебные заседания?
23. Приведите примеры судебных заседаний, совершённые в отношении них ошибки и их последствия.
24. Какие есть особенности (плюсы и минусы) производства допроса эксперта посредством использования видеоконференцсвязи?

Заключение, ссылки, литература

Для желающих изучить отдельные изложенные вопросы глубже авторы постарались привести максимум отсылок к другим источникам в сносках по тексту. В дополнение к этому и к последующему списку литературы, отметим ключевые направления сформировавшегося с 1990-х годов [36, 58] отечественного научного знания в сфере собирания и фиксации доказательств по уголовным делам о преступлениях, совершённых с использованием информационных технологий:

- технико(инженерно)-криминалистическое направление, достаточно качественно изложено в работах [31, 34, 41, 42, 44, 58, 60, 62, 69, 78, 84, 85];
- процессуально-криминалистическое направление, опирающиеся на работы и документы технического регулирования – [22, 25, 33, 37-39, 47, 53-57, 59, 63, 66-68, 71-74, 76, 81, 86, 95, 98-109];
- научно-аналитическое направление, представленное в основном научными работами, материалами сравнительного правоведения и личными диссертациями с проектами законодательных инициатив – [45, 46, 51, 75, 77, 83, 87, 110-202].

Ниже приведён список использованных источников, материалы которых в той или иной мере нашли отражение на страницах данного учебного пособия.

Нормативные правовые акты

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями на 31.12.2022) // СПС «Консультант Плюс».

2. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (Ратифицировано Федеральным законом от 1 октября 2008 г. № 164-ФЗ) // СПС «Консультант Плюс».

3. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий (Ратифицировано Федеральным законом от 1 июля 2021 г. № 237-ФЗ) // СПС «Консультант Плюс».

4. Гражданский кодекс Российской Федерации (часть четвёртая) от 18.12.2006 № 230-ФЗ (ред. от 11.06.2021) (с изм. и доп., вступ. в силу с 01.08.2021) // СПС «Консультант Плюс».

5. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 01.07.2021) (с изм. и доп., вступ. в силу с 01.12.2021) // СПС «Консультант Плюс».

6. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 01.07.2021, с изм. от 23.09.2021) // СПС «Консультант Плюс».

7. «Основы законодательства Российской Федерации о нотариате» (утв. ВС РФ 11.02.1993 № 4462–1), (ред. от 25.08.2021) // СПС «Консультант Плюс».

8. Федеральный закон от 12 августа1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» (ред. 01.07.2021) // СПС «Консультант Плюс».

9. Федеральный закона от 31 мая 2001 г. № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации» (ред. от 01.07.2021) // СПС «Консультант Плюс».

10. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 01.10.2021) // СПС «Консультант Плюс».

11. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (ред. от 02.07.2021) // СПС «Консультант Плюс».

12. Федеральный закон РФ от 26 июня 2008 г. № 102-ФЗ «Об обеспечении единства измерений» (ред. от 11.06.2021) // СПС «Консультант Плюс».

13. Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции» (ред. от 24.08.2021) // СПС «Консультант Плюс».

14. Федеральный закон от 1 июля 2021 г. № 237-ФЗ «О ратификации Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий» // СПС «Консультант Плюс».

15. Постановление Правительства Российской Федерации «Об утверждении государственной программы Российской Федерации "Информационное общество"» от 15 апреля 2014 г. № 313.

16. Распоряжение Правительства Российской Федерации «Об утверждении концепции перевода обработки и хранения государственных информационных ресурсов, не содержащих сведения, составляющие государственную тайну, в систему федеральных и региональных центров обработки данных» от 7 октября 2015 г. № 1995-р.

17. Распоряжение Правительства Российской Федерации «Об утверждении программы Российской Федерации"Цифровая экономика"» от 28 июля 2017 г. № 1632-р.

18. Распоряжение Правительства Российской Федерации «Об утверждении концепции создания государственной единой облачной платформы» от 28 августа 2019 г. № 1911-р.

19. Постановление Правительства Российской Федерации «О проведении эксперимента по переводу информационных систем и информационных ресурсов федеральных органов исполнительной власти и государственных внебюджетных фондов в государственную единую облачную платформу, а также по обеспечению федеральных органов исполнительной власти и государственных внебюджетных фондов автоматизированными рабочими местами и программным обеспечением» от 28 августа 2019 г. № 1114.

20. Распоряжение Правительства РФ «О Перечне видов судебных экспертиз, проводимых исключительно государственными судебно-экспертными организациями» от 16 ноября 2021 г. № 3214-р // СПС «Консультант Плюс».

21. Приказ Следственного комитета России от 12.07.2011 № 109 (ред. от 27.03.2013) «О мерах по противодействию экстремистской деятельности» // СПС «Консультант Плюс».

22. Приказ МВД России № 776, Минобороны России № 703, ФСБ России № 509, ФСО России № 507, ФТС России № 1820, СВР России № 42, ФСИН России № 535, ФСКН России № 398, СК России № 68 от 27.09.2013 «Об утверждении Инструкции о

порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд» // СПС «Консультант Плюс».

23. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (в редакции приказа ФСТЭК России от 15 февраля 2017 г. № 27).

24. Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также на объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей среды» (в редакции приказа ФСТЭК России от 23.03.2017 № 49.

25. Приказ ФСБ РФ от 23 июня 2011 г. № 277 «Об организации производства судебных экспертиз в экспертных подразделениях органов федеральной службы безопасности».

26. Приказ ФСБ России от 24 июля 2018 г. № 366 «О Национальном координационном центре по компьютерным инцидентам».

27. Приказ ФСБ России от 24 июля 2018 г. № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения».

28. Приказ ФСБ России от 6 мая 2019 г. № 196 «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты».

29. Положение Банка России от 9 июня 2012 года № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств». – М: Центральный банк Российской Федерации, 2012 г.

30. Положение Банка России от 9 января 2019 года № 672-П «О требованиях к защите информации в платёжной системе Банка России». – М: Центральный банк Российской Федерации, 2019 г.

Научная и учебная литература

31. *Агибалов В. Ю.* Виртуальные следы в криминалистике и уголовном процессе: монография. – М.: Юрлитинформ, 2012. – 152 с.

32. *Аминов И. И.* Юридическая психология: учеб. для вузов / И. И. Аминов. – М.: Издательство «Обега-Л», 2011. – 415 с.

33. *Аносов А. В.* и др. Деятельность органов внутренних дел по борьбе с преступлениями, совершёнными с использованием информационных, коммуникационных и высоких технологий: учебное пособие в 2 ч. М.: Академия управления МВД России, 2019. – Ч. 1. – 208 с.

34. *Айков Д.,Сейгер К., Фонсторх У.* Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями: пер. с англ. /В. И. Воропаев, Г. Г. Трехалин. – М.: Мир, 1999. – 351 с.

35. *Бабкин С. А.* Право, применимое к отношениям, возникающим при использовании сети Интернет: основные проблемы. М.: Центр ЮрИнфоР, 2003.

36. *Батурин Ю. М.* Проблемы компьютерного права. М.: Юрид. лит., 1991.

37. *Белкин Р. Р.* Курс криминалистики. 3-е изд., доп. М.: ЮНИТИ-ДАНА, Закон и Право, 2001.

38. *Белкин Р. С.* Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики. М.: Норма: НОРМА-ИНФРА-М, 2001.

39. *Бессонов А. А.* Частная теория криминалистической характеристики преступлений: Автореф. дис. … докт. юрид. наук. М., 2017.

40. *Бурлаков М. Е.* Алгоритм обнаружения вторжений в информационных сетях на основе искусственной иммунной системы: Дис. ... канд. техн. наук. Самара, 2017.

41. *Васильева И. Н.* Расследование инцидентов информационной безопасности : учебное пособие / И. Н. Васильева. – СПб. : Изд-во СПбГЭУ, 2019. – 113 с.

42. *Вехов В. Б.* Основы криминалистического учения об исследовании и использовании компьютерной информации и средств её обработки: монография. Волгоград: ВА МВД России, 2008.

43. *Вехов В. Б.* Криминалистическое учение о компьютерной информации и средствах её обработки: Дис. … докт. юрид. наук. Волгоград, 2008.

44. *Галяшина Е. И.* Судебная фоноскопическая экспертиза. – М.: Триада, 2001.

45. *Галяшина Е. И.* Проблемы криминалистической диагностики фальсификации фонограмм, получаемых при проведении оперативно-розыскных мероприятий // Научная школа уголовного процесса и криминалистики Санкт-Петербургского государственного университета и современная юридическая наука, СПб.: Издательский Дом СПбГУ, 2016.

46. *Григорян Г. Р.* Мошенничество в сфере компьютерной информации: проблемы криминализации, законодательной регламентации и квалификации : дис. ... канд. юрид. наук. Самара, 2021

47. *Гончар В. В., Грибкова К. А., Михайленко Н. В., Мурадян С. В., Фурсов Р. А.* Организация расследования хищений денежных средств из банкоматов (учебное пособие). / Казань: Изд-во «Бук», 2021 г. – 151 с.

48. *Дорот В. Л., Новиков Ф. А.* Толковый словарь современной компьютерной лексики. СПб.: БХВ-Петербург, 2004.

49. *Закляков В. Ф.* Информатика: учеб. для вузов 5-е изд., перераб. и доп. – М.:ДМК Пресс, 2021. – 752 с.

50. *Земскова А. В.* Теоретические основы использования результатов оперативно-розыскной деятельности при расследовании преступлений : монография. – Волгоград: ВА МВД России, 2002. – 292 с.

51. *Земскова А. В.* Теоретические основы использования результатов оперативно-розыскной деятельности при расследовании преступлений : диссертация ... докт. юрид. наук : 12.00.09. – Москва, 2002. – 420 с.

52. *Земскова А. В.* Усмотрение следователя в уголовном судопроизводстве : (теоретико-правовые и прикладные аспекты) : монография / А. В. Земскова, О. В. Химичева, М. А. Кунашев. – Москва : Юрлитинформ, 2022. – 165 с.

53. *Зинин А. М.* Криминалист в следственных действиях: учебно-практическое пособие. М.: Экзамен, Право и закон, 2004.

54. *Колычева А. Н., Васюков В. Ф.* Расследование преступлений с использованием компьютерной информации из сети Интернет: учебное пособие / Под ред. А. Г. Волеводза. М.: Проспект, 2020.

55. Криминалистика в условиях развития информационного общества (59-е ежегодные криминалистические чтения) [Электронный ресурс]: сборник статей Международной научно-практической конференции. – Электронные текстовые данные (2,33 МБ). – М. : Академия управления МВД России, 2018.

56. Криминалистическая методика расследования отдельных видов и групп преступлений: учеб. пособие / В. Д. Зеленский, Г. М. Меретуков, А. В. Гусев, С. А. Данильян – Краснодар: КубГАУ, 2013. – 355 с.

57. Криминалистическая методика расследования отдельных видов преступлений: Учебное пособие в 2-х частях. Ч. 2: / Под ред. А. П. Резвана, М. В. Субботиной. – М.: ИМЦ ГУК МВД России, 2002. – 232 с.

58. *Крылов В. В.* Информационные компьютерные преступления: Учебное и практическое пособие. М.: Инфра-М-Норма, 1997.

59. *Кушниренко С. П.* Методика расследования преступлений в сфере высоких тех-нологий: конспект лекций / С. П. Кушниренко; СПб юрид. ин-т Генеральной прокуратуры РФ. СПб., 2007. 64 с.

60. *Кэрриэ Б.* Криминалистический анализ файловых систем. – Спб.: Питер, 2007. – 480 с.

61. *Минаков С. С.* [Рецензия] / С. С. Минаков // ГИАЦ МВД России. - 2022. С. 2. – Рец. на сборник: Направление запросов при расследовании уголовных дел о преступлениях, совершённых с использованием IT-технологий: организации и располагаемые ими сведения : сборник / [В. В. Гончар и др.]. – М.: МосУ МВД России, 2022. – 63 с.

62. *Минаков С. С.* [Рецензия] / С. С. Минаков // АК РФ, ГИАЦ МВД России. – 2022. С. 4-6. – Рец. на уч.пос.: Е.А.Русскевич, А.В. Андреев, Д.В. Галиев [и др.]. Противодействие преступлениям, совершаемым в сфере оборота криптовалюты: учебное пособие / Е. А. Русскевич, А. В. Андреев, Д. В. Галиев [и др.]. – Москва: ИНФРА-М, 2022. – 211 с. – DOI 10/12737/1870566.

63. *Нехорошев А.Б.* Компьютерные преступления: квалификация, расследование, экспертиза. Ч. 2./ Под ред. В. Н. Черкасова. Саратов: СЮИ МВД России, 2004.

64. *Образцов В. А.* Выявление и изобличение преступника. М.: Юристъ, 1997.

65. Оперативно-розыскная деятельность и уголовный процесс : Учеб.-практ. пособие / Гл. правовое упр. МВД России. ВНИИ МВД России; [А. В. Земскова и др.]. – М. : Инфра-М, 2002. – 84 с.

66. Организация и нормативно-правовые основы деятельности подразделений дознания в органах внутренних дел : учебное пособие / В. В. Кардашевский, Н. В. Ми-

хайленко, М. В. Кардашевская, О. В. Мичурина. – Москва : Московский университет МВД России имени В. Я. Кикотя, 2021. – 212 с.;

67. *Петраков С. В., Ушаков А. Ю., Попов А. А., Дудаль К. Н.* Раскрытие и расследование преступлений, совершаемых с использованием информационно--телекоммуникационных технологий или в сфере компьютерной информации: учебное пособие.– СПб.: Санкт-Петербургская академия Следственного комитета, 2021.– 84 с.

68. Предварительное расследование преступлений как направление правоохранительной деятельности : (теоретические, правовые и организационные аспекты) : монография / [Волынская О. В., Ендольцева А. В., Мичурина О. В. и др.] ; [под общ. ред. О. В. Химичевой] – Москва : Московский ун-т МВД России им. В. Я. Кикотя, 2018. – 188 с.

69. *Россинская Е. Р., Усов А. И.* Судебная компьютерно-техническая экспертиза. М.: Право и Закон, 2001.

70. *Россинская Е. Р.* Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе. 4-е изд., перераб. и доп. М.: Норма, 2019.

71. *Россинский С. Б.* Следственные действия: монография. М.: Норма, 2018.

72. *Русскевич Е. А.* Уголовное право и «цифровая преступность»: проблемы и решения: монография / Е. А. Русскевич. М. : ИНФРА-М, 2019.

73. *Русскевич Е. А.* Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий (2-е издание, дополненное): учебное пособие / Е. А. Русскевич. М. : ИНФРА-М, 2019.

74. *Русскевич Е.А., Рядовский И.А., Голованов С.Ю.* [и др.] Методические рекомендации по расследованию преступлений в сфере компьютерной информации: учеб. пособие / под ред. И. Г. Чекунова. – 2-е изд., доп. М.: Московский университет МВД России имени В. Я. Кикотя, 2019.

75. *Русскевич Е. А.* Дифференциация ответственности за преступления, совершаемые с использованием информационно-телекоммуникационных технологий, и проблемы их квалификации : Дис. ... докт. юрид. наук. Москва, 2021 г.

76. *Савельева Н. В.* Проблемы доказательств и доказывания в уголовном процессе : учеб. пособие / Н. В. Савельева. – Краснодар : КубГАУ, 2019. – 95 с.

77. *Семикаленова А. И.* Судебная программно-компьютерная экспертиза по уголовным делам: Дис. ... канд. юрид. наук. М., 2005.

78. *Скиба В. Ю., Курбатов В. А.* Руководство по защите от внутренних угроз информационной безопасности. – Спб.:Питер, 2008. – 320 с.

79. Судебная экспертиза в цивилистических процессах: монография / Под ред. Е. Р. Россинской. М.: Проспект, 2018.

80. *Таненбаум Э., Остин Т.* Архитектура компьютера. 6-е изд. СПб., 2013.

81. Теория информационно-компьютерного обеспечения криминалистической деятельности: монография / под. ред. заслуженного деятеля науки РФ, доктора юридических наук, профессора Е. Р. Россинской. – М.: Проспект, 2022. – 235 с.

82. Уголовное право России : учебник в 2 т. Т. 2: Особенная часть / под ред. Н.Г. Кадникова. – М.: Юриспруденция, 2018. – 836 с.

83. *Усов А. И.* Концептуальные основы судебной компьютерно-технической экспертизы: Дис. … докт. юрид. наук. М., 2002.

84. *Усов А. И.* Судебно-экспертное исследование компьютерных средств и систем: Основы метод. обеспечения [Учеб. пособие для вузов] / под ред. Е. Р. Россинской. М.: Экзамен, Право и закон, 2003.

85. *Федотов Н. Н.* Форензика – компьютерная криминалистика – М.: Юридический Мир, 2007. – 432 с.

86. *Химичева О. В.* Допустимость доказательств в уголовном процессе : (по материалам уголов. дел о преступлениях, соверш. организ. группами) : учеб. пособие / О. В. Химичева, Р. В. Данилова; М-во внутр. дел России. Моск. ин-т МВД России. – Москва, 1998. – 73 с.

87. *Шарипов Р.Р.* Экспертиза подлинности документов на основе компьютерных методов обработки информации: Дис. ... канд. техн. наук. Волгоград, 2011.

Практические материалы

88. Информационное письмо Президиума ВАС РФ от 7 июля 2004 г. № 78 «Обзор практики применения арбитражными судами предварительных обеспечительных мер» // Вестник ВАС РФ. 2004. № 8.

89. Постановление Арбитражного суда Хабаровского края от 5 августа 2013 г. по делу № А73-14263/2012. – URL: https://sudact.ru/ (дата обращения 01.12.2021).

90. Решение Арбитражного суда Курской области от 29 мая 2018 г. по делу № А35-5996/2017. – URL: https://sudact.ru/ (дата обращения 01.12.2021).

91. Решение Арбитражного суда Саратовской области от 4 марта 2019 г. по делу № А57-15203/2018. – URL: https://sudact.ru/ (дата обращения 01.12.2021).

92. Приговор Стерлитамакского городского суда Республики Башкортостан № 1-567/2019 от 11 декабря 2019 г. по делу № 1-567/2019. – URL: https://sudact.ru/ (дата обращения 01.12.2021).

93. Приговор Новочебоксарского городского суд Чувашской Республики № 1-456/2019 от 19 декабря 2019 г. по делу № 1-456/2019. – URL: https://sudact.ru/ (дата обращения 01.12.2021).

94. Приговор Евпаторийского городского суда Республики Крым № 1-456/2019 от 24 декабря 2019 г. по делу № 1-456/2019. – URL: https://sudact.ru/ (дата обращения 01.12.2021).

95. «Конвенция о преступности в сфере компьютерной информации» (ETS № 185) (Заключена в г. Будапеште 23.11.2001) (с изм. от 28.01.2003) // СПС «Консультант Плюс».

96. Сертификат соответствия на «Мобильный комплекс аудита информационной безопасности информационных систем» ЦИАТ.461979.001 от 03 июня 2019 г. № СФ/СЗИ-0270 (система сертификации СЗИ-ГТ ФСБ России № РОСС RU.0003.01БИ00).

97. Сертификат соответствия на «Модернизированное доверенное инструментальное программное обеспечение научно-технического контроля и инженерного анализа машинных носителей информации (программное средство "Урок-9") ЦИАТ.00101» от 03 июня 2019 г. № СФ/СЗИ-0279 (система сертификации СЗИ-ГТ ФСБ России № РОСС RU.0003.01БИ00).

98. Методические рекомендации по криминалистическому исследованию мобильных телефонов сотовой связи в органах по контролю за оборотом наркотических

средств и психотропных веществ / Д. Л. Русских, С. В. Сыромятников, С. В. Баталин [и др.]. М.: ЭКУ 9 Департамента ФСКН России, 2008.

99. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации. – М.: Ген.прок-ра РФ, 2013.

100. ГОСТ 6.10.4–84. Межгосударственный стандарт. Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники. Основные положения. Unified systems of documentation. Confirment of legal force to documents on software and machinogramme created by computers. General principles. Дата введения 01.07.1987. Группа Т54. ОКСТУ 0006.

101. ГОСТ 16325–88. Машины вычислительные электронные цифровые общего назначения. Общие технические требования. – URL: https://docs.cntd.ru/document/1200016704 (дата обращения 01.12.2021)

102. ГОСТ 15971–90. Системы обработки информации. Термины и определения. – URL: https://docs.cntd.ru/document/1200015664 (дата обращения 01.12.2021).

103. ГОСТ Р 51275–2006. Национальный стандарт Российской Федерации. «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» (утв. и введён в действие Приказом Ростехрегулирования от 27.12.2006 № 374-ст). – URL: https://docs.cntd.ru/document/1200057516 (дата обращения 01.12.2021).

104. ГОСТ Р ИСО/МЭК ТО 18044–2007. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. ISO/IEC TR 18044:2004 Information technology – Security techniques – Information security incident management (IDT). Дата введения 01.07.2008. Группа Т00. ОКС 01.040.01.

105. ГОСТ Р ИСО/МЭК 27037–2014. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме. ISO/IEC 27037:2012 Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence (IDT). Дата введения 01.11.2015. ОКС 35.040.

106. СТО БР ИББС-1.3–2016. Стандарт Банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Сбор и анализ технических данных при реагировании на инциденты информационной безопасности при осуществлении переводов денежных средств. Дата введения: 01.01.2017.

107. РС БР ИББС-2.9–2016. Рекомендации в области стандартизации Банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Предотвращение утечек информации. Дата введения: 01.05.2016.

108. РС БР ИББС-2.5–2014. Рекомендации в области стандартизации Банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности. Дата введения: 01.06.2014.

109. ГОСТ Р 57429–2017. Национальный стандарт Российской Федерации. «Судебная компьютерно-техническая экспертиза. Термины и определения» (утв. и введён в действие приказом Росстандарта от 28.03.2017 № 198-ст). – URL: http://docs.cntd.ru/document/1200144960 (дата обращения 01.12.2021).

Научные статьи

110. *Ализаде В. А., Волеводз А. Г.* Неприменение ст. 174.1 УК РФ по делам о наркопреступлениях, совершённых с использованием криптовалюты, как следствие непонимания сущности легализации (отмывания) нового вида преступных активов // Наркоконтроль. – 2018. – № 1 (50). – С. 5–13.

111. *Ахмедшин Р. Л.* Актуальные аспекты тактики допроса эксперта // Вестник Том. гос. ун-та. Право. – 2014. № 4(14). – С. 15–21.

112. *Бессонов А. А.* Цифровая криминалистическая модель преступления как основа противодействия киберпреступности // Академическая мысль. 2020. № 4(13). С. 58–61.

113. *Ватрушкин А. А.* Правовые основы обеспечения кибербезопасности критической инфраструктуры Российской Федерации // Евразийская адвокатура. 2017. № 6(31). С. 78–84.

114. *Вилкова Т. Ю.* Законность и унификация в уголовном судопроизводстве: от бланков процессуальных документов – к электронному уголовному делу / Т. Ю. Вилкова, Л. Н. Масленникова // Вестник Пермского университета. Юридические науки. 2019. № 46. С. 728–751.

115. *Вехов В. Б.* Электронные доказательства: проблемы теории и практики // Правопорядок: история, теория, практика. – 2016. – № 4(11). – С. 46–50.

116. *Вехов В. Б.* Электронная криминалистика: понятие и система / В. Б. Вехов // Криминалистика: актуальные вопросы теории и практики. Сборник трудов участников Международной научно-практической конференции. Ростов-на-Дону, 2017. С.40–46.

117. *Волеводз А. Г.* Следы преступлений, совершённых в компьютерных сетях / А. Г. Волеводз // Российский следователь. – 2002. – № 1. – С. 4–12.

118. *Гаврилин Ю. В.* Понятие, свойства и криминалистическое значение компьютерно-технических следов преступления / Ю. В. Гаврилин, Н. Н. Лыткин // Вестник криминалистики. – 2005. – № 4(16). – С. 49–55.

119. *Гончар В. В., Галиев Д. В.* Особенности осмотра и изъятия электронных носителей информации с учётом требований ст. 164.1 УПК РФ // Вестник Московского университета МВД России, № 2, М., 2020, С. 134–138.

120. *Гришин А. В.* Особенности допроса эксперта в суде // Евразийская адвокатура. – 2015. – № 1(14). – С. 26–30.

121. *Гужаева В. А.* Преступность в сети Интернет: криминологические характеристики / В. А. Гужаева, Е. В. Прокофьева, О. Ю. Прокофьева // Вестник экономической безопасности. – 2019. – № 4. – С. 111–114.

122. *Закатов А. А.* Особенности первоначального этапа расследования хищений денежных средств, совершенных с использованием вредоносных компьютерных программ / А. А. Закатов, А. А. Намнеясев // Юридическая наука и практика: вестник Нижегородской академии МВД России. – 2017. – № 2(40). – С. 130–134.

123. *Захарова В. А.* Допрос эксперта: рекомендации и ошибки // Российский следователь. 2021. № 5. С. 2–24.

124. *Иванцов С. В., Сидоренко Э. Л., Спасенников Б. А., Берёзкин Ю. М., Суходолов Я. А.* «Преступления, связанные с использованием криптовалюты: основные криминологические тенденции» Всероссийский криминологический журнал. 2019 Т. 13, № 1 С. 85–93.

125. *Клишина Н. Е.* Некоторые вопросы совершенствования действующего законодательства, регламентирующего расследование киберпреступлений / Н. Е. Клишина, Р. С. Торичко // Вестник экономической безопасности. 2018. № 3. С. 179–184.

126. *Лопатина Т. М.* Кибершантаж как средство условно-цифрового вымогательства // Вопросы правоведения. 2014. № 4(26). С. 288–298.

127. *Ляскало А. Н.* Криптовалюта как предмет и средство преступления // Уголовное право: стратегия развития в XXI веке: материалы XVI Международной научно-практической конференции. М., 2019. С. 87–92.

128. *Любан В. Г., Книжникова А. Н.* Оперативно-разыскная характеристика криптовалютных мошенничеств в сфере инвестиционных проектов // Актуальные вопросы теории и практики оперативно-разыскной деятельности (к 102-летию образования службы уголовного розыска): сборник научных трудов Межведомственной научно-практической конференции. – М.: Московский университет МВД России имени В. Я. Кикотя, 2021. – С. 143–149;

129. *Мещеряков В. А.* «Виртуальные следы» под «скальпелем Оккама» // Информационная безопасность регионов. 2009. № 1(4). С. 28–33.

130. *Минаков С. С.* Основные криптографические механизмы защиты данных, передаваемые в облачные сервисы и сети хранения данных. // Вопросы кибербезопасности, 2020 г., № 3(37), С. 66–75.

131. *Минаков С. С., Хворенков С. В., Пахомова А. С.* О перспективах применения технологий искусственного интеллекта для повышения защищённости ИСОД МВД России // Вестник МВД России, 2022 г. Выпуск № 2/3 (174/175), С. 112–121. (УДК.004.056.52)

132. *Михайленко Н. В., Бондарь Е. О.* Архитектура компетенций и навыков сотрудников органов внутренних дел в современных условиях. // Международный журнал конституционного и государственного права. – 2021. – № 2. – С. 114–116.

133. *Михайленко Н. В., Мурадян С. В.* Проблемы организации деятельности органов внутренних дел по противодействию финансированию терроризма и экстремистской деятельности, совершаемых с использованием одноранговых сетей. // Противодействие терроризму и экстремизму в информационных сферах./ Всероссийская научно-практическая конференция : сборник научных статей / [сост. И. С. Мельцева]. – М.: Московский университет МВД России имени В. Я. Кикотя, 2021. – С. 62–66.

134. *Мурадян С. В.* Актуальные проблемы противодействию финансированию терроризма с использованием криптовалюты. // Актуальные проблемы международного сотрудничества в борьбе с преступностью : сборник статей по итогам Международной научно-практической конференции, приуроченной к 20-летию принятия Конвенции ООН против транснациональной организованной преступности, 29 октября 2020 г. М. : Московский университет МВД России имени В. Я. Кикотя, 2020. С. 110–118.

135. *Мурадян С. В.* Факторы, обусловливающие рост числа преступлений, совершаемых с использованием криптовалют, и способы их нивелирования в России. // Ак-

туальные вопросы современной криминологической и уголовно-исполнительной науки. Сборник тезисов Международной научно-практической заочной конференции памяти доктора исторических наук, профессора А. В. Шаркова от 15.04.2021 г. Минск: Академия МВД, 2021. С. 208 – 210.

136. *Немова М. И.* Использование криптовалюты при легализации (отмывании) денежных средств или иного имущества: приобретённых преступным путём: анализ судебной практики // Уголовное право. – 2019. – № 4. – С. 63–68.

137. *Осипенко А. Л.* Организованная преступная деятельность в киберпространстве: тенденции и противодействие // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2017. № 4(40). С. 181–188.

138. *Пинкевич Т. В.* Проблемы уголовно-правового противодействия преступной деятельности с использованием криптовалюты // Юристъ-правоведъ. 2020. № 4.

139. *Побегайло Э. Ф.* Некоторые вопросы уголовно-правовой защиты интеллектуальной собственности в сфере компьютерной информации // Публичное и частное право. 2012. № 3. С. 157–168.

140. *Поляков В. В.* К вопросу об использовании понятий «виртуальные следы» и «электронно-цифровые следы» в криминалистике // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. 2013. № 11–1. С. 123–125.

141. *Поляков В. В.* Начальные следственные ситуации расследования высокотехнологичных преступлений // Цифровые технологии в юриспруденции: генезис и перспективы. Материалы I Международной межвузовской научно-практической конференции. Красноярск, 2020. С. 123–127.

142. *Россинская Е. Р., Усов А. И.* Классификация компьютерно-технической экспертизы // Уголовный процесс и криминалистика на рубеже веков. М.: Академия управления МВД РФ, 2000.

143. *Россинская Е. Р.* Судебная компьютерно-техническая экспертиза: проблемы становления и подготовки кадров экспертов // Теория и практика судебной экспертизы. 2008. № 3. С. 62–63.

144. *Россинская Е. Р.* Информационно-компьютерное обеспечение криминалистической деятельности как частная криминалистическая теория // Воронежские криминалистические чтения. 2017. № 2(19). С. 168–176.

145. *Россинская Е. Р.* Ситуационный подход в судебно-экспертной деятельности // Современное право. 2017. № 12. С. 93–100.

146. *Россинская Е. Р.* Концепция цифровых следов в криминалистике / Е. Р. Россинская, И. А. Рядовский // Аубакировские чтения: материалы международной научно-практической конференции (19 февраля 2019 г.). Алматы: Республика Казахстан, 2019. С. 6–9.

147. *Россинская Е. Р.* Современные способы компьютерных преступлений и закономерности их реализации / Е. Р. Россинская, И. А. Рядовский // Lex Russica. 2019. № 3(148). С. 87–99.

148. *Россинская Е. Р., Семикаленова А. И.* Судебно-экспертное обеспечение борьбы с преступностью и иными правонарушениями среди молодёжи в информационно-компьютерной среде // Криминалистические проблемы эффективности борьбы с преступностью и иными правонарушениями среди молодёжи. Материалы Международной научно-практической конференции, посвящённой 95-летию профессора Л. Л. Каневского. Уфа, 2019. С. 79–86.

149. *Россинская Е. Р.* Проблемы собирания цифровых следов преступлений из социальных сетей и мессенджеров / Е. Р. Россинская, Т. А. Сааков // Криминалистика: вчера, сегодня, завтра. 2020. № 3(15). С. 101–122.

150. *Россинская Е. Р.* Дидактические проблемы в подготовке следователей в эпоху цифровизации // Юридическое образование и наука. 2020. № 7. С. 3–9.

151. *Россинская Е. Р., Семикаленова А. И.* Основы учения о криминалистическом исследовании компьютерных средств и систем как часть теории информационно-компьютерного обеспечения криминалистической деятельности // Вестник Санкт-Петербургского университета. Право. Том 11. 2020. Вып. 3. С. 745–759.

152. *Рудов Д. Н.* Программное обеспечение как объект расследования преступлений о нарушении авторских прав (процессуальный и криминалистический аспект) // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2015. № 3 (41). С. 31–33.

153. *Русскевич Е. А.* Уголовное право и информатизация / Е. А. Русскевич // Журнал российского права. – 2017. – № 8 (248). – С. 73–80.

154. *Русскевич Е. А.* О проблемах квалификации неправомерного доступа к компьютерной информации / Е. А. Русскевич // Уголовное право. – 2017. – № 5. – С. 62–64.

155. *Русскевич Е. А.* Понятие вредоносной компьютерной программы // Актуальные проблемы российского права. 2018. № 11(96). С. 207–215.

156. *Рядовский И. А.* Компетенции специалиста по работе с цифровыми следами при производстве следственных действий // Законы России. Опыт. Анализ. Практика. 2020. № 9. С. 94–100.

157. *Сааков Т. А.* Письменные речевые следы, оставленные в цифровой среде, как источник значимой информации о личности неизвестного // Законы России: опыт, анализ, практика. 2021. № 3. С. 55–59.

158. *Семикаленова А. И.* Мобильные телефоны сотовой связи – новые объекты судебной компьютерно-технической экспертизы / А. И. Семикаленова, К. А. Сергеева // Законы России, опыт, анализ, практика. 2011. № 12. С. 89–94.

159. *Семикаленова А. И.* Цифровые следы: назначение и производство экспертиз // Вестник Университета имени О. Е. Кутафина. 2019. № 5. С. 113–115.

160. *Семикаленова А. И.* Цифровые следы и их носители как объекты судебно-экспертного исследования // Современные проблемы цифровизации криминалистической и судебно-экспертной деятельности: материалы научно-практической конференции с международным участием. Москва: РГ-Пресс, 2019. С. 212–215.

161. *Семикаленова А. И.* Цифровые следы: неожиданные проблемы исследования // Цифровой след как объект судебной экспертизы: материалы Международной научно-практической конференции. М.: РГ-Пресс С. 195–198.

162. *Семикаленова А. И.* Компьютерная программа как объект комплексной товароведческой и компьютерно-технической экспертизы. Теория и практика судебной экспертизы в современных условиях: материалы VII Международной научно-практической конференции. Москва: РГ-Пресс, 2019. С. 466–472.

163. *Семикаленова А. И.* Использование специальных знаний при обнаружении и фиксации цифровых следов: анализ современной практики / *А. И. Семикаленова, И. А. Рядовский* // Актуальные проблемы российского права. 2019. № 6(103). С. 178–185.

164. *Сидоренко Э. Л.* Криптовалюта и преступления: проблемы правовой оценки / Э. Л. Сидоренко // Банковское дело. – 2018. – № 7. – С. 80-85.

165. *Сидоренко Э. Л.* Криминологические риски оборота криптовалюты / Э. Л. Сидоренко // Экономика. Налоги. Право. – 2017. – Т. 10, № 6. – С. 147-155.

166. *Смушкин А. Б.* Виртуальные следы в криминалистике // Законность. 2012. № 8. С. 43–45.

167. *Трунцевский Ю. В., Сухаренко А. Н.* Противодействие использованию криптовалюты в незаконных целях: состояние и перспективы // Международное публичное и частное право. – 2019. – № 1. – С. 43–47.

168. *Харисова З. И.* Актуальные проблемы деятельности правоохранительных органов по противодействию преступности в глобальной сети «Интернет» // Вестник УЮИ. 2019. № 3(85). С. 92–98.

169. *Чекунов И.Г.* Современные киберугрозы. Уголовно-правовая и криминологическая классификация и квалификация киберпреступлений // Право и кибербезопасность. 2012. № 1. С. 9–22.

170. *Чекунов И. Г.* Некоторые особенности квалификации преступлений в сфере компьютерной информации [Текст] / И.Г. Чекунов // Российский следователь. – 2012. – № 3. – С. 26–28.

171. *Щеглов В. Ю.* Угрозы информационной безопасности предприятий в связи с цифровой трансформацией экономики и возможности их нейтрализации / В. Ю. Щеглов, А. А. Надькина // Известия высших учебных заведений. Поволжский регион. Экономические науки. 2019. № 1(9). С. 33–39.

172. *Яковлев А. Н.* Цифровая криминалистика и её значение для расследования преступлений в современном информационном обществе / А. Н. Яковлев // Совершенствование следственной деятельности в условиях информатизации: сб. материалов междунар. науч.-практ. конф. (Минск, 12–13 апреля 2018 г.), 2018. С. 357–362.

Иностранная литература

173. Eoghan Casey. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press, 2011.

174. John Sammons. The Basics of Digital Forensics. The Primer for Getting Started in Digital Forensics. Waltham, MA: Syngress, 2015.

175. Larry Daniel, Lars Daniel, Robert Maxwell, Sue Spielman. Digital Forensics for Legal Professionals. Understanding Digital Evidence from the Warrant to the Courtroom. Waltham, MA: Syngress, 2012.

176. Matrosov A., Rodionov E., Bratus S. Rootkits and Bootkits: Reversing Modern Malware and Next Generation Threats. No Starch Press, 2015.

177. Maras Marie-Helen. Cybercriminology: Oxford University Press, 2016.

178. Graeme Horsman. Raiders of the lost artefacts: Championing the need for digital forensics research. Forensic Science International: Reports 1, 2019: https://doi.org/10.1016/j.fsir.2019.100003.

179. Farnood Faghihi, Mohammd Zulkernine. Ransom Care: Data-centric detection and mitigation against smartphone crypto-ransomware // Computer Networks, Volume 191. 2021.

180. H.M.A. van Beek, J. van den Bos, M. Ugen. Digital forensics as a service: Stepping up the game // Forensic Science International: Digital Investigation, Volume 35. 2020.

181. Kent Marett, Misty Nabors. Local learning from municipal ransomware attacks: A geographically weighted analysis // Information & Management, Volume 58, Issue 7. 2021.

182. M. Humayun, NZ Jhanjhi, A. Alsayat, V. Ponnusamy. Internet of things and ransomware: Evolution, mitigation, and prevention // Egyptian Informatics Journal, Volume 22, Issue 1. 2020.

183. Roldán, J., Boubeta-Puig, J., Luis Martínez, J., Ortiz, G. Integrating complex event processing and machine learning: An intelligent architecture for detecting IoT security attacks // Expert Systems with Applications, 2020, Volume 149.

184. Simon R. Davies, Richard Macfarlane, William J. Buchanan. Evaluation of live forensic techniques in ransomware attack mitigation // Forensic Science International: Digital Investigation, Volume 33. 2020.

Электронные ресурсы

185. *Баскин А. С., Боткин О. И.* Основы экономической теории. Курс лекций. – URL: https://economicportal.ru/ponyatiya-all/proizvodstvo.html (дата обращения 01.12.2021).

186. Законопроект № 1184595–7 «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации». Официальный сайт. Система обеспечения законодательной деятельности. – URL: https://sozd.duma.gov.ru/bill/1184595-7 (дата обращения: 01.12.2021).

187. *Левцов В.* Анатомия таргетированной атаки. – URL: https://www.kaspersky.ru/blog/targeted-attack-anatomy/4388/ (дата обращения: 01.12.2021).

188. Официальный сайт Министерства иностранных дел Российской Федерации. Проект Конвенции Организации Объединённых Наций «О сотрудничестве в сфере противодействия информационной преступности» от 16 октября 2017 г. – URL: https://www.mid.ru/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/3025418/ (дата обращения: 01.12.2021).

189. Официальный сайт Министерства юстиции Российской Федерации [Электронный ресурс]. – Режим доступа: https://minjust.gov.ru/. (Дата обращения: 21.11.2021).

190. Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций. – URL: https://rkn.gov.ru/press/publications/news67418.htm (дата обращения: 01.12.2021).

191. Портал правовой статистики Генеральной прокуратуры Российской Федерации. – URL: http://crimestat.ru/analytics/ (даты обращения: 18.07.2020, 01.12.2021).

192. *Сабитов Р.* Развитие русскоязычной киберпреступности: что изменилось с 2016 по 2021 год. – URL: https://securelist.ru/russian-speaking-cybercrime-evolution-2016-2021/103920/ (дата обращения: 01.12.2021).

193. *Чебышев В.* Развитие информационных угроз в первом квартале 2021 года. Мобильная статистика. – URL: https://securelist.ru/it-threat-evolution-q1-2021-mobile-statistics/101595/ (дата обращения 01.12.2021).

194. *Чернышова Е.* Что такое DDoS-атаки и как от них защищаться бизнесу. – URL: https://trends.rbc.ru/trends/industry/6062ec9e9a79477e19624d6a (дата обращения 01.12.2021).

195. В Group-IB рассказали об ущербе от атак вирусов-шифровальщиков. – URL: https://tass.ru/ekonomika/10092623 (дата обращения 01.12.2021).

196. Энциклопедия Лаборатории Касперского. Классификация детектируемых объектов. Вредоносные программы. [Электронный ресурс]. – URL: https://encyclopedia.kaspersky.ru/knowledge/malicious-programs (дата обращения – 01.12.2021).

197. ISO/IEC 27037. Guidelines for identification, collection, acquisition and preservation of digital evidence. – URL: https://www.iso.org/ru/standard/44381.html (дата обращения 01.12.2021).

198. NIST Special Publication 800-53. Revision 4. – URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf (дата обращения: 01.12.2021).

199. Joshua I. James, Pavel Gladyshev. Challenges with Automation in Digital Forensic Investigations. – URL: https://arxiv.org/pdf/1303.4498 (дата обращения 01.12.2021).

200. Antoine Valette. How Kroll Ontrack Recovered the Data from Space Shuttle Columbia. – URL: https://www.ontrack.com/blog/2017/06/21/kroll-ontrack-space-shuttle-columbia (дата обращения 01.12.2021).

201. Bert Rankin. How Malware Works – Malicious Strategies and Tactics. – URL: https://www.lastline.com/blog/how-malware-works-malicious-strategies-and-tactics/ (дата обращения: 01.12.2021).

202. James Wyke, Anand Ajjan. The Current State of Ransomware. – URL: https://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/sophos-current-state-of-ransomware.pdf (дата обращения 01.12.2021).

203. Lenny Zeltser. The History of Fileless Malware – Looking Beyond the Buzzword. – URL: https://zeltser.com/fileless-malware-beyond-buzzword (дата обращения – 01.12.2021).

204. Tom Spring. Threat List: Latest DDoS Trends by the Numbers. – URL: https://threatpost.com/threatlist-latest-ddos-trends-by-the-numbers/141614 (дата обращения 01.12.2021).

205. Introduction to Cybercrime. United Nations Office on Drugs and Crime. – URL: https://www.unodc.org/e4j/en/tertiary/cybercrime.html (дата обращения 01.12.2021).

Алфавитный указатель

Содержание

Книги издательства «ДМК Пресс» можно заказать в торгово-издательском холдинге «АЛЬЯНС-КНИГА» по электронному адресу: **orders@alians-kiniga.ru**.

При оформлении заказа следует указать адрес (полностью), по которому должны быть высланы книги; фамилию, имя и отчество получателя. Желательно также указать свой телефон.

Эти книги вы можете заказать и в Интернет-магазине: **www.dmkpress.com**.

Оптовые закупки: электронный адрес **books@alians-kniga.ru**.

Минаков С.С. (с.н.с. Академии криптографии РФ)
Закляков П.В.

Информационные технологии и преступления

(взгляд на цифровые следы со стороны следствия)

(учебное пособие)

Главный редактор *Мовчан Д. А.*
dmkpress@gmail.com

Вёрстка *Минаков С.С., Закляков П. В.*
Дизайн обложки *Минаков С.С., Закляков П. В.*

Подписано в печать 15.05.2023. Формат 70×100 $^{1}/_{16}$.
Гарнитура «Liberation Serif». Печать цифровая.
Усл. печ. л. 10. Тираж 100 экз.

Web-сайт издательства: www.дмк.рф
Интернет магазин: www.dmpkress.com

Отпечатано в ООО «Издательство ДМК Пресс»