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.

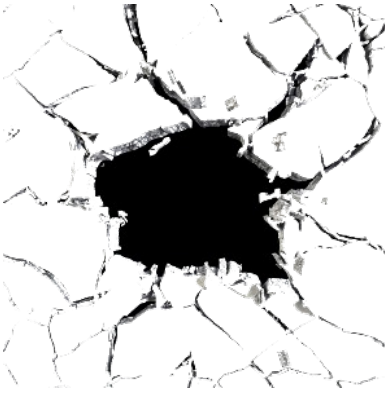
Как видно из вышеприведённого примера, запрос органов, ведущих расследование преступления на территории Российской Федерации, в правоохранительные органы США остался без ответа, в связи с чем предварительное расследование было приостановлено, так как дальнейший сбор доказательств оказался невозможен.

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].