Федеральное государственное автономное образовательное учреждение высшего образования «Московский государственный юридический университет имени О. Е. Кутафина (МГЮА)»

На правах рукописи

Шихалиева Сельджан Заур кызы

СУДЕБНЫЕ ЭКСПЕРТИЗЫ ОБЪЕКТОВ В ЦИФРОВОЙ ФОРМЕ: ПРОГНОЗИРОВАНИЕ И ПРОФИЛАКТИКА ЭКСПЕРТНЫХ ОШИБОК

Специальность 5.1.4. Уголовно-правовые науки

Диссертация
на соискание ученой степени
кандидата юридических наук

Научный руководитель:
доктор юридических наук,
доцент,
Дьяконова Оксана Геннадьевна

Москва – 2025

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ 4

ГЛАВА 1. ПОНЯТИЕ ЭКСПЕРТНЫХ ОШИБОК И ИХ ТРАНСФОРМАЦИЯ В СВЕТЕ ПОЯВЛЕНИЯ ОБЪЕКТОВ СУДЕБНЫХ ЭКСПЕРТИЗ В ЦИФРОВОЙ ФОРМЕ 18

1.1. Объекты судебных экспертиз в цифровой форме: сущность, виды и перспективы их исследования 18

1.2. Экспертные ошибки: генезис и современное состояние 56

1.3. Причины и предпосылки появления новых экспертных ошибок в условиях цифровизации 81

ГЛАВА 2. ТИПИЧНЫЕ ОШИБКИ ПРИ ПРОВЕДЕНИИ РАЗЛИЧНЫХ ВИДОВ ЭКСПЕРТИЗ НОВЫХ ОБЪЕКТОВ: СОВРЕМЕННЫЕ ВОЗМОЖНОСТИ ПРОГНОЗИРОВАНИЯ И ПРОФИЛАКТИКИ 94

2.1. Процессуальные ошибки судебных экспертиз объектов в цифровой форме .. 94

2.2. Гносеологические и операционные ошибки судебных экспертиз объектов в цифровой форме 146

ЗАКЛЮЧЕНИЕ 189

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 195

Приложение 1. Общий вид анкеты для сотрудников следственных и судебных органов по вопросам, связанным с назначением экспертизы цифровых следов . 218

Приложение 2. Результаты опроса сотрудников следственных и судебных органов по вопросам, связанным с назначением экспертизы цифровых следов 220

Приложение 3. Общий вид анкеты для государственных, негосударственных и частных судебных экспертов по вопросам, связанным с производством судебных экспертиз цифровых следов 223

Приложение 4. Примеры ответов на вопросы из анкеты для государственных, негосударственных и частных судебных экспертов по вопросам, связанным с производством судебных экспертиз цифровых следов 226

Приложение 5. Макет рабочей программы для следователей, направленной на приобретение знаний и навыков, необходимых для расследования преступлений в цифровой среде 230

Приложение 6. Перечень программ для исследования цифровых объектов 240

Приложение 7. Правила изъятия и фиксации цифровых следов в ходе следственных и оперативно-розыскных действий 241

ВВЕДЕНИЕ

Актуальность темы диссертационного исследования. Повсеместная цифровизация человеческой жизнедеятельности оказала значительное влияние на качественную составляющую преступной деятельности. На сегодняшний день наблюдается трансформация многих традиционных способов совершения преступления и объектов преступного посягательства в цифровой формат. Противодействовать преступной деятельности становится все сложнее, поскольку компьютерные технологии и технологии искусственного интеллекта (далее – ИИ) облегчили совершение преступлений, а обнаружение их следов для органов правосудия существенно затруднили. Указанные обстоятельства побуждают правоохранительные органы оперативно подстраиваться под быстро изменяющиеся реалии. Кардинальные изменения произошли и в судебно-экспертной деятельности, традиционно обеспечивающей выявление криминалистически значимых фактов и сведений.

Судебная экспертиза на протяжении многих лет является одним из наиболее надежных средств доказывания в судопроизводстве. Однако практика показывает, что привычный подход экспертов к исследованию традиционных объектов экспертизы не может полностью охватить весь перечень вопросов, которые возникают при исследовании цифровых следов. Существовавшие ранее методы исследования, типичные методики, прежний инструментарий и программное обеспечение не способны надлежаще обеспечить изучение новых свойств, которыми обладают цифровые следы. Более того, традиционных компетенций судебных экспертов оказывается уже недостаточно.

Все это закономерно влечет за собой противоречивость следственной и экспертной практики, а также совершение множества ошибок, которые нельзя игнорировать, поскольку в таком случае высоки риски подрыва процесса отправления правосудия некачественными, недостоверными экспертными заключениями.

Указанные обстоятельства обуславливают необходимость серьезного изучения теоретических и практических предпосылок допущения экспертных и следственных ошибок при исследовании объектов, представленных в цифровой форме, а также их упреждающего прогнозирования, включающего разработку профилактических мер по их предотвращению.

В последнее время появились научные исследования, отражающие результаты изучения природы цифровых следов. В то же время представляется правильным рассматривать цифровой след с учетом комплексного экспертологического подхода, что подтверждает актуальность выбранной темы исследования. Учитывая очевидный переход от традиционных следов преступления к цифровым, которые зачастую невозможно воспринимать без специальных технологий, следует полагать, что судебная экспертиза, как один из надежных способов проверки доказательств, обретает особо важное значение.

Таким образом, необходимо изучить теоретические, правовые, организационные и методические основы прогнозирования и профилактики экспертных и следственных ошибок объектов в цифровой форме.

Степень разработанности темы исследования. Природа экспертных ошибок являлась предметом исследования в трудах многих видных ученых в области криминалистики и судебной экспертологии в течение последних десятилетий, среди них: Т.В. Аверьянова, Ф.Г. Аминев, А.А. Аубакирова, Р.С. Белкин, В.В Бушуев, Ю.В. Гаврилин, Е.И. Галяшина, Г.Л. Грановский, С.В. Зуев, В.А. Клевно, Н.И. Клименко, А.Ю. Краснобаева, Л.В. Лазарева, Н.П. Майлис, С.Л. Мельник, Г.Г. Омельянюк, А.К. Педенчук, И.О. Перепечина, М.Л. Подкатилина, Е.Р. Россинская, А.А. Савицкий, С.С. Самищенко, Т.П. Соколова, И.Н. Сорокотягин, О.А. Соколова, А.И. Усов, Ш.Н. Хазиев, Е.В. Чеснокова, Г.П. Шамаев и другие.

Следует отметить фундаментальные диссертационные исследования: А.Ю. Краснобаевой (1997 г.), в котором были определены теоретические и методологические аспекты экспертных ошибок, отдельные их причины и

профилактические меры; А.А. Аубакировой (2010 г.), изучившей гносеологические, логические и психологические закономерности формирования внутреннего убеждения следователя и эксперта при получении, исследовании и оценке доказательственной информации и возникающие при этом следственные и экспертные ошибки.

Частично вопросы внедрения технологий искусственного интеллекта в судебно-экспертную деятельность были изучены Н.Ф. Бодровым, Д.В. Воронковым, А.М. Зининым, А.В. Кокиным, А.В. Поляковой, В.А. Федоренко и другими. В частности, по результатам проведенных исследований авторы отмечают необходимость осторожно относиться к результатам, сформулированным благодаря технологиям ИИ. Авторы резюмируют, что на данном этапе без проработки ошибок, допускаемых нейросетями, их применение должно иметь только вспомогательное и ориентирующее значение.

Анализ научной и учебной литературы позволяет заключить, что изучению трансформации экспертных ошибок ввиду появления объектов в цифровой форме, их прогнозированию и профилактике до сих пор не уделялось достаточного внимания, фундаментальных трудов по данной проблематике практически нет, существующие материалы находятся в разрозненном виде в ряде научных публикаций, что в целом свидетельствует о необходимости более глубокого изучения данной темы.

Объектом исследования является экспертная, следственная и судебная практика, содержащая следственные и детерминированные ими экспертные ошибки, сформировавшиеся при назначении экспертизы объектов в цифровой форме и при исследовании объектов в цифровой форме.

Предметом настоящего исследования являются закономерности объективной действительности, обусловливающие появление следственных и экспертных ошибок при назначении и производстве судебных экспертиз объектов в цифровой форме, их прогнозирования и профилактики с учетом теоретических,

организационных и методических основ цифровизации судебно-экспертной деятельности.

Цель диссертационного исследования заключается в выявлении и последующем прогнозировании следственных и экспертных ошибок при работе с объектами в цифровой форме, а также разработке теоретических, правовых, организационных и методических рекомендаций для их профилактики.

Для достижения указанной цели исследования последовательно решались следующие **задачи**:

– изучение сущности и качественных характеристик цифровых следов, рассмотрение видов цифровых следов в ракурсе дискуссии относительно виртуальной или материальной природы цифровых следов;

– изучение сущности цифровых следов в совокупности с объектами-носителями, на которых они фиксируются для направления на судебную экспертизу;

– введение комплексного понятия «цифровой объект» и авторской дефиниции понятия «цифровой документ» в терминологию судебной экспертизы;

– исследование генезиса и видов экспертных ошибок, причин их трансформации в свете появления объектов в цифровой форме;

– анализ судебной, следственной и экспертной практики, выделение новых следственных ошибок, допускаемых при выявлении, изъятии, фиксации цифровых следов, а также назначении судебной экспертизы цифровых объектов;

– анализ судебной, следственной и экспертной практики, выделение новых экспертных ошибок, допускаемых при исследовании цифрового объекта;

– разработка профилактических мер для ликвидации следственных и экспертных ошибок;

– изучение практики и рассмотрение рисков внедрения технологий ИИ в судебно-экспертную деятельность.

Методология и методы научного исследования основаны на диалектическом подходе к познанию определенных выше закономерностей,

который предполагает рассмотрение явлений в их взаимосвязи и развитии. В исследовании применялись методы формальной логики, общенаучные (наблюдение, описание, сравнение, моделирование и другие) и частнонаучные (специальные) методы (формально-юридический, исторический, статистический, метод экспертных оценок и другие). Например, метод сравнения позволил определить процесс трансформации экспертных ошибок, обусловленный цифровизацией и появлением связанных с этим ошибок в цифровой форме; в процессе применения метода моделирования с помощью дескриптивной и прогнозной моделей были определены и обоснованы возникающие в современных условиях экспертные ошибки, спрогнозировано появление экспертных ошибок, а также выделены риски использования технологий ИИ.

Формально-юридический метод использовался при анализе и толковании нормативных правовых актов по тематике исследования и позволил выявить экспертные ошибки, обусловленные регламентацией правовых явлений и процессов; исторический метод применялся при изучении генезиса экспертных ошибок; статистическое изучение материалов уголовных дел, заключений судебных экспертиз, рецензий специалистов позволило обеспечить достоверность поставленных гипотез; использование метода экспертных оценок способствовало совершенствованию процедуры собирания, обобщения и анализа мнений опрошенных экспертов и правоприменителей с последующей качественной и количественной оценкой высказанных суждений.

Общеэкспертные и частноэкспертные методы применялись при проведении изучения цифровых объектов, что позволило выявить экспертные ошибки гносеологического и операционного характера и сформулировать рекомендации по их предотвращению.

Для достижения целей исследования и решения поставленных задач указанные методы применялись системно и в совокупности.

Теоретическую основу исследования составляют фундаментальные труды ученых в области криминалистики и судебной экспертологии: Т.В. Аверьяновой,

Ф.Г. Аминева, Р.С. Белкина, В.Б. Вехова, А.И. Винберга, Т.С. Волчецкой, Е.И. Галяшиной, О.Б. Дроновой, О.Г. Дьяконовой, А.М. Зинина, Ю.Г. Корухова, Л.В. Лазаревой, Н.П. Майлис, Т.Ф. Моисеевой, Г.Г. Омельянюка, Ю.К. Орлова, Е.Р. Россинской, О.А. Соколовой, Е.В. Чесноковой, Л.Г. Шапиро, А.И. Усова и многих других.

Диссертационное исследование основано также на специальной литературе, посвященной теории цифровизации судебно-экспертной деятельности, практическим изысканиям о совершения экспертных ошибок, среди которых работы Е.И. Галяшиной, А.М. Зинина, А.В. Качука, А.В. Кокина, А.К. Лебедевой, Е.В. Меланич, А.В. Мишина, И.В. Огорелкова, Г.Г. Омельянюка, Е.Р. Россинской, Г.В. Парамоновой, Т.А. Саакова, А.И. Семикаленовой, Ш.Н. Хазиева, Н.А. Хатунцева и другие.

Нормативную основу исследования составляют Конституция Российской Федерации, Уголовно – процессуальный кодекс Российской Федерации (далее — УПК РФ), Федеральный закон «О государственной судебно-экспертной деятельности в Российской Федерации» (далее — ФЗ о ГСЭД), Федеральный закон «Об обеспечении единства измерений», Кодекс Российской Федерации об административных правонарушениях (далее — КоАП РФ), Федеральный закон «Об информации, информационных технологиях и о защите информации».

В исследовании также были использованы Постановления Пленума Верховного Суда Российской Федерации и Постановления Пленума Высшего Арбитражного суда Российской Федерации, приказы Министерства юстиции Российской Федерации, Министерства внутренних дел Российской Федерации, Следственного Комитета Российской Федерации и другие, регламентирующие судебно-экспертную деятельность.

Эмпирическая база научного исследования представлена:

– материалами судебной практики, размещенными в Государственной автоматизированной системе Российской Федерации «Правосудие», а также в справочно-правовых системах: «КонсультантПлюс», «Гарант» и Интернет-

ресурсах (Право.ru: законодательство, судебная система, новости и аналитика, база судебных актов, судебных решений и нормативных документов «Судебные и нормативные акты РФ»);

– результатами изучения материалов 198 уголовных дел, при расследовании которых назначались и проводились судебные экспертизы цифровых объектов;

– результатами изучения 220 заключений экспертов по судебным экспертизам цифровых объектов и рецензий, подготовленных специалистами в целях оказания помощи органам следствия и суду в оценке заключений экспертов;

– результатами проведенного анкетирования 94 следователей следственных подразделениях системы МВД России и следственных отделов Следственного комитета Российской Федерации;

– 117 экспертов, включая сотрудников государственных судебно-экспертных учреждений (47 экспертов) и сотрудников негосударственных судебно-экспертных организаций (70 экспертов).

Кроме того, использован личный опыт автора (более трех лет работы) в негосударственной судебно-экспертной организации при производстве судебных почерковедческих экспертиз.

Научная новизна исследования выражается в выявлении новых экспертных и следственных ошибок, обусловленных активным использованием цифровых технологий в преступной деятельности и появлением цифровых объектов, обладающих качественно иными характеристиками, требующими иного подхода к их исследованию; определении причин возникновения существующих и прогнозировании новых ошибок; определении профилактических мер по предотвращению совершения изученных ошибок, а также способов расширения компетенции следователей и экспертов путем внедрения дополнительных дисциплин в образовательные траектории и программы повышения квалификации.

Основные положения, выносимые на защиту.

1. Материальная природа цифровых следов предопределяет их фиксацию на определенных носителях, что позволяет выделить в качестве объекта экспертного

исследования цифровой объект (или объект в цифровой форме), состоящий из двух компонентов – цифрового следа, как информации, и его носителя.

Предлагается в судебно-следственной и экспертной практике использовать термин цифровой объект, под которым понимается *объект судебно-экспертного исследования, состоящий из цифровых следов различных видов, находящихся на объекте-носителе*. Существующие в отечественном законодательстве понятия «электронный носитель информации» и «электронный след» не учитывают всех характеристик и свойств самого носителя, сужая физическую природу цифровых следов и носителей до электронных. Однако электронными являются только носители с флеш-памятью, помимо них существуют электромагнитные, электрические, магнитные, оптические, механические и др.

Главным критерием для определения цифрового объекта как сочетания цифрового следа и материального носителя является обязательность указания на двойственную природу таких объектов.

2. Отдельным видом цифровых объектов являются цифровые документы, под которыми предлагается понимать *самостоятельный вид цифровых объектов, созданных с помощью компьютера (иного устройства) и подтверждённых электронной цифровой подписью (ЭЦП), либо переведённых из цифрового формата в бумажный и нотариально заверенных, содержащих в себе информацию о фактах или событиях, имеющих доказательственное значение по делу.* Требование о нотариальном заверении или подтверждении электронной цифровой подписи (ЭЦП) необходимо для придания легитимности представленному цифровому документу как объекту экспертного исследования.

3. Причины и предпосылки трансформации экспертных ошибок ввиду появления новых цифровых объектов:

- замена аналоговых способов собирания и фиксации информации цифровыми, что привело к появлению новых объектов в цифровой форме, требующих применения новых подходов, правил и методов исследования;

- отсутствие апробированной методики, использование неповеренного оборудования, нелицензионных программ и приложений, искажающих первоначальные характеристики цифрового объекта и др.;

- неполное исследование цифрового объекта вследствие недостаточности имеющихся у эксперта компетенций.

4. Одними из наиболее существенных следственных и экспертных ошибок являются отсутствие в постановлении/определении о назначении судебной экспертизы следователем/судом и в заключении эксперта признаков, позволяющих идентифицировать цифровой след (контрольной суммы (хеш-суммы), рассчитанной по криптографическому алгоритму), размера файла и других его атрибутов. Хеш-суммы должны быть указаны, а совпадение контрольных цифр подтвердит достоверность цифрового файла. Следственной ошибкой является отсутствие расчета хеш-суммы файла. В качестве профилактики данной ошибки предлагается разработать и обсудить на заседании Правительственной комиссии о координации судебно-экспертной деятельности в Российской Федерации «Правила изъятия и фиксации цифровых следов в ходе следственных и оперативно-розыскных действий» с последующим их закреплением в межведомственном приказе.

Экспертные ошибки, связанные с нивелированием значимости хеш-суммы:

- эксперт получил сведения о хеш-сумме, но не провёл самостоятельный расчёт показателя;

- эксперт не получил никаких сведений о хеш-сумме цифрового следа и не сделал об этом никакой пометки в своём заключении.

5. В перечень следственных ошибок при назначении экспертизы цифровых объектов входят:

- ненадлежащая упаковка цифровых объектов, не обеспечивающая невозможность несанкционированного доступа к носителю цифровых объектов;

- ненадлежащее описание упаковки цифрового объекта в процессуальных документах, предоставляемых эксперту, содержание которой не позволяет однозначно ее идентифицировать;

- ненадлежащее описание цифрового объекта;

- копирование цифрового следа на материальный носитель неизвестной природы, в том числе на личный флеш-накопитель следователя, а не на входящий в перечень объектов, стоящих на балансе следственных подразделений (карты память, флеш-карты, дисковые накопители и т.д.) или относящихся к расходным материалам одноразового использования (CD диски);

- действия следователя по самостоятельному изъятию или копированию без привлечения специалиста в области информационно-коммуникационных технологий при отсутствии у него соответствующих компетенций, особенно при изъятии цифровой информации из активной сети, в том числе создание следователем образа жёсткого диска, в отсутствие проверки наличия активных сетевых подключений;

- проведение выборочного осмотра компьютерных средств и систем (установленных и использующихся приложений, файловой системы, дерева каталогов и пр.), что по природе является как процессуальной, так и операционной ошибкой;

- неполное отражение примененных специалистом технических и программных средств и результатов их применения в протоколе осмотра места происшествия или иного следственного действия;

- несопоставление внешней обстановки места происшествия (в том числе осмотра сопутствующих предметов) с непосредственным изучением цифрового устройства и изъятия цифрового следа;

- несоблюдение требования о фиксации предметов/окружающей обстановки на фотоаппарат и видеокамеру, производство фиксации с использованием личных мобильных устройств членов следственно-оперативной группы (смартфоны, планшеты и т.д.), которые значительно искажают объект отображения.

6. Экспертные ошибки при исследовании цифровых объектов во многом обусловлены следственными ошибками, но не связаны ими исключительно:

- неправильное, неполное описание экспертом упаковки, в которой был получен цифровой объект;

- выход эксперта за пределы компетенции при отсутствии у него специальных знаний, при неправильной постановке задачи исследования (эксперту поручили исследовать не сам цифровой след (например, базу 1С), а установить факт изменения технических свойств программы);

- недопустимые обработка и редактирование объектов в цифровой форме, конвертирование, кадрирование, обрезка аудио- и видеодорожек с использованием неапробированного инструментария, в частности в приложениях на мобильных устройствах, а также посредством использования интернет-сайтов;

- использование недопустимого программного обеспечения: недоступного для использования в связи с невозможностью продления или покупка официальной лицензии; использование недостаточно апробированных и неадаптированных отечественных аналогов;

- необоснованное внедрение технологий ИИ в процесс исследования, недостаточно апробированных для решения задач судебно-экспертной деятельности, а также чрезмерное доверие эксперта результатам работы технологии ИИ.

7. В качестве мер профилактики ошибок для следователей предлагается использовать разработанную инструкцию по работе с цифровыми следами, их изъятию, а также расчёту хеш-суммы и рабочую программу учебной дисциплины, направленную на приобретение необходимых знаний о цифровых следах, потенциальных ошибках и их предотвращению. Для экспертов предлагается проводить программы дополнительного профессионального образования по работе с цифровыми следами и применять рекомендуемый перечень программного обеспечения, заслуживающего доверия при исследовании цифровых следов.

8. В рамках риск-менеджмента экспертных лабораторий предлагается выделить направление по изучению рисков при использовании технологий ИИ в экспертных исследованиях. Для реализации этого направления следует:

1) определить риски, связанные с недостатками машинного обучения, недостатками баз данных, используемых системой ИИ. Для минимизации рисков следует внедрять в обозримом будущем только алгоритмы искусственного интеллекта контролируемого обучения (обучение с учителем);

2) сформулировать критерии допустимости использования технологий ИИ в судебной экспертизе, к которым можно отнести:

- обучение системы ИИ на достаточном количестве сравнительных образцов с учетом всех известных признаков, присущих каждому отдельно взятому объекту судебной экспертизы;

- обеспечение процесса обучения на верифицированных образцах;

- обеспечение единства баз данных и методик для различных ведомственных экспертных организаций.

Теоретическая значимость результатов научного исследования определяется совершенствованием и развитием общей теории судебной экспертологии, теории цифровизации судебно-экспертной деятельности, в частности, разработана авторская дефиниция цифрового объекта, выделены и изучены виды экспертных ошибок, совершаемые при исследовании цифровых объектов, спрогнозированы ошибки, которые могут иметь место при некритичном восприятии результатов технологий ИИ в экспертном исследовании. Изложенные в диссертации результаты научного исследования могут быть использованы в целях прогрессивного развития учения об экспертных ошибках в судебной экспертологии.

Практическая значимость результатов научного исследования заключается: 1) в разработке рекомендаций и профилактических мер, направленных на предотвращение ошибок со стороны правоприменителей и экспертов и обеспечивается:

– инструкцией по изъятию и фиксации цифровых следов, а также подсчету хеш-суммы;

– рабочей программой, направленной на приобретение знаний о цифровых следах, возможных ошибках при работе с ними;

– предложением о необходимости принятия ведомствами Межведомственного приказа об утверждении «Правил изъятия и фиксации цифровых следов в ходе следственных и оперативно-розыскных действий», включающего положения по изъятию и фиксации цифровых следов, а также подсчету хеш-суммы;

2) в предложениях по совершенствованию судебно-экспертной деятельности при исследовании объектов в цифровой форме, которые могут использоваться:

- для разработки курса дополнительного профессионального образования по цифровизации судебно-экспертной деятельности;

- для создания примерного перечня программ, которые могут использоваться экспертами при исследовании цифровых следов;

- для разработки направления риск-менеджмента экспертных лабораторий при работе с технологиями ИИ;

- в учебном процессе при проведении лекционных и практических занятий по дисциплинам «Судебная экспертология», «Криминалистика», «Участие специалиста в процессуальных действиях».

Апробация результатов исследования. Основные теоретические положения и практические рекомендации диссертационного исследования отражены в 5 научных публикациях, 4 из которых опубликованы в изданиях, входящих в Перечень ведущих рецензируемых научных журналов и изданий, рекомендованных Высшей аттестационной комиссией при Министерстве науки и высшего образования Российской Федерации (ВАК при Минобрнауки России), в которых должны быть опубликованы основные результаты диссертаций на соискание ученой степени кандидата наук.

В опубликованных работах в достаточной степени отражено содержание диссертации, что отвечает предъявленным требованиям. Основные теоретические положения и практические рекомендации доложены на следующих конференциях: XXII Международная научно-практическая конференция «Кутафинские чтения» «Труды профессора Р.С. Белкина как вектор развития теории и практики судебной экспертизы. К 100-летию со дня рождения ученого и педагога» (Москва, 24 ноября 2022 г.), IX Международная научно-практическая конференция «Теория и практика судебной экспертизы в современных условиях» (Москва, 26-27 января 2023 г.), X Международная научно-практическая конференция «Теория и практика судебной экспертизы в современных условиях» (Москва, 30-31 января 2025 г.)., Международная научно-практическая конференция — «Экспертные ошибки: современные проблемы возникновения, выявления и профилактики» (Москва, 19 января 2024 г.), Научно-практическая конференция с международным участием «Правовое и судебно-экспертное обеспечение безопасности логистических потоков материальных ценностей» (Москва, 5 апреля 2024 г.), Научно-практическая конференция с международным участием «Национальные и международные тенденции и перспективны развития судебной экспертизы» (Нижний Новгород, 14-15 мая 2025 г.).

Достоверность результатов исследования обеспечивается эффективным сочетанием методов научного познания, эмпирического материала по тематике исследования, нормативно-правовой базы и научных работ по исследуемой тематике.

Объем и структура диссертации. Диссертация состоит из введения, двух глав, включающих пять параграфов, заключения, списка использованных источников, приложений.

ГЛАВА 1. ПОНЯТИЕ ЭКСПЕРТНЫХ ОШИБОК И ИХ ТРАНСФОРМАЦИЯ В СВЕТЕ ПОЯВЛЕНИЯ ОБЪЕКТОВ СУДЕБНЫХ ЭКСПЕРТИЗ В ЦИФРОВОЙ ФОРМЕ

1.1. Объекты судебных экспертиз в цифровой форме: сущность, виды и перспективы их исследования

Изучение теории о трансформации экспертных ошибок в свете цифровизации невозможно без рассмотрения вопроса о сущности новых объектов в цифровой форме.

Цифровизации судебно-экспертной деятельности за последние несколько лет уделялось внимание целого ряда ученых и исследователей.

О внедрении большого массива информационных технологий, систем и программ, появившихся в эпоху цифровизации и позволяющих совершенствовать работу эксперта и всю судебно-экспертную деятельность, говорят М.Д. Лебедев и С.А. Саввоев. Перечисляя такие вспомогательные информационные системы и технологии, как аппаратно-программный комплекс «ВОКОРД Видеоэксперт», программное обеспечение «БиоНейроАвтограф», Экспертная система «Анализ ДТП» и др., они пишут следующее: «Судебно-экспертную деятельность можно представить в качестве сложной системы, включающей в себя как научные основы и элементы правового регулирования, так и используемые технические средства, методы и методики производства судебных экспертиз. При этом особое место в указанной системе на современном этапе развития занимают информационные технологии, достижения которых существенно расширяют возможности судебно-экспертной деятельности и, безусловно, способствуют повышению степени научной обоснованности получаемых результатов»[1].

[1] Лебедев, М. Д., Саввоев, С. А. К вопросу об оптимизации судебно-экспертной деятельности в эпоху цифровизации / М. Л. Лебедев, С. А. Саввоев // Скиф. — 2021. — №3 (55). С. 55.

А.А. Саркисян в качестве нового инструмента цифровизации судебно-экспертной деятельности выделяет цифровые базы данных, заменяющие натурные коллекции и картотеки. Она также отмечает тенденцию к цифровизации, говоря следующее: «На данном этапе уже активно разрабатываются теория цифровизации судебно-экспертной деятельности, рекомендации по обращению с новыми видами объектов судебных экспертиз, формируются методы исследования, анализируется экспертная практика, решаются различные задачи судебно-экспертной деятельности. Судебные эксперты отчетливо понимают, насколько стремительно движется процесс цифровизации, и стараются активно использовать достижения современной науки и техники в целях оптимизации и совершенствования процесса экспертного исследования, профилактической и прогностической деятельности, расширения компетенций и т.д.»[2].

Е.Р. Россинская в целях решения судебно-экспертных задач выделяет два основных направления цифровизации судебно-экспертной деятельности:

1) использование современных информационных технологий для решения различных судебно-экспертных задач и совершенствование информационных процессов сбора, хранения, обработки, предоставления информации для производства судебных экспертиз;

2) исследование новых объектов экспертного исследования, представляющих собой криминалистически значимую информацию, фиксируемую в цифровом виде на специфических электронных носителях. Это касается фототехнических, портретных, фоноскопических и ряда других экспертиз[3].

Как мы видим, автор отмечает направление изучения природы новых объектов судебных экспертиз в качестве одного из наиболее приоритетных. В

---

[2] Саркисян, А. А. Цифровые базы данных в судебно-экспертной деятельности / А. А. Саркисян // Вестник Университета имени О. Е. Кутафина. — 2020. — №6 (70). С. 134.

[3] Россинская, Е. Р. Современное состояние и перспективы цифровизации судебно-экспертной деятельности: материалы Межд. науч.-практ. конф. «Теория и практика судебной экспертизы в современных условиях» (г. Москва, 17-18 января 2019 г.). М.: РГ-Прогресс, 2019.

первую очередь речь идет про объекты в цифровой форме, что обусловлено следующим.

С появлением высокотехнологичных способов совершения «традиционных» преступлений закономерно изменились и привычные практике способы отображения объектов. На смену типичным аналоговым способам отображения пришли их электронные аналоги, представленные в цифровом виде. Иначе говоря, сам процесс следообразования изменился вместе с переходом преступлений в цифровое пространство. Это значит, что и объекты следообразования предстают теперь в новом, трансформированном, цифровом виде. Они возникают в ответ на изменения в правовой системе, технологиях, общественных запросах и криминальных тенденциях. Такие объекты требуют применения современных методов и подходов для обеспечения справедливости и точности в экспертном исследовании.

Анализ специальной литературы и информации из открытых интернет-источников позволяет сделать вывод о том, что на сегодняшний день существует множество подходов в криминалистике и судебной экспертологии к способам преобразования новых объектов следообразования ввиду цифровизации. Рассмотрим некоторые из них.

А.Н. Савенков и Е.Р. Россинская отмечают неизбежный процесс «оцифровки» преступности, масштаб которого неограничен и растет параллельно с развитием технологий, что само по себе является серьезным вопросом для науки криминалистики[4]. Авторы обращают внимание на появление новых цифровых сущностей: «Значение фактора новых цифровых сущностей заключается в том, что в цифровом пространстве появляются сущности, у которых нет прямых аналогов в реальной жизни, но которые имеют финансовый эквивалент и влияние на объекты реального мира»[5]. Например, среди таких можно выделить криптовалюты,

[4] Савенков, А. Н., Россинская, Е. Р. Вектор развития криминалистической науки в условиях глобальной цифровизации / А. Н. Савенков, Е. Р. Россинская // Государство и право. — 2023. — № 5. С. 103.
[5] Там же.

вычислительные мощности информационных систем и т.д. Справедливо отмечается, что появление новых объектов следообразования, цифровых сущностей, целого класса преступлений, совершающихся с использованием компьютерных систем и отличающихся определенными общими признаками, системы и информационные инструменты, использующиеся криминалистами при расследовании преступлений, в совокупности образуют новую частную теорию. Следует согласиться со следующим высказыванием Е.Р. Россинской: «К сожалению, закономерности возникновения, движения и видоизменения потоков криминалистически значимой информации с использованием компьютерных средств и систем пока не нашли достойного места в криминалистической науке»[6]. Данное положение натолкнуло авторов на идею формирования частной криминалистической теории информационно-компьютерного обеспечения криминалистической деятельности.

Согласно позиции автора, «предметом теории информационно-компьютерного обеспечения криминалистической деятельности являются закономерности возникновения, движения, собирания, исследования и использования компьютерной информации при раскрытии и расследовании преступлений и судебном рассмотрении уголовных, гражданских (в том числе арбитражных), административных дел. Объектами теории информационно-компьютерного обеспечения криминалистической деятельности являются, с одной стороны, сами компьютерные средства и системы как носители розыскной и доказательственной криминалистически значимой информации, с другой — система действий и отношений в механизмах преступлений с использованием компьютерных средств и систем, а также криминалистических компьютерных технологий выявления, фиксации, изъятия, сохранения, исследования и

[6] Россинская, Е. Р. К вопросу о частной теории информационно-компьютерного обеспечения криминалистической деятельности / Е. Р. Россинская // Известия ТулГУ. Экономические и юридические науки. — 2016. — Вып. 3, ч. II. — С. 109—117; Вехов, В. Б. Электронная криминалистика: понятие и система / В. Б. Вехов // Криминалистика: актуальные вопросы теории и прак-тики: сб. тр. участников Междунар. науч.-практ. конф. Ро-стов н/Д. — 2017. — С. 40-46.

использования криминалистически значимой доказательственной и ориентирующей информации»[7].

Среди изучаемых в рамках частной теории закономерностей примечательно следующее. К закономерностям, составляющим предмет данной теории, можно отнести: закономерности возникновения, существования и исчезновения (утраты) в компьютерных средствах и системах цифровых следов, содержащих криминалистически значимую информацию; закономерности отражения в компьютерных средствах и системах криминалистически значимой информации — цифровых следов — о событии преступления / правонарушения и др[8].

Таким образом, Е.Р. Россинская предлагает рассматривать в качестве новых объектов следообразования, а, следовательно, и объектов исследования цифровые следы. Можно полагать, что цифровые следы, как качественно новый объект, выступают центром частной криминалистической теории информационно-компьютерного обеспечения криминалистической деятельности, поскольку все ее положения связаны с цифровыми следами их фиксацией, изъятием и исследованием.

Приведем еще один подход, в рамках которого предлагается выделять цифровую криминалистику как частную криминалистическую теорию. В.Б. Вехов и С.В. Зуев, как основатели данной теории, предлагают под ней понимать следующее: «Цифровая криминалистика — это частная криминалистическая теория, система научных положений и разрабатываемых на их основе технических средств, приемов, методик и рекомендаций по обнаружению, фиксации,

---

[7] Россинская Е.Р., Семикаленова А.И., Рядовский И.А., Сааков Т.А. Теории информационно-компьютерного обеспечения криминалистической деятельности : монография / под. ред. заслуженного деятеля науки РФ, доктора юридических наук, профессора Е.Р. Россинской. — М.: Проспект, 2022. С. 197.

[8] Россинская Е.Р., Семикаленова А.И., Рядовский И.А., Сааков Т.А. Теории информационно-компьютерного обеспечения криминалистической деятельности : монография / под. ред. заслуженного деятеля науки РФ, доктора юридических наук, профессора Е.Р. Россинской. — М.: Проспект, 2022. С. 212.

предварительному исследованию, использованию компьютерной информации и средств ее обработки»[9].

В качестве предмета теории цифровой криминалистики авторы предлагают рассматривать следующее: «закономерности обнаружения, фиксации, предварительного исследования, использования компьютерной информации и средств ее обработки в целях выявления, раскрытия, расследования и предупреждения правонарушений, создания на знании этих закономерностей технических средств, приемов, методик и рекомендаций, направленных на оптимизацию деятельности по борьбе с правонарушениями»[10].

Анализируя приведенные выше теории, можно заметить сходство между ними, в частности, в рамках обеих теорий изучаются компьютерные технологии, системы, компьютерная информация. Обе теории предлагается выделять в качестве частной криминалистической теории. Однако мы считаем важным обозначить, что система цифровой криминалистики намного уже системы теории информационно-компьютерного обеспечения криминалистической деятельности, поскольку она изучает лишь узкий перечень из трех направлений, в то время, как последняя теория охватывает целых восемь. Так, в рамках системы цифровой криминалистики изучаются следующие три направления:

- криминалистическое учение о цифровой (компьютерной) информации;

- криминалистическое исследование компьютерных устройств, информационных систем и информационно-телекоммуникационных сетей;

- криминалистическое использование цифровой (компьютерной) информации, средств ее обработки и защиты.

Е.Р. Россинская говорит следующее: «система теории информационно-компьютерного обеспечения криминалистической деятельности включает в себя: теории информационно-компьютерного обеспечения криминалистической

---

[9] Вехов, В. Б. и др. Цифровая криминалистика: учебник для вузов / В. Б. Вехов; под редакцией В. Б. Вехова, С. В. Зуева. — 2-е изд., перераб. и доп. — Москва: Изда-тельство Юрайт, 2024. С. 169.
[10] Вехов, В. Б. Указ.соч.

деятельности, включая предмет теории и ее объекты; учение о способах компьютерных преступлений/правонарушений; учение о цифровых следах как источниках криминалистически значимой компьютерной информации; учение о криминалистическом исследовании компьютерных средств и систем, реализуемое в новом разделе криминалистической техники; учение об информационно-компьютерном криминалистическом обеспечении тактики следственных и судебных действий; учение об информационно-компьютерных криминалистических моделях видов компьютерных преступлений; учение об информационно-компьютерном криминалистическом обеспечении методик расследования компьютерных преступлений; учение о цифровизации системы криминалистической регистрации»[11].

Изменения, связанные с появлением новых объектов в цифровой форме, коснулись не только науки криминалистики. Закономерная теория появилась и в судебной экспертологии. Использование информационных компьютерных технологий не является чем-то новым в судебно-экспертной деятельности, однако, если раньше это ограничивалось лишь вспомогательным, технологическим аспектом, то теперь компьютерные технологии и информация стали непосредственным объектом исследования новой частной теории судебной экспертологии. Наряду с уже устоявшимися четырьмя направлениями – экспертной идентификацией, диагностикой, профилактикой и прогнозированием Е.Р. Россинская предлагает выделять теорию цифровизации: «частная теория цифровизации судебно-экспертной деятельности представляет собой систематизацию знаний об основных направлениях трансформации объектов судебных экспертиз, экспертных методологии и технологии, экспертной дидактики»[12].

---

[11] Россинская Е.Р., Семикаленова А.И., Рядовский И.А., Сааков Т.А. Теории информационно-компьютерного обеспечения криминалистической деятельности : монография / под. ред. заслуженного деятеля науки РФ, доктора юридических наук, профессора Е.Р. Россинской. — М.: Проспект, 2022. С. 26.

[12] Россинская, Е. Р. Система теории цифровизации судебно-экспертной деятельности / Е. Р. Россинская // Теория и практика судебной экспертизы. — 2024. — Т. 19. № 3. С. 22.

В криминалистике сама задача исследования не только цифровых следов, но и любых следов в принципе, сводится к «кресту следов». Так, К.Д. Поль связывал изучение следов с возможностью выявления взаимосвязи между преступником, потерпевшим, местом происшествия и орудием преступления, что в свою очередь позволяет в максимально возможных рамках воссоздать ход преступления либо реконструировать его результатами аналитических исследований[13].

Согласно всеобщим гносеологическим позициям, независимо от рода и вида объектов, все элементы процесса следообразования, позволяющие проникнуть в сущность следа как объекта познания объединяет механизм следообразования, и не важно, идет ли речь об отпечатках пальцев, следах оружия, транспортных средствах и т.д. В свою очередь, что цифровые следы появляются благодаря использованию определенного набора компьютерных средств. Следовательно, применение компьютерных средств и систем для совершения различных видов преступлений в соответствии со всеобщим законом отражения привело к формированию нового механизма следообразования, который связан с процессами возникновения, обработки и передачи компьютерной информации[14].

Рассмотрим понятие «цифровой след» более подробно.

В различных словарях предлагаются следующие трактовки термина «цифровой»:

- цифровой, цифровая, цифровое. Обозначенный цифрами, выраженный в цифрах. Цифровое выражение. Цифровое обозначение. Цифровые данные. Цифровая система[15];

- термин, описывающий информацию, выраженную при помощи чисел. Данные, такие как слова, изображения, звуки, представляются в виде набора цифр (1 и 0) в двоичной системе, которая используется в компьютерах. Понятие

---

[13] Поль, К.Д. Естественно-научная криминалистика / пер. с нем.; под общ. ред. и со вступ. ст. В.Я. Колдина. / К.Л. Поль. — М.: Юридическая литература, 1985. С. 290, 291.

[14] Россинская, Е. Р. Система теории цифровизации судебно-экспертной деятельности / Е. Р. Россинская // Теория и практика судебной экспертизы. — 2024. — Т. 19. № 3. С. 23.

[15] Ефремова Т. Ф. Новый словарь русского языка. Толково-словообразовательный. – М.: Русский язык, 2000.

«цифровой» используют также как термин, противоположный аналоговому (непрерывному) представлению данных[16];

- двоичная информация, выводимая из компьютера или терминала. В коммуникационной сфере – дискретная (импульсная) передача информации (в отличие от непрерывной аналоговой)[17].

Обзор вышеуказанных источников позволяет выделить некоторые черты, схожие для всех определений. Так, термин «цифровой» в большинстве словарей противопоставляется «аналоговому», таким образом интерпретатор обращает внимание на различия в способах передачи данных (информации).

Следующей общей чертой, характеризующей данный термин, является указание на способ «записи» таких объектов – цифровые данные представляются в виде двоичного кода. В словарях IT-терминов двоичный код имеет следующее значение: «Двоичный код (бинарный код) — система записи информации с помощью двух символов — 0 и 1. Он является основой цифровых вычислений, так как компьютеры используют внутреннюю архитектуру и операции, основанные на двоичной системе. Это обеспечивает возможность представления и обработки информации в виде электрических импульсов, с которыми работает современная вычислительная техника. Понимание двоичного кода необходимо для программирования, сетевых технологий и других областей, связанных с цифровой информацией»[18]. Можно заключить, что цифровые данные, регистрируемые при помощи двоичного кода, содержатся на компьютерах и других видах техники.

Ограничиваться лишь подобным пониманием природы цифровых данных не следует, поскольку в таком случае сущность цифровых следов сильно сужается, сводя все только к записи в виде бинарного кода. Несмотря на то, что цифровая информация существует в информационном поле и является результатом

---

[16] Научно-технический энциклопедический словарь. URL: https://rus-scientific-technical.slovaronline.com/?ysclid=mah6lznq5b462907443 (дата обращения: 06.10.2024).

[17] Справочник технического переводчика // Интент. 2009-2013. Инженерная переводческая компания. URL: https://intent.gigatran.com/ (дата обращения: 13.11.2024).

[18] Двоичный код // SkillFactory Media. Словарь IT. URL: https://blog.skillfactory.ru/glossary/dvoichnyy-kod/ (дата обращения: 20.07.2024).

компьютерной информации[19], она не может появляться сама по себе, без осознанного участия человека в данном процессе. В подтверждение данной позиции представляется уместным процитировать Ю. Хуэя: «Цифровые следы могут быть представлены в различных формах. Цифровой след является пользователю многоцветной и видимой сущностью. На уровне программирования они являются текстами; для оперативной системы они – бинарные коды; на уровне микросхем они – сигналы и т. д. С точки зрения автора, нельзя увидеть картину в целом, если понимать цифровое только как запись бинарного кода. Скорее цифровое следовало бы понимать, как новую технологию управления данными по сравнению с аналоговыми технологиями»[20].

На аспект совместного процесса создания цифрового следа как объекта обращает внимание также Е.Р. Россинская. Она выделяет цифровые следы в отдельную группу и связывает их с информацией, формирующейся в процессе работы человека с вычислительной техникой, объясняя это тем, что их образование связано со спецификой реализации информационных технологий и представлением информации в доступной для восприятия цифровой форме[21].

Такая позиция является полностью оправданной, поскольку цифровой след не способен появляться сам по себе. Поле образования цифрового следа – информационное, существующее в компьютерах, современных гаджетах, мобильных устройствах, оснащенных функциями записи голосовых фонограмм, средствами запечатления действительности при помощи камеры, и т.д. Однако стоит учитывать, что все вышеперечисленное является продуктом человеческой деятельности. Исходные параметры, вводные данные, функционал, код выполнения задачи – все это изначально задавалось компьютерам человеком для

---

[19] Ростовцев, А. В. Особенности судебно-экспертного исследования «Цифровых следов» / А. В. Ростовцев // Академическая мысль. — 2019. —№3 (8). С. 71.

[20] Боброва, Л.А., Хуэй, Ю. Что такое цифровой объект? / Л. А. Боброва, Ю. Хуэй // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 3, Философия: Реферативный журнал. — 2014. — №3. С. 387.

[21] Россинская, Е. Р. Современное состояние и перспективы цифровизации судебно-экспертной деятельности: материалы Межд. науч.-практ. конф. «Теория и практика судебной экспертизы в современных условиях» (г. Москва, 17-18 января 2019 г.). М.: РГ-Прогресс, 2019.

облегчения и автоматизации различных задач. Следовательно, даже в самом процессе создания цифрового следа, казалось бы, доведенного до автоматизма и занимающего нередко доли секунды, изначально участвуют и компьютер, и человек.

Важность указания роли человека в процессе формирования цифровых следов объясняется также тем, что цель их существования и итогового назначения – использоваться человеком. Из приведенного выше определения следует, что цифровая информация представляется в доступной для восприятия форме. Иными словами, она не создается сама по себе и сама для себя, чтобы просто где-то содержаться, такая информация в конечном итоге представляется восприятию человека. Можно сказать, что цифровой след создается в симбиозе действий человека и компьютера для того, чтобы человек имел возможность воспринимать язык компьютера наглядным, «читаемым» образом.

О.В. Гайдаш под цифровым следом понимает уникальный набор действий в интернете или на цифровых устройствах[22]. С.В. Низаева в качестве цифрового следа определяет следующее: «Под цифровым следом понимается уникальный набор действий, производимый в информационно-телекоммуникационной среде, а также информация, оставленная в результате просмотра веб-страниц»[23]. Можно согласиться с приведенными высказываниями, однако с небольшой оговоркой. Очевидно, авторы имели в виду, что под цифровым следом понимается информация о действиях, поскольку сам по себе цифровой след действием не является.

В данном случае можно провести аналогию цифрового следа с обычным. Например, при расследовании преступления назначается трасологическая экспертиза, объектом которой выступает след ботинка. По такому следу можно

---

[22] Гайдаш, О. В. Феномен цифрового следа в современном обществе / О. В. Гайдаш // Вестник магистратуры. — 2020. — №6 (105). С. 10.

[23] Низаева, С. В. Цифровые следы, виды, перспективы использования в целях раскрытия и расследования преступлений / С. В. Низаева // Государственная служба и кадры. — 2020. — №4. С. 189.

определить размер и модель обуви преступника, модель, изучить особенности походки человека по расположению следов и т.д. Точно так же и с цифровым следом в интернете.

Совершение преступления в среде информационно-коммуникационных технологий неизбежно создает вокруг преступника целое поле цифровых следов. К таким следам Ю.В. Гаврилин относит перечень следов, позволяющих установить лицо, совершившее преступление с использованием информационно-коммуникационных технологии: IP-адрес компьютера в сети, MAC-адрес сетевого оборудования, адрес электронной почты, идентификатор социальной сети, номер банковской карты, произведенные с ней транзакции, номер телефона, информация о соединениях абонента, информация базовых станций мобильной связи, данные систем геолокации и т.д.[24] Также сюда можно отнести весь перечень операций, которые были совершены лицом – посещенные страницы и сайты, выбранные для выполнения действий клавиши и их порядок, наименование поисковых запросов и др.

По мнению О.В. Флерова, цифровые следы фактически выступают «отпечатком жизни и личности человека»: основываясь на его данных, можно составить портрет пользователя – представить примерный уровень его мышления и мировоззрения, выявить его интересы и основные потребности, раскрыть его социальный статус и даже уровень интеллектуального развития и психического состояния[25].

По мнению А.А. Бессонова, «электронные следы — это информация, зафиксированная в цифровом формате, содержащаяся в электронно-вычислительных машинах и иных цифровых устройствах, созданных на основе их технологий, в средствах подвижной радиотелефонной связи и на различных носителях цифровой информации, причинно связанная с событием преступления,

---

[24] Гаврилин, Ю. В. Особенности следообразования при совершении мошенничеств в сфере компьютерной информации / Ю. В. Гаврилин // Российский следователь. — 2013. — № 23. С. 3.
[25] Флеров, О. В. Цифровой след человека в интернете: основные гуманитарные подходы / О. В. Флеров // Образовательные ресурсы и технологии. — 2018. — №4 (25). С. 80.

позволяющая установить обстоятельства совершенного преступления и преступника»[26].

Ранее нами упоминалось о том, что для восприятия цифрового следа в привычном для человека виде необходимо применение специализированных компьютерных средств и программ, позволяющих декодировать цифровой объект в графический, текстовый, аудиовизуальный формат. Данное положение обуславливает технологическую природу цифрового следа, что в свою очередь свидетельствует о материальности таких объектов.

Как известно в результате совершения преступления как общественно опасного деяния неизбежно образуется совокупность следов, которые в криминалистике принято разделять на материальные и идеальные. Если материальные следы влекут за собой изменения в элементах вещной обстановки, возникающие в результате механического, химического, иного воздействия, то идеальные следы находят свое отображение лишь в сознании людей, хранящееся в памяти человека. На первый взгляд цифровые следы, как компьютерная информация, созданная в Интернет-сети, на серверах, дампах памяти и т.д. и представленная в виде записи бинарного кода, могут представляться как следы виртуальные. Однако с таким мнением можно поспорить, поскольку в конечном итоге у цифровых следов есть определенное «место», где они существуют.

Данный вопрос уже на этапе формирования теории о цифровизации нашел неоднозначное отражение среди ученых и исследователей. Например, такой позиции придерживается В.А. Мещеряков, называя цифровые следы виртуальными, что он объясняет следующим: «в искусственной, электронно-цифровой среде происходит не напрямую, а опосредованно, через целую иерархию формализованных (математических) моделей, используемых для описания реальных физических явлений. Наблюдая цифру/число, но ничего не зная о

[26] Бессонов, А. А. О некоторых возможностях современной криминалистики в работе с электронными следами / А. А. Бессонов // Вестник Университета имени О.Е. Кутафина (МГЮА). — 2019. — №3. С.47.

формализованной модели, положенной в основу электронно-цифрового отражения, мы не сможем понять, как она связана с событием преступления, и, как следствие, она не может рассматриваться в качестве следа. С точки зрения криминалистики важным является тот факт, что один и тот же объект или явление может быть зафиксировано с использованием различных формализованных (математических) моделей»[27].

В противовес указанным положениям следует привести иную точку зрения, принадлежащую Е.Р. Россинской, согласно которой цифровые следы являются не виртуальными, а материальными: «цифровые следы нельзя отделять от традиционных по характеру следов-отображений, ведь помимо них в трасологии есть большое количество следов, которые на первый взгляд неочевидно связаны с преступлением, но при исследовании которых для нахождения их связи с событием преступления используются технологии, представляющие собой формализованные модели»[28]. В подтверждение этому А.Н. Савенков и Е.Р. пишут следующее: «в качестве примера можно взять молекулярно-генетические, пожарно-технические, взрывотехнические исследования, где один и тот же объект или явление может быть зафиксировано с использованием различных формализованных (математических) моделей»[29].

В.А. Штофф относительно гносеологической природы моделей говорит: «Модели являются гносеологическим отражением постольку, поскольку условием их формирования, построения и использования в процессе познания являются либо физическое подобие, либо аналогия, либо изоморфизм... С фактической (технической, логической, математической стороны) любая модель представляет

---

[27] Мещеряков, В.А. Теоретические основы механизма следообразования в цифровой криминалистике: монография / В.А. Мещеряков. — М.: Проспект, 2022. С. 105, 106.

[28] Россинская Е. Р. Теория информационно-компьютерного обеспечения криминалистической деятельности: концепция, система, основные закономерности // Вестник Восточно-Сибирского института МВД России. — 2019. — № 2 (89). С. 196.

[29] Савенков, А. Н., Россинская, Е. Р. Актуальные направления развития общей теории криминалистики сквозь призму современных технологий / А. Н. Савенков, Е. Р. Россинская // Государство и право. — 2024. — № 10. С. 162.

собой по меньшей мере образ объекта»[30]. Н.П. Майлис отмечает, что: «…компьютерное моделирование используется в классической трасологии для лучшего воспроизведения признаков следообразующего объекта»[31].

Стоит обратить внимание на механизм следообразования, который может ошибочно рассматриваться как исключительно электронный. Раз сами цифровые следы являются материальными и по происхождению технологическими, поскольку их формирование обусловлено спецификой реализации информационных технологий, то и для их преобразования в доступную для восприятия форму также используются информационные технологии.

Следовательно, по механизму следообразования цифровые следы могут быть отнесены к электронным либо электромагнитным в зависимости от носителя, на котором они отображены — твердотельном либо на магнитных дисках. Но возможны и механические следы — образуются в структуре материала оптического диска под воздействием лазерного луча. Исходя из этого неправильно называть сами следы электронными или электронными носителями информации. Однако в положениях статьи 164.1 УПК РФ отражаются особенности изъятия электронных носителей информации и копирования с них информации при производстве следственных действий, в то время как речь очевидно идет о цифровых следах. Таким образом, при работе с данной статьей следователи, судьи, правоприменители могут ошибочно принимать одно за другое, что безусловно требует корректировки со стороны законодательства.

Обобщая все вышесказанное и возвращаясь к криминалистическому «кресту следов», представляется уместным привести позицию Е.Р. Россинской, которая предлагает ввиду появления цифровых следов скорректировать существующую взаимосвязь между компонентами механизма следообразования, добавляя туда

---

[30] Штофф, В. А. Моделирование и философия / В. А. Штофф. — М. — Л.: Издательство «Наука», 1966. С. 148.

[31] См.: Майлис, Н. П. Цифровая трасология: современное состояние и пути решения проблем / Н. П. Майлис // Роль права в обеспечении благополучия человека: сб. докладов XXII Междунар. науч.-практ. конф.: в 5 ч. М. — 2022. — Ч. 4. — С. 490-494.

технологии исследования: «…цифровые следы вписываются в схему «креста следов», поскольку таким же образом, как и остальные разновидности следов, они связывают субъект со средством и местом совершения преступного посягательства на конкретный предмет, следовательно, цифровые следы могут содержать информацию обо всех элементах «креста следов»[32].

Поскольку криминалистика является обосновывающим знанием для всех судебных экспертиз, то приведенное выше учение о механизме следообразования можно считать подходящим и для судебной экспертологии. В своем исследовании мы склоняемся к определению цифрового следа из криминалистики, которое неоднократно приводилось ранее.

Цифровым следам присущи следующие характеристики:

- во-первых, цифровой след содержит в себе цифровую информацию или цифровые данные, в которых заключаются сведения о действии, предмете, продукте, явлениях действительности;

- во-вторых, цифровой след создается в результате совместных действий человека и компьютера (гаджета, мобильного устройства, другого устройства), не создается сам по себе;

- в-третьих, цифровой след обеспечивает представление цифровой информации в доступной для восприятия форме;

- в-четвертых, цифровой след может быть создан как в интернете, так и за его рамками – в компьютерных программах, с помощью мобильных устройств и т.д.;

- в-пятых, как правило, цифровой след является результатом преобразования информации в конкретную форму. Однако, не стоит упускать из виду такой вид непреобразованной цифровой информации, как цифровой мусор. Цифровой мусор – это ненужные и забытые данные, копии файлов, многочисленные копии файлов, кеш приложений, вся неструктурированная информация в облачных хранилищах,

---

[32] Савенков, А. Н., Россинская, Е. Р. Актуальные направления развития общей теории криминалистики сквозь призму современных технологий / А. Н. Савенков, Е. Р. Россинская // Государство и право. — 2024. — № 10. С. 165.

памяти устройств, мессенджерах, фото- и видеосервисах[33]. Представленное определение в смысловом аспекте соответствует сущности цифрового мусора, но не соотносится с его спецификой в экспертном понимании, поскольку оно сформулировано с точки зрения программирования.

А.А. Саркисян выделяет цифровой мусор как отдельный вид цифровых следов, давая ему следующее определение: «Цифровой мусор – это поврежденные или остаточные записи с дефектами структуры цифровых следов, которые образуются в результате повреждения / самоповреждения / фрагментации цифрового следа вследствие нарушения алгоритма его работы, т. е. это цифровые следы, которые уже не несут в себе первоначальной информации и существуют лишь набором остаточных и зачастую несвязных частей машинного кода»[34]. Также А.А. Саркисян отмечает: «Цифровой мусор представляет собой именно самостоятельный объект, поскольку он обладает своими свойствами и признаками, которые необходимо проанализировать, чтобы диагностировать причину его повреждения, установить его первоначальную форму, а также смоделировать процесс его повреждения»[35]. Данная дефиниция представляется нам более корректной и соответствующей экспертной специфике, поскольку изучение цифрового мусора экспертом может впоследствии привести к экспертной ошибке или наоборот предотвратить ее совершение.

Среди свойств цифровых следов необходимо упомянуть легкоизменяемость. Относительная простота алгоритма создания виртуальной среды в целом и цифровых данных в частности, минимальные затраты и небольшой арсенал средств, участвующих в процессе создания цифровых следов, повсеместная автоматизация – все это значительно упрощает возможность внести в цифровой след при желании любые изменения. Фотографии, аудиовизуальные файлы

---

[33] Цифровой мусор // Словарь «Makves». URL: https://makves.ru/blog/slovar-cifrovoy-musor/ (дата обращения: 26.07.2024).
[34] Саркисян, А. А. Цифровизация судебно-экспертной деятельности: теоретические, правовые и организационные аспекты : дис ...канд. юрид. наук : 5.1.4 / Саркисян Анна Ашотовна. — М., 2023. С. 98.
[35] Там же, С. 99.

подвержены содержательному изменению благодаря существованию специализированных приложений и редакторов. Файлы форматов word и pdf без труда можно отформатировать даже незаметным для глаза образом в тех же программах, в которых эти файлы создавались, что является уязвимым местом цифровых следов.

Цифровые следы изменчивы, процесс внесения корректировок быстрый, тяжело отслеживается и выявляется. Простоту видоизменения цифрового следа обеспечивает цифровая (виртуальная) среда, в которой они пребывают. Исследователи уже работают над решением данной проблемы. Например, на данный момент активно используется технология блокчейнов, что будет рассмотрено во второй главе.

Виды цифровых следов. В качестве цифровых следов могут выступать:

- данные из мобильных устройств, компьютеров и облачных хранилищ;

- вредоносные ПО, фишинговые сайты и программы, вирусы (троянские кони и т.д.);

- сообщения, отправленные и полученные по электронной почте;

- чаты и переписки в мессенджерах (WhatsApp, Telegram, Viber и др.), переписка и комментарии в системах управления проектами (например, Trello, Asana);

- информация, размещенная в социальных медиа, страницы, посты, блоги на различных платформах, сообщения на интернет-форумах;

- запросы и результаты интернет-поиска, которые могут быть использованы для анализа интересов и намерений пользователей;

- электронные финансовые документы и другие объекты судебных экономических, финансовых, бухгалтерских экспертиз. Например, электронные счета, контракты, накладные и другие финансовые документы, хранящиеся в цифровом формате. Также среди таких объектов можно выделить данные из бухгалтерских программ (например, 1С, SAP и др.), которые могут содержать информацию о финансовых операциях, начислениях, расчетах с контрагентами и

т.д. Сюда же относятся электронные платежные системы, данные транзакций из таких систем, как PayPal, Яндекс.Деньги, Qiwi и др.; информация из систем управления взаимоотношениями с клиентами (CRM), которая может содержать данные о продажах, контрактах и взаимодействиях с клиентами;

- аудио-, фото- и видеозаписи, видеозаписи с камер наблюдения, записи телефонных разговоров или видеозаписи, содержащие диалоги, которые могут быть проанализированы для выявления манипуляций, угроз или других намерений;

- криптовалюты и другие цифровые активы;

- подписи, выполненные на планшетах и гаджетах и др.

А.И. Семикаленова, обозначая цифровой след как декодированную цифровую информацию, выделяет следующие виды цифровых следов: «Сегодня цифровыми следами являются дампы оперативной памяти и дампы трафиков, файлы и их обрывки, создаваемая программными и аппаратным средствами их получения служебная информация о этих файлах, располагающиеся на материальных носителях информации в виде цифровых кодированных последовательностей»[36].

В последние годы тенденция к минимизации рукописного письма и распространению использования информационных технологий для создания текстов, записей и даже подписей, привела к тому, что в области ряда экспертиз, в первую очередь, почерковедческих и компьютерно-технических, появились новые объекты исследования.

В качестве одного из подобных объектов рассмотрим клавиатурный почерк. Под клавиатурным почерком предлагается понимать следующее: «Это основанная на печатно-двигательном функционально-динамическом комплексе навыков и получающая отображение в печатных символах программа их выполнения, содержащая субъективный и объективный зрительно-двигательные образы набираемых символов, и специально приспособленную для их реализации систему

[36] Семикаленова, А. И. Цифровые следы: назначение и производство экспертиз / А. И. Семикаленова // Вестник Университета имени О. Е. Кутафина. —2019. — №5 (57). С. 117.

движений»[37]. Автором предлагается рассматривать компьютерный почерк не с технологической точки зрения, а криминалистической, обуславливая это тем, что анализ клавиатурного почерка человека позволяет выявить целый комплекс важных признаков. Например, традиционные для почерковедения признаки (степень выработанности); темп набора; скорость печати; динамика ввода; сила нажатия; наличие или отсутствие системных опечаток с изучением последующих моделей внесения исправлений; использование определенных букв, символов и «горячих клавиш»; характер наложений. Компьютерный почерк, как и обычный, подвергается воздействию различных факторов, среди которых эксперты могут выявить психоэмоциональное и физиологическое состояние исполнителя; характер набираемого текста, его содержимое; степень вовлеченности, привычность клавиатуры и т.д.

А.Д. Цветкова выделяет следующие объекты комплексной экспертизы компьютерного (клавиатурного) почерка:

а) технические, включающие в себя компьютер; клавиатуру; устройство, фиксирующее информацию о почерке (аппаратный перехватчик клавиатуры, диктофон, видеокамера); носитель цифровой информации, содержащий операционную систему, в которой осуществлялась работа с текстом; данные программного перехватчика клавиатуры и пр.;

б) почерковедческие, к которым относятся технически полученные и переведенные в языковую форму записи, фиксирующие особенности почерка («переводы» кодов и функций, расшифровки аудиограмм, аналитические карты видеозаписей), видеоматериалы и спорный текст. Несмотря на то что в рассматриваемой ситуации итоговые материалы не отражают видимых признаков почерка исполнителя, совмещение текста с описанием того, как он был набран, облегчит проведение экспертизы[38].

---

[37] Цветкова, А. Д. Криминалистическое исследование компьютерного (клавиатурного) почерка / А. Д. Цветкова // Электронное приложение к Российскому юридическому журналу. — 2022. — №2. С. 59.

[38] Цветкова А.Д. Указ.соч.

Отличающимися цифровыми следами, которые могут исследоваться в области судебного почерковедения, Н.Ф. Бодров и Е.Р. Россинская предлагают считать удостоверительные записи и подписи, выполняемые на экранах мобильных устройств, планшетов, специализированных терминалов и т.д. Так, авторы говорят следующее: «С учетом положений частной теории о цифровизации судебно-экспертной деятельности[39], такие подписи и записи являются образами цифровых следов, представленными в виде криминалистически значимой компьютерной информации о реализации письменно-двигательного функционально-динамического комплекса навыков, отраженной в материальной среде, в процессе ее возникновения, обработки, хранения и передачи»[40].

Помимо предложенных видов цифровых следов следует рассматривать и другие. Виды цифровых следов обусловлены бесчисленным количеством действий и операций, совершаемых на просторах информационно-телекоммуникационных сетей. Каждое из таких действий приводит в результате к формированию определенного набора цифровой информации, метаданных, облеченных в какую-то форму – страницу, сайт, набор сведений и т.д. А.А. Ананьев и В.Х. Худяков пишут: «Цифровые следы представляют собой информацию, оставляемую человеком в результате использования сети Интернет. Они являются «отпечатком жизни личности человека», своего рода совокупностью индивидуально-психологических характеристик, потребностей и личностных черт человека. По своему содержанию цифровые следы представляют собой некую совокупность неструктурированных или сложно структурированных данных, хранящих разнообразную и разностороннюю, собранную по крупицам, информацию об

---

[39] Россинская Е.Р., Семикаленова А.И., Рядовский И.А., Сааков Т.А. Теории информационно-компьютерного обеспечения криминалистической деятельности : монография / под. ред. заслуженного деятеля науки РФ, доктора юридических наук, профессора Е.Р. Россинской. — М.: Проспект, 2022. С. 160.

[40] Россинская, Е. Р., Бодров, Н. Ф. Современное состояние и перспективы исследования образов цифровых следов в судебной почерковедческой экспертизе / Е. Р. Россинская, Н. Ф. Бодров // Криминалистика: вчера, сегодня, завтра. — 2022. — Т. 21. — № 1. С. 127.

использовании глобальной информационной сети конкретной личностью»[41]. Таким образом, любой цифровой след является совокупностью конкретных данных, содержащих в себе информацию о действиях, совершаемых лицом в интернете.

Среди исследователей сформировалась точка зрения, согласно которой цифровые следы можно подразделять на активные и пассивные. Так, в пункте 4.7 Концепции комплексного регулирования (правового регулирования) отношений, возникающих в связи с развитием цифровой экономики, подготовленной на основе отчета Института законодательства и сравнительного правоведения при Правительстве РФ, выделяются два вида цифрового следа:

- активный цифровой след формируется самим пользователем, который намеренно оставляет в информационных системах о себе различную информацию;

- пассивный цифровой след образуют данные, которые оставляются ненамеренно или вследствие работы программного обеспечения[42].

Активный цифровой след создается в результате целенаправленных действий человека во время использования различного рода информационно-телекоммуникационных ресурсов: образовательных, экономических, развлекательных и т.д. В качестве таких следов можно рассматривать:

- публикации в социальных сетях, посты, треды, записи из блогов, обзоры на форумах, комментарии и отзывы под карточками товаров на маркетплейсах;

- сведения о покупках товаров и услуг через интернет-ресурсы;

- авторизация, регистрация личной страницы или профиля на сайтах или в социальных сетях, содержащая перечень личных данных лица, которые он вводит самостоятельно;

---

[41] Худяков, В. В., Ананьев, А. А. Цифровые следы / В. В. Худяков, А. А. Ананьев // Криминологический журнал. — 2023. — №4. С. 244.

[42] Концепция комплексного регулирования (правового регулирования) отношений, возникающих в связи с развитием цифровой экономики // Некоммерческая организация «Фонд развития центра разработки и коммерциализации новых технологий». URL: https://webcache.googleusercontent.com/search?q=cache:ZUfngxYZ6X0J:https://sk.ru/documents/358/ (дата обращения: 29.07.2024).

- личная переписка в мессенджерах социальных сетей, отдельных приложений, специализированных сервисов (email, gmail и т.д.);

- «cookie»-файлы. Cookie-файлы являются обычными текстовыми файлами, хранящимися на компьютере человека. Сохраняются они веб-сайтами с помощью браузера[43].

В отличие от активного цифрового следа, пассивный создается без ведома человека. Основными источниками получения пассивных цифровых следов выступает большинство мобильных устройств и иных гаджетов (умные часы и т.д.), которые в процессе работы записывают информацию о своем владельце. Еще одним способом образования пассивного цифрового следа является сбор статистики посещения пользователем конкретного сайта, запоминание его IP адреса, анализ предпочтений. По такой схеме работает большинство современных приложений, направленных на предоставление контента развлекательного и досугового характера. В результате предпочтений лица, которые выражаются в анализе частоты просмотров контента схожего характера, переходов и лайков, формируется лента рекомендаций. Помимо приведенной классификации нужно также учитывать цифровой мусор, являющийся самостоятельным видом цифровых следов.

В словаре Общества Американских Архивистов (Society of American Archivists) содержится следующее определение цифровых следов: «Цифровой след – это информация в двоичной форме и связанные с ней метаданные. Цифровые следы могут быть простыми и сложными. Простые цифровые следы состоят из одного файла, например, PDF-файла или изображения, тогда как сложные цифровые следы состоят из нескольких файлов, например, веб-сайт или оцифрованная книга. В любом случае цифровые следы включают в себя информационный контент, а также метаданные, которые поддерживают

[43] Худяков, В. В., Ананьев, А. А. Цифровые следы / В. В. Худяков, А. А. Ананьев // Криминологический журнал. — 2023. — №4. — С. 245.

администрирование, доступ и хранение»[44]. Мы видим, что в основу классификации американские ученые закладывают количественный критерий. По их мнению, простым цифровым следом предлагается считать такой след, который содержится в одном файле – одно фотоизображение, одна PDF-страница. Собрание PDF-страниц, например, книга, уже является сложным цифровым следом, так как состоит из нескольких простых файлов. Примером сложного цифрового следа нами предлагается считать веб-сайты. Даже те сайты, которые состоят формально из одной страницы и не содержат большого количества функциональных вкладок, создаются посредством объединения большого количества кодов, адресных строк и иных метаданных.

Важность изучения особенностей цифровых следов связана с тем, что такие следы не только способны выступать способом совершения преступления, но и могут также являться объектом преступного посягательства. В качестве такого примера можно привести Определение Верховного Суда Российской Федерации от 22 января 2021 г. по делу № А55-23131/2018. Так, в качестве объектов преступного посягательства выступили такие цифровые следы, как доменное имя и веб-сайт. Компания «XXX» обратилась в Арбитражный суд Самарской области с исковым заявлением к ответчику ФИО о признании регистрации, администрирования и использования доменного имени «ecolabhealthcare.ru», а также использования веб-сайта «www.ecolabhealthcare.ru» нарушением прав истца на товарные знаки и фирменное наименование, об обязании пресечь нарушение исключительных прав истца на товарные знаки и фирменное наименование путем запрета ответчику использовать (администрировать) доменное имя, а также веб-сайт, о взыскании компенсации за незаконное использование товарных знаков в размере 3 000 000

[44] Digital object // Archives Terminology. URL: https://dictionary.archivists.org/entry/digital-object.html (дата обращения: 26.07.2024 г.).

руб., а также о признании порочащими деловую репутацию истца сведений, опубликованных на сайте ответчика[45].

В рамках уголовного судопроизводства был вынесен Приговор Октябрьского районного суда г. Саранска (Республика Мордовия) № 1-236/2023 от 21 декабря 2023 г. по делу № 1-236/2023, на основании которого гражданин А был признан виновным в совершении восьми преступлений, предусмотренных ч. 4 ст. 159 и восьми преступлений, предусмотренных ч. 2 ст. 187 УК РФ. В комплекс основных мероприятий и действий, непосредственно направленных на реализацию возникшего преступного умысла, входило использование находящихся в распоряжении лица № 1 систем электронных расчетов, прикрепленных к расчетным счетам ООО «Памир», ООО «Эльбрус» и ИП П1., в том числе системы дистанционного банковского обслуживания «Клиент-Банк» и электронной цифровой подписи директора ООО «Памир» и ООО «Эльбрус» П2. и ИП П1[46].

По возможности получения доступа к цифровым следам, их можно подразделить на:

- находящиеся в свободном доступе;

- ограниченные в доступе;

- зашифрованные (например, доступ к цифровому следу невозможен без ввода специального ключа).

В зависимости от субъекта процесса, который является собственником (владельцем) цифрового следа или на хранении которого они находятся:

- цифровые следы, содержащиеся на материальном носителе потерпевшего;

---

[45] Определение Верховного Суда Российской Федерации от 22.01.2021 № 306-ЭС20-21597 по делу № А55-23131/2018 // Картотека арбитражных дел «Мой арбитр». — URL: https://goo.su/du2HQ (дата обращения: 30.07.2024 г.).

[46] Приговор Октябрьского районного суда г. Саранска Республики Мордовия от 21.12.2023 № 1-236/2023 г. по делу № 1-236/2023 // Судебные и нормативные акты РФ (СудАкт). — URL: https://sudact.ru/regular/doc/cndyay1eS8UK/?regular-txt=%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%BE%D0%B9+%D1%81%D0%BB%D0%B5%D0%B4&regular-case_doc=&regular-lawchunkinfo=&regular-date_from=&regular-date_to=&regular-workflow_stage=&regular-area=&regular-court=&regular-judge=&snippet_pos=1310#snippet (дата обращения: 30.07.2024 г.).

- цифровые следы, содержащиеся на материальном носителе подозреваемого/обвиняемого;

- цифровые следы, содержащиеся на материальном носителе свидетеля;

- цифровые следы, содержащиеся на материальном носителе операторов связи;

- цифровые следы (например, запись с видеокамеры) содержащиеся на материальном носителе, принадлежащем юридическому лицу, и запечатлевшие событие правонарушения или иные сведения, имеющие значение для расследования и рассмотрения дела;

- цифровые следы, содержащиеся на материальном носителе, принадлежащем муниципалитету, входящие в состав комплекса технических и программных средств для совместной работы городских ведомств и служб по предотвращению и устранению последствий происшествий, которые вредят природе или человеку (система «Безопасный город»).

Анализируя приведенные выше виды цифровых следов, способы их создания и особенности, можно заключить, что все они существуют не отдельно, сами по себе, а содержатся на каком-то носителе. В качестве форм существования цифровых следов можно выделить следующие:

- цифровые следы – на отдельных носителях, например, на жестком магнитном диске (HDD), флеш-накопителе и др.;

- цифровые следы в компьютерных системах и сетях, мобильных коммуникаторах, планшетах, на серверах, в облачных хранилищах;

- электронные (цифровые) документы;

- образы цифровых следов, отображаемые в цифровом виде с помощью различных программных продуктов;

- образы цифровых следов, отображаемые на бумажных носителях, например, распечатки скриншотов, распечатки электронных документов и др.

Таким образом, цифровой след содержится на конкретном носителе. А.И. Семикаленова и Е.Р. Россинская, описывая особенности цифровых доказательств,

утверждают следующее: «Данные манипуляции с доказательствами, создаваемыми, распространяемыми, хранимыми в компьютерных средствах и системах, возможны в силу того, что к ним применимо понятие двуединства существования: одно — это существование следов на конкретном материальном носителе в виде зафиксированной различными физическими методами информации, а другое — их способность перемещаться с этих физических носителей практически без изменения на другие носители, зачастую сохраняясь на них с помощью совершенно других технологий»[47].

В подтверждение тому, что цифровые следы не могут существовать с отрывом от носителя, следует подчеркнуть материальную природу цифровых следов. Таковыми они являются как раз потому, что, в отличие от чего-то виртуального, они содержатся на материальном носителе.

Следует выделить следующие категории объектов, которые могут быть носителями криминалистически значимой компьютерной информации:

— устройства хранения информации;

— устройства ввода/вывода информации;

— устройства обработки информации;

— устройства передачи информации по каналам связи;

— информационные комплексы и системы.

Все перечисленные виды объектов содержат цифровые следы, могут продуцировать собственные цифровые следы и участвуют в формировании криминалистически значимой компьютерной информации[48].

Таким образом, существующие в законодательстве понятия «электронный носитель информации» и «электронный след» не учитывают всех характеристик и

---

[47] Россинская, Е. Р., Семикаленова, А. И. 2020. Основы учения о криминалистическом исследовании компьютерных средств и систем как часть теории информационно-компьютерного обеспечения криминалистической деятельности / Е. Р. Россинская, А. И. Семикаленова // Вестник Санкт-Петербургского университета. Право 3. — 2020. — Том. 11. №3. С. 747.

[48] Россинская, Е. Р., Семикаленова, А. И. 2020. Основы учения о криминалистическом исследовании компьютерных средств и систем как часть теории информационно-компьютерного обеспечения криминалистической деятельности / Е. Р. Россинская, А. И. Семикаленова // Вестник Санкт-Петербургского университета. Право 3. — 2020. — Том. 11. №3. С. 747.

содержания самого носителя, сужая физическую природу цифровых следов и носителей до электронных. Однако, электронными являются только носители с флеш-памятью, помимо них существуют электромагнитные, электрические, магнитные, оптические, механические свойства. Предлагается использовать термин «цифровой объект», отражающий реальную физическую природу цифровых объектов, а именно – объединяет существующие в экспертологии и компьютерных науках понятия цифрового следа и носителя.

Подробное изучение цифровых следов, присущих им свойств и характеристик, а также видов и форм, позволяет нам сформулировать авторское определение понятия «цифровой объект», применимое в судебной экспертологии и судебно-экспертной практике, которое в дальнейшем будет взято за основу в рамках диссертационной работы. Итак, учитывая все вышесказанное, под цифровым объектом предлагается понимать следующее: ***цифровой объект*** *– это объект судебно-экспертного исследования, состоящий из цифровых следов разных видов, находящихся на объекте-носителе.* Во избежание путаницы сразу оговоримся, что понятия «цифровой объект» и «объект в цифровой форме» являются тождественными.

Самым главным критерием для определения цифрового объекта как сочетания цифрового следа и материального носителя является обязательность указания на двойственную природу таких объектов.

Существует также отдельный вид цифровых объектов. Речь идет об электронных (цифровых) документах. Тенденция к глобальной цифровизации повлекла за собой переворот в сфере судопроизводства, имеющий как положительные, так и отрицательные стороны. Удобству работы с процессуальными документами и упрощению процесса документооборота противостоит появление недопонимания между различными органами власти и суда при определении статуса цифрового документа. Представляется важным разобраться, что входит в понятие цифрового документа, а также изучить ошибки, возникающие при неправильной трактовке этого термина.

При исследовании понятия «цифровой документ» необходимо отметить следующее. В силу того, что в научной терминологии понятие «цифровой документ» пока встречается не так часто, в рамках нашей диссертации будут использованы определения электронного документа только для того, чтобы сформировать общие представления о цифровых документах. Это также объясняется тем, что термин «цифровой» пришел на замену «электронному» относительно недавно, что находит свое отражение в нормативно-правовых актах. Так, Федеральная цифровая программа «Электронная Россия (2002–2010 годы)» была утверждена постановлением Правительства Российской Федерации от 28 января 2002 г. №65[49]. Несмотря на то, что период действия данной программы датируется с 2002 по 2010 год, фактически первое упоминание о «цифровой» России приходится на 2017 год. Программа «Цифровая экономика Российской Федерации» была утверждена распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р[50]. Также в рамках реализации Указов Президента Российской Федерации от 7 мая 2018 г № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года»[51] и от 21.07.2020 г. № 474 «О национальных целях развития Российской Федерации на период до 2030 года»[52], в том числе с целью решения задачи по обеспечению ускоренного внедрения цифровых технологий в экономике и

---

[49] О федеральной целевой программе «Электронная Россия (2002 - 2010 годы) : Постановление Пленума ВС РФ № 65 : принято Пленумом ВС РФ 28 января 2002 г.: послед. ред. 09.06.2010 г. // КонсультантПлюс : сайт. URL: http://consultant.ru/document/cons_doc_LAW_90180/ (дата обращения: 13.02.2025).

[50] Об утверждении программы «Цифровая экономика Российской Федерации» : Распоряжение Правительства РФ № 1632-р : принято Правительством РФ 28 июля 2017 г. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_221756/ (дата обращения: 13.02.2025).

[51] Указы Президента Российской Федерации. О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года : Указ Президента РФ № 204 : принят Президентом РФ 07 мая 2018 г.: послед. ред. 21.07.2020 г. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_297432/ (дата обращения: 13.02.2025).

[52] Указы Президента Российской Федерации. О национальных целях и стратегических задачах развития Российской Федерации на период до 2030 года и на перспективу до 2036 года : Указ Президента РФ № 309 : принят Президентом РФ 07 мая 2024 г. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_475991/ (дата обращения: 13.02.2025).

социальной сфере, Правительством Российской Федерации сформирована национальная программа «Цифровая экономика Российской Федерации» утвержденная протоколом заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 4 июня 2019 г. № 7. Паспорт Федерального проекта «Нормативное регулирование цифровой среды» начинает отчет о деятельности с 30.06.2021 года. Все это свидетельствует о том, что в последние два десятилетия на законодательном уровне преимущественно употреблялся термин «электронный», что и объясняет его преобладание над словом «цифровой».

Таким образом, государство уже положило начало эре цифровой среды, в силу чего и конечное понятие, которое мы будем формировать, будет свключать в себя термин «цифровой», а не «электронный».

В первую очередь, следует обратиться к нормативным правовым актам, разъясняющим понятие электронного документа. Так, в ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» содержится следующее определение: «Электронный документ – это документированная информация, которая представлена в электронной форме: то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также – для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах»[53]. Подобное понятие электронного документа содержится и в ГОСТ Р 7.0.8-2013: «Электронный документ – это документ, информация которого представлена в электронной форме»[54]. Для того чтобы разобраться, насколько полноценно указанные понятия передают сущность цифрового документа,

[53] Об информации, информационных технологиях и о защите информации : Федер. закон № 149-ФЗ : принят Государственной Думой 8 июля 2006 г. : одобрен Советом Федерации 14 июля 2006 г. : послед. ред. // КонсультантПлюс : сайт. URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 13.02.2025).

[54] ГОСТ Р 7.0.8-2013 «Делопроизводство и архивное дело. Термины и определения». Раздел 3». — Москва : Стандартинформ, 2014. — 16 с.

необходимо выделить его основные характеристики, без которых сам термин «цифровой» не будет оправдан.

Любой цифровой документ – это документ, и такое уточнение необходимо указывать, поскольку неправильное толкование изначальной природы документа может значительно сузить круг того, что может входить в понятие электронного документа. Согласно ст. 1 Федерального закона от 29.12.1994 № 77-ФЗ «Об обязательном экземпляре документов» под документом понимается материальный носитель с зафиксированной на нем в любой форме информацией в виде текста, звукозаписи, изображения и (или) их сочетания, который имеет реквизиты, позволяющие его идентифицировать[55]. Следовательно, любой текст, аудио-, видеозапись, изображение или их сочетание, представленное в цифровом виде, вправе считаться цифровым документом.

Во-вторых, приведенные выше определения дают указания на способы создания и передачи таких документов:

- документ может стать цифровым при переводе информации с бумажного носителя на цифровой посредством средств сканирования, в случае с аудио-, видеозаписями и изображениями – при помощи USB-накопителей, флеш-карт и т.д.;

- документ может не иметь бумажного предшественника и быть создан изначально в виртуальной среде при помощи различных программ.

В-третьих, информация, содержащаяся в таком документе, может передаваться по информационно-телекоммуникационным сетям и обрабатываться в информационных системах.

Таким образом, в основу понятия цифрового документа входит перечень содержащейся в нем информации, способ создания (первичный или вторичный) и возможность его использования, поскольку само существование цифрового

---

[55] Об обязательном экземпляре документов : Федер. закон № 77-ФЗ : принят Государственной Думой 23 ноября 1994 г. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_112701/ (дата обращения: 13.02.2025).

документа предполагает расширение перечня совершаемых с ним операций при помощи ЭВМ.

О связи ЭВМ и цифровых документов, а также касаемо обоснованности выделения цифрового документа как принципиально нового явления, высказывалась М.П. Бобылева: «выявленные в ходе тщательного анализа многоаспектные и системные различия между цифровыми и бумажными документами свидетельствуют о качественно новой природе цифровых документов»[56].

В Постановлении Пленума Верховного Суда РФ (далее – ППВС РФ) от 26.12.2017 № 57 «О некоторых вопросах применения законодательства, регулирующего использование документов в электронном виде в деятельности судов общей юрисдикции и арбитражных судов» содержится следующее определение электронного документа: «Документ в электронном виде – это электронный образ документа или электронный документ. Электронный образ документа – это переведенная в электронную форму с помощью средств сканирования копия документа, изготовленного на бумажном носителе, которая заверена электронной подписью в порядке, установленном законодательством Российской Федерации. Электронный документ – это документ, который создан в электронной форме без предварительного документирования на бумажном носителе, и подписан электронной подписью в порядке, установленном законодательством РФ»[57].

Из приведенного понятия следует, что Пленумом Верховного Суда обозначается возможность существования двух способов создания цифрового документа, однако с оговоркой на то, что в случае перевода информации с уже

---

[56] Бобылева, М.П. Управленческий документооборот: от бумажного к электронному: монография / М. А. Бобылева. — М.: ООО «ТЕРМИКА.РУ», 2023. С. 32.

[57] О некоторых вопросах применения законодательства, регулирующего использование документов в электронном виде в деятельности судов общей юрисдикции и арбитражных судов : Постановление Пленума ВС РФ № 57 : принято Пленумом ВС РФ 26 декабря 2017 г. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_286321/ (дата обращения: 13.02.2025).

существующего бумажного носителя на цифровой, это будет всего лишь цифровым образом документа. На наш взгляд, такой подход является не совсем правильным. В первую очередь, это создает путаницу при работе судов с юридическими терминами, которых и без того немало. Во-вторых, использование термина «образ» в данном случае не совсем корректно. В словарях понятие «образ» имеет множество значений и может трактоваться как воспроизведение чего-либо, подобное первоначальному объекту, но не являющееся им[58]. Встречается и такое определение образа, как облик, вид, подобие чего-либо, живого, наглядного представления о ком или чем-нибудь[59]. По нашему мнению, использование термина «образ» в данном случае не подходит, поскольку документ, переведенный в цифровой формат, остается тем же самым документом, меняя только форму, а не содержание, тогда как образ обозначал бы лишь внешнее сходство бумажного и цифрового содержимого документа, цифровое подобие содержимого бумажного носителя.

Разграничение на цифровой документ, весь жизненный цикл которого протекает в цифровой среде, и цифровую копию документа, оцифрованного с бумажного носителя, не обязательно потому, что в конечном итоге и первый, и второй документ приобретает статус цифрового, может быть всячески отформатирован при помощи ряда средств и программ, однако с небольшими операционными различиями. Содержание и правовой статус документа как доказательства у этих двух документов будет одинаков[60].

Особое внимание стоит уделить характеристикам, которыми ППВС наделяет электронный документ. Он вводит обязательный реквизит, который должен содержаться в электронном документе, – электронную подпись. Такая подпись

---

[58] Словарь русского языка: В 4-х т. / РАН, Ин-т лингвистич. исследований; Под ред. А. П. Евгеньевой. — 4-е изд., стер. — М.: Рус. яз.; Полиграфресурсы, 1999; (электронная версия): Фундаментальная электронная библиотека.

[59] Ефремова Т. Ф. Новый словарь русского языка. Толково-словообразовательный. – М.: Русский язык, 2000.

[60] Шихалиева С.З. Проблема определения понятия электронных доказательств: законодательные и судебно-практические аспекты/ С. З. Шихалиева // Российский судья. — 2024. — № 9. С. 38.

прилагается к основному документу в виде отдельного файла, являясь необходимым элементом и для текстовых документов, и для электронных переписок, для фотоизображений и т.д. Указание на необходимость наличия электронной подписи идет вразрез с разъяснениями Верховного Суда касательно работы судов с таким видом электронных документов, как скриншоты. Об этом говорит судебная практика, а также ППВС РФ № 10 от 23 апреля 2019 г. «О применении части четвертой Гражданского кодекса Российской Федерации».

В п. 55 указанного Постановления прописаны требования, которые предъявляются для того, чтобы скриншот (снимок экрана) был признан в качестве доказательства по делу: «…при разрешении вопроса о том, имел ли место такой факт, суд в силу статей 55 и 60 ГПК РФ, статей 64 и 68 АПК РФ вправе принять любые средства доказывания, предусмотренные процессуальным законодательством, в том числе полученные с использованием информационно-телекоммуникационных сетей, в частности сети Интернет»[61]. В том случае, если такие скриншоты предоставляются в виде распечаток (распечатанный скриншот уже будет не цифровым следом, а цифровым объектом на носителе) может потребоваться их заверение.

На практике же вопрос о заверении скриншотов интерпретируется судами по-своему. Так, при рассмотрении дела о нарушении исключительного права, где в качестве одного из доказательств истцом был представлен скриншот, Коптевский районный суд г. Москвы, а затем и Московский городской суд отказали в приобщении скриншота к делу, сославшись на отсутствие заверения. После обращении истицы в Верховный Суд РФ с кассационной жалобой и дальнейшим рассмотрением судом дела Верховным Судом РФ было разъяснено, что нижестоящие инстанции необоснованно отказали в приобщении скриншота к делу,

[61] О применении части четвертой Гражданского кодекса Российской Федерации : Постановление Пленума ВС РФ № 10 : принято Пленумом ВС РФ 23 апреля 2019 г. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_323470/ (дата обращения: 13.02.2025).

поскольку такой документ может быть не заверен. В данном случае прослеживается расхождение в требованиях к электронным документам.

По нашему мнению, скриншот является именно цифровым документом. Что же касается тех случаев, когда снимки экрана распечатываются на бумажном носителе, то это делается исключительно для удобства зрительного восприятия данного объекта судом, следователем, сторонами и т.д. Предоставлять суду или следователю скриншот, демонстрируя экран мобильного устройства или ПК было бы затруднительно. В свою очередь, к цифровым документам относятся и текстовые документы, существующие в цифровой форме. Однако, если скриншоты могут быть приобщены к делу без заверения, то цифровые документы, по мнению Верховного Суда РФ, в обязательном порядке должны подписываться электронной подписью. Таким образом, Верховный Суд РФ, во-первых, не совсем верно интерпретирует природу цифрового документа, а во-вторых, прописывает разные, противоречащие друг другу требования для их приобщения к делу в качестве доказательства. В силу изложенного в судебной практике отсутствует единообразие практики при работе с цифровыми документами.

Поскольку процессуальное законодательство никак не обозначает особые правила оценки цифровых доказательств, суды на практике оценивают такие доказательства на свое усмотрение. Например, согласно АПК РФ[62], документы, полученные посредством электронной или иной связи, могут заверяться электронной подписью, а могут и не быть заверены. В любом случае указанные документы будут признаны письменными доказательствами при отсутствии сомнений в их достоверности, а также при приобщении к делу будут представлены в печатной форме.

Немного иначе обстоят дела с УПК РФ, где электронным (и здесь прослеживается тенденция употребления устаревшего наименования

---

[62] Арбитражный процессуальный кодекс Российской Федерации : Федер. Закон № 95-ФЗ : принят Государственной Думой 14 июня 2002 г.: одобрен Советом Федерации 10 июля 2002 г.: послед. ред. 01.04.2025 г. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_37800/ (дата обращения: 13.02.2025).

«электронные документы») документам посвящен раздел XIX УПК РФ. Использование в уголовном судопроизводстве электронных документов и бланков процессуальных документов. Так, глава 56 содержит в себе 2 статьи – 474 и 474.1[63], где прописаны требования к наличию электронной подписи таких документов, а также некоторые другие моменты, однако определения электронного документа в УПК РФ нет.

Таким образом, неопределенность позиции судов по отношению к факту обязательной заверки цифровых документов как доказательств является одной из основных проблем, существующих на сегодняшний день в области цифровизации. На наш взгляд, представляется необходимым ввести единые и четко прописанные условия признания цифрового доказательства допустимым, а именно – сделать наличие электронной подписи или нотариальное заверение обязательным пунктом. Так, согласно ФЗ от 06.04.2011 № 63-ФЗ «Об электронной подписи»[64], который регулирует отношения в области использования электронных подписей, электронная подпись формируется при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций. Например, электронная или квалифицированная электронная подпись может использоваться при регулировании правоотношений между юридическими лицами, индивидуальными предпринимателями, оформлении доверенностей и т.д. Менее официальные документы, например, скриншоты, могут заверяться нотариально.

Во-первых, процедура создания электронной подписи, как и получения нотариального подтверждения (заверения), достаточна простая и доступная. Во-вторых, наличие электронной подписи как обязательного реквизита обеспечит

---

[63] Уголовно-процессуальный кодекс Российской Федерации : Федер. закон № 174-ФЗ : принят Государственной Думой 22 ноября 2001 г.: одобрен Советом Федерации 05 декабря 2001 г.: послед. ред. 21.04.2025 г. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_34481/ (дата обращения: 13.02.2025).

[64] Об электронной подписи : Федер. закон № 63-ФЗ : принят Государственной Думой 25 марта 2011 г.: одобрен Советом Федерации 30 марта 2011 г.: послед. ред. 06.04.2011 г. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_112701/ (дата обращения: 13.02.2025).

уверенность суда и сторон в истинности и достоверности документа, устранит сомнения в факте подлога и увеличит шансы на приобщение такого доказательства к делу.

В процессе анализа практики удается выделить разный подход судов к различным видам цифровых доказательств. Если цифровые документы с текстовым содержимым в большинстве случаев принимаются, то, например, SMS-сообщения, которые также создаются в цифровой среде и могут нести в себе информацию о фактах или событиях, на практике могут быть отклонены судами. Так, постановлением Десятого арбитражного апелляционного суда от 25.04.2016 № 10АП-17900/2014 по делу № А41-50304/14 в удовлетворении исковых требований о взыскании задолженности, процентов по дистрибьюторскому договору отказано, поскольку истец не представил доказательств наличия у сотрудников ответчика полномочий на направление оферт-заказов и акцептов на поставку товаров по спорному договору, а также не предоставил доказательств того, что указание в электронной переписке фамилии отправителя электронного сообщения является предусмотренным законом аналогом собственноручной подписи[65]. В качестве доказательств истцом была предоставлена электронная переписка с сотрудниками ответчика, которая не содержала электронной подписи либо иных аналогов собственноручной подписи. Если в случае со скриншотом, такое доказательство, не имея заверения, было в итоге признано доказательством, SMS-сообщения, также не обладая ни электронной подписью, ни нотариальным подтверждением, в качестве доказательства приняты не были, в результате чего в иске было отказано.

В качестве вывода можно выделить недостаток в практике работы с цифровыми документами, заключающийся в отсутствии единообразия судебной практики при решении вопроса о приобщении цифрового документа к делу в силу наличия или отсутствия электронной подписи либо нотариального заверения.

---

[65] Постановление Десятого Арбитражного апелляционного суда от 25.04.2016 № 10АП-17900/2014. [Электронный ресурс]. — Доступ из справ.-правовой системы «КонсультантПлюс».

Суммируя все вышесказанное, необходимо сформулировать понятие цифрового документа. Под цифровыми документами предлагается понимать *самостоятельный вид цифровых объектов, созданных с помощью компьютера (иного устройства) и подтвержденных электронной цифровой подписью (ЭЦП), либо переведенных из цифрового формата в бумажный и нотариально заверенных, содержащих в себе информацию о фактах или событиях, имеющих доказательственное значение по делу. Требование о нотариальном заверении или подтверждении электронной цифровой подписи (ЭЦП) необходимо для придания представленному цифровому документу как объекту экспертного исследования легитимности.*

Таким образом, в результате теоретических изысканий о природе, свойствах и разновидностях объектов в цифровой форме можно сделать следующие выводы.

Прежде всего, цифровой след – это криминалистически значимая компьютерная информация о событиях / действиях в процессе ее возникновения, обработки, хранения, передачи, отраженная в материальной среде. Появление таких следов обусловило формирование новых частных криминалистических и экспертных теорий о цифровизации, в рамках которых изучаются принципы выявления, изъятия и исследования подобных объектов.

Цифровой след, как и любой след, является одним из элементов «креста следов». Однако, в силу того, что для восприятия и работы с цифровыми следами необходимо применение специальных технических и информационных средств, появляется новый механизм следообразования, что в конечном итоге приводит к формированию нового «креста следов».

Следует также учитывать природу цифрового следа: цифровые следы являются следами материальными. Механизм следообразования цифровых следов может быть электронным, электромагнитным или механическим. Поэтому называть цифровые следы электронными нецелесообразно.

Цифровые следы подразделяются на различные виды. Например, они могут разделяться в зависимости от вида экспертизы: в почерковедении – это

клавиатурный почерк, подписи и записи, выполненные на экранах устройств и т.д.; в судебной экономической экспертизе – это данные бухгалтерских учетов, цифровые рубли и т.д. В зависимости от структуры цифровые следы подразделяются на простые и сложные. По способу появления выделяют активные и пассивные цифровые следы.

Также среди цифровых объектов есть самостоятельные виды, такие, как цифровые документы.

В результате изучения цифровых следов и их видов мы пришли к выводу о том, что они не существуют сами по себе, а всегда содержатся на чем-либо, соответственно, все цифровые следы располагаются на каких-либо носителях. И поскольку изучение только цифровых следов или только носителей представляется слишком узким, мы пришли к выводу о том, что вместе эти два компонента образуют единый цифровой объект, который и выступает в качестве объекта экспертного исследования, что позволило сформулировать дефиницию «цифровой объект». *Под цифровым объектом предлагается понимать объект судебно-экспертного исследования, состоящий из цифровых следов разных видов, находящихся на объекте-носителе.*

Всесторонний анализ понятия и разновидности цифровых следов и цифровых объектов позволил выявить ряд сложностей, возникающих при их выявлении, фиксации, исследовании, что в свою очередь неизбежно приводит к новым экспертным ошибкам.

1.2. Экспертные ошибки: генезис и современное состояние

На протяжении нескольких тысячелетий преступность неизменно являлась неотъемлемой частью любого общества. С течением времени изменился только уровень сложности совершаемых преступлений: появились новые изощренные способы совершения и сокрытия преступного деяния, увеличился процент

преступлений, практически не оставляющих за собой никаких следов. Как отмечает О.Б. Дронова, реалиями настоящего времени являются применяемые преступным сообществом технологии искусственного интеллекта в процессе совершения преступлений с использованием цифрового пространства[66].

Преступники научились искусно маскировать свою криминальную деятельность, выдавая ее за другое, менее тяжкое преступление, а в некоторых случаях и вовсе создавая иллюзию правомерного поведения. Все эти факторы привели к очевидному усложнению для правоохранительных органов возможности раскрытия и расследования преступлений в силу нехватки источников информации о совершенном деянии и, как следствие, ущербности доказательственной базы, способной свести к минимуму шанс изобличения преступника в принципе. Особенно сейчас, в век информационных технологий, совершить, предположим, преступление коррупционной направленности, становится все проще в связи с возможностью использования в качестве средства или метода преступления современные достижения науки и техники.

Учитывая такое положение дел, суд и органы расследования должны обращать особое внимание на ту доказательственную базу, которая у них имеется – природа каждого доказательства должна быть проверена на «прочность» и соответствовать критериям достоверности и объективности.

Одним из видов доказательств, получивших в свете изменения характера преступности особое распространение, является заключение судебного эксперта. Однако широкое использование данного вида доказательств не следует путать с его возможным привилегированным значением по сравнению со всеми другими доказательствами, которое ему присуще на практике, из чего вытекает необходимость тщательной проверки экспертного заключения и его правильной оценки.

---

[66] Дронова, О. Б. Криминалистические аспекты противодействия преступности в цифровом обществе: современные проблемы и перспективы развития / О. Б. Дронова // На страже закона. — 2024. — № 4. С. 12.

Эксперт, хотя и лицо высококвалифицированное, обладающее набором специальных знаний, а иногда и из разных областей, все же не застрахован от совершения ошибок. Речь идет о совершении экспертной ошибки на любой стадии экспертного исследования, что безоговорочно приведет к порождению ошибки в дальнейшем ходе расследования преступления, которая будет иметь как следственный, так и судебный характер. Опасность такой ошибки также обусловлена определенным кругом негативных последствий, начиная от затягивания сроков расследования и заканчивая нанесением урона правосудию и причинением вреда законным правам и свободам лиц, пострадавших от преступления. Именно это и является причиной необходимости своевременного и всестороннего выявления, исследования и предотвращения экспертных ошибок, что и будет рассмотрено в рамках данного исследования.

Стоит учитывать, что судебно-экспертная деятельность по сей день не лишена недостатков: отсутствие разработанной методики у отдельных видов экспертиз, устаревшая техника, игнорирование или непринятие разработок судебной экспертологии практиками, некомпетентность эксперта – как раз все те факторы, которые способны привести к экспертной ошибке. Анализ природы экспертных ошибок позволяет если не исключить, то хотя бы свести к минимуму возможность их совершения экспертами в дальнейшем, что, несомненно, сыграет роль в улучшении свершения правосудия.

Рассмотрение понятия «экспертная ошибка» невозможно без понимания сущности термина «ошибка» в принципе. И.П. Петрухин дает следующее толкование понятия ошибки, согласно которому в самом общем виде ошибка – это утверждение, не соответствующее действительности, или мера, действие, не приводящее к достижению поставленной цели, если искажение в познании или отклонение от цели допущены непреднамеренно, т.е. являются результатом добросовестного заблуждения[67]. На наш взгляд, такое определение является не

[67] Кудрявцев, В. Н. Эффективность правосудия и проблема устранения судебных ошибок / под ред. В.Н. Кудрявцева. — М., 1975. С. 94.

совсем правильным, представляется уместным внести в данное определение небольшую корректировку – не утверждение и умозаключение, так как эти процессы первичны и предшествуют процессу формирования экспертом заключения, а утверждение – его результат. В русском языке ошибку трактуют как неправильность мыслей, действий. Ошибиться – это значить сделать (допустить) ошибку, т.е. неправильно оценить что-нибудь, поступить неправильно[68].

Определение термина «ошибка» на сегодняшний момент разрабатывается многими науками и отраслями, например, юридическими науками, медициной, математикой. Однако не стоит забывать, что и до этого данному понятию уделялось большое внимание на всех этапах развития науки философии. К примеру, Аристотель понятие ошибки связывал с проблемой взаимосвязи таких трех положений, как познание, самопознание и самосознание. Говоря «воспринимать же друга означает некоторым образом воспринимать самого себя, а познавать друга – некоторым образом познавать самого себя»[69], Аристотель дает нам наглядное представление о разграничении самопознания и самосознания и обращает наше внимание на важность данных положений для гносеологического понимания ошибок познания.

Другим значимым высказыванием является тезис древнего философа Августина. Своей фразой «если я обманываюсь, значит, я существую» Августин к предыдущему положению Аристотеля добавляет проблемы сомнения в познании и возможности ошибочного познания[70]. Такая точка зрения, по нашему мнению, вполне оправдана, поскольку сводит совершение ошибок к одной из обязательной составляющей существования человека и процесса познания им действительности, и, что немаловажно, познания самого себя, факторов, ставших причиной

---

[68] Толковый словарь русского языка [Текст] : 72500 слов и 7500 фразеологических выражений / С. И. Ожегов, Н. Ю. Шведова ; Российская АН, Ин-т рус. яз., Российский фонд культуры. - 2-е изд., испр. и доп. - Москва : Азъ, 1994. С. 487.

[69] Гарнцев, М.А. Проблема самосознания в западноевропейской философии (от Аристотеля до Декарта) : монография / М.А. Гарнцев. — М. : Изд-во МГУ, 1987. С. 33.

[70] Гарнцев, М.А. Проблема самосознания в западноевропейской философии (от Аристотеля до Декарта) : монография / М.А. Гарнцев. — М. : Изд-во МГУ, 1987. С. 81.

ошибочного суждения. Стоит сказать, что познавательная деятельность, не имеющая ошибок и проблемных областей, в конечном итоге не принесет никаких плодов, поскольку не сможет стать двигателем прогресса в исследовании чего-либо, ведь в таком случае будет иметь место изучение уже устоявшихся и проверенных положений, а когда их рассмотрение закончится, настанет тупик.

Подходя ближе к современному периоду, следует начать с рассмотрения понятия «экспертная ошибка» с точки зрения наиболее значимой для нас в рамках данного исследования науки – юридической. Ошибки в судопроизводстве в целом – это ошибки, совершаемые в социальной среде при решении социальных (по своей природе) вопросов. Относительно экспертных ошибок следует отметить, что ранее в специальной литературе на разных этапах развития судебной экспертизы они рассматривались только при производстве отдельных видов криминалистических экспертиз, т.е. трактовка экспертной ошибки была достаточно узкой, что не позволяло понять сущность данной проблемы в полной мере. На наш взгляд, ее стоит рассматривать шире хотя бы потому, что классификация судебных экспертиз на сегодняшний день значительно пополнилась новыми видами, классами, помимо этого формируются новые методы и технические средства, которые используются в настоящее время в экспертной практике.

Р.С. Белкин экспертную ошибку определил следующим образом: «не соответствующее объективной действительности суждение эксперта или его действия, не приводящие к цели экспертного исследования, если и искаженное суждение, и неверные действия представляют собой результат добросовестного заблуждения»[71]. Данное утверждение в юридической науке признается одним из наиболее точных и полных, и находит отклик в работах многих деятелей судебной экспертизы, в их числе – Е.Р. Россинская, которая использовала определение Р.С. Белкина при составлении комментария к ФЗ о ГСЭД, что вызывает доверие к этому высказыванию.

---

[71] Белкин, Р. С. Курс криминалистики: Криминалистические средства, приемы и рекомендации : в 3 т / Р. С. Белкин. — Т. 3. — М. : Юристъ, 1997. С. 335-336.

Понятие экспертной ошибки также приводится Н.И. Клименко, предположительно отграничивающей экспертные ошибки от возможных терминов – синонимов с помощью признаков типичности и существенности. В соответствии с этим, Н.И. Клименко определила экспертную ошибку как «недостатки экспертного исследования непреднамеренного характера, которые повлекли дачу неправильного решения»[72]. На наш взгляд, такая трактовка экспертной ошибки как «недостатка» не может являться правильной и в полной мере исчерпывающей, способной дать грамотное истолкование данной дефиниции в соответствии с присущей ей спецификой, ведь недостаток в известной степени означает «погрешность, ошибку», что и является синонимичным термином, а значит, высказывание автора в некоторой мере противоречит самому себе. Также автор приводит другое определение, согласное которому ошибка – это результат добросовестного заблуждения эксперта[73]. При этом автор допускает, что ошибка может быть и следствием сознательного нарушения экспертом требований методики исследования. Такая точка зрения кажется не совсем обоснованной, поскольку в случае сознательного нарушения речь идет уже не об ошибке, а о заведомой ложности.

Исследуя проблему предотвращения экспертных ошибок в аспекте обеспечения истинности экспертного заключения, А.К. Педенчук определяет экспертную ошибку как «неумышленное, неправильное или неистинное суждение либо действие эксперта в процессе исследования и формулирования выводов, вследствие чего дано ошибочное заключение»[74]. В целом поддерживая признаки, выделенные указанным автором, полагаем, что ошибочные суждения или действия эксперта возможны не только на этапе непосредственного экспертного исследования, но и при нарушении процессуального закона.

---

[72] Клименко, Н. И. Экспертные ошибки и их причины / Н. И. Клименко /Криминалистика и судебная экспертиза. — 1988. — Вып. 37. С. 36.
[73] Там же, С. 38.
[74] Педенчук, А. К. Заключение судебного эксперта: логика, истинность, достоверность: автореферат дис. ... д-ра юрид.наук. Москва, 1995. С.36.

По мнению А.Ю. Краснобаевой под экспертной ошибкой подразумевается следующее: «неправильное суждение или действие эксперта, объективно выразившиеся в нарушении законов логики, уголовно-процессуального закона, последовательности рекомендованных процедур при исследовании объектов, их неправильном применении, не приводящее к достижению поставленной цели (истинного вывода), или бездействие, если они допущены непреднамеренно»[75]. В данной дефиниции автор отразил не только само понятие, но и перечень предшествующих ошибке причин, определяющих, в чем выражается неправильное суждение или действие эксперта, т.е. помимо уже известного добросовестного заблуждения говорится о нарушениях законов логики, норм УПК РФ, что, безусловно, делает это определение наиболее развернутым и удобным для понимания. Таким образом, и в определениях Р.С. Белкина, и в определении А.Ю. Краснобаевой есть отсылка к трактовке понятия «ошибка», изложенном в русском толковом словаре, в части действий, не приводящих к достижению поставленной цели. Во-вторых, оба ученых в своих высказываниях затронули такое важное положение, как добросовестность заблуждения эксперта. Поэтому, мы считаем необходимым остановиться на этом моменте подробней.

Действительно, в рассуждении об экспертной ошибке, подразумевается только добросовестное заблуждение, так как это является именно тем обстоятельством, которое отличает экспертную ошибку от заведомо ложного заключения, что уже является преступлением, караемым законом. Данный аспект является важным потому, что в судебной практике до сих пор эти два понятия – экспертная ошибка и заведомо ложное заключение путают, поэтому требуется обязательный учет тех положений, при помощи которых они разграничиваются.

Заведомо ложное заключение эксперта является умышленным действием, выражающимся в сознательном игнорировании или умалчивании в процессе исследования существенных фактов и признаков объектов экспертизы, их заведомо

---

[75] Краснобаева, А. Ю. Экспертные ошибки: причины, последствия, профилактика : дис. … канд. юрид. наук : 12.00.09 / Анна Юрьевна Краснобаева. — Волгоград, 1997. С. 21.

неправильной оценке или заведомо неверных действиях по их исследованию, а также умышленно неверном выборе методики исследования объектов. Исходя из данного определения можно увидеть слова-сигналы для отграничения от экспертной ошибки – «заведомо», «умышленно». В некоторых случаях действия эксперта могут быть замаскированы под непредумышленную ошибку, однако на самом деле они являются способом совершения преступления против правосудия: «Одной из разновидностей причин, приводящих к получению недостоверных результатов судебно-экспертной деятельности, являются умышленные «ошибки», которые в зависимости от дальнейшего развития криминальной ситуации могут быть рассмотрены в качестве способа совершения преступлений»[76]. В таком случае эксперт намеренно в преступных целях совершает действия, лишь внешне схожие с ошибкой.

Другой вопрос, как правильно опознать эту добросовестность, если, как бы это странно ни звучало, она происходит в голове эксперта. Мы не можем наверняка знать, что ошибочные действия человека были совершены неумышленно, что лицом были предприняты все попытки для того, чтобы освоить и применить, например, необходимую методику правильно, ведь иногда экспертом некоторые важные положения могут быть и вовсе проигнорированы. Поэтому представляется очень важным обращать особое внимание на фактор добросовестности. Возможно, экспертом здесь могут быть приведены даже какие-то доказательства, например, наличие установленного факта неоднократных попыток разобраться в моментах, вызывающих затруднение, или наличие противоречий в методике, не получившей еще такого широкого и повсеместного применения, однако, как это все будет осуществляться на практике – непонятно. В связи с этим Г.Л. Грановский, учитывая важность такого признака, как добросовестное заблуждение, предлагает понимать под экспертной ошибкой выводы, не соответствующие действительности, а также

[76] Дронова, О. Б. Экспертные «ошибки» как способ совершения преступлений / О. Б. Дронова // Экспертные ошибки: современные проблемы возникновения, выявления и профилактики : материалы Международной научно-практической конференции. — Москва : РГ-Пресс, 2024. С. 52.

неправильность в действиях или рассуждениях, отражающих процесс экспертного исследования – в представлениях, суждениях, понятиях[77].

Представляется интересной также точка зрения, согласно которой понятие экспертной ошибки рассматривается в соотношении с врачебной ошибкой в рамках судебно-медицинской экспертизы. В.А. Клевно, А.В. Максимов рассмотрели научную литературу в области как судебной экспертизы, так и судебной медицины (в частности акты судебно-медицинского исследования трупа) и пришли к выводу, что понятие «экспертная ошибка» близко к определению «врачебная ошибка». Главным отличительным признаком врачебной/экспертной ошибки, по их мнению, является добросовестное заблуждение в правильности своих действий и суждений. То есть экспертную ошибку можно трактовать как непреднамеренное ошибочное суждение (мнение) врача – судебно-медицинского эксперта при установлении фактических данных в процессе экспертного исследования и дачи заключения[78]. Здесь мы также можем видеть некую схожесть с предыдущими определениями.

На наш взгляд, наиболее исчерпывающим представляется определение экспертной ошибки, сформулированной А.А. Аубакировой. Согласно позиции автора, «под экспертной ошибкой следует понимать непреднамеренное неверное суждение (умозаключение) или действие эксперта при установлении фактических данных в процессе исследования объектов и оценки результатов, а также нарушение уголовно-процессуального закона, способные привести к неверному решению, не обеспечивающему полноту, объективность и всесторонность проведенного исследования»[79]. Автор не только отделяет понятие ошибки от заведомо ложного суждения или действия, но и закладывает основу для дальнейшей классификации экспертных ошибок. Говоря о нарушениях уголовно-

---

[77] Грановский, Г. Л. Природа, причины экспертных ошибок и пути их устранения / Г. Л. Грановский // Новые разработки и дискуссионные проблемы теории и практики судебной экспертизы. Экспресс-информация. —1983. — Вып. №2. С. 7.

[78] Клевно, В. А., Максимов, А. В. К вопросу о классификации и терминологии экспертных ошибок / А. В. Клевно, А. В, Максимов // Судебная медицина. — 2017. — №2. С.11.

[79] Аубакирова, А. А. Следственные и экспертные ошибки при формировании внутреннего убеждения : дис.... д-ра юрид. наук : 12.00.12 / Аубакирова Анна Александровна. — Челябинск, 2010. С. 358.

процессуального закона, очевидно, А.А. Аубакирова имеет в виду процессуальные ошибки, которые составляют значимую долю ошибок на практике, однако при определении экспертных ошибок о них часто напрямую не говорят.

Рассматривая понятие ошибок, нельзя не сказать, что их природа неоднородна, в связи с чем ошибки могут быть условно подразделены на классы. Согласно классификации ошибок, допускаемых в судопроизводстве, предложенной Р.С. Белкиным (исходя из сущности ошибки), а затем преобразованной Е.Р. Россинской применительно к экспертным ошибкам, они подразделяются на три класса:

- ошибки процессуального характера;

- гносеологические ошибки;

- деятельностные (операционные) ошибки[80].

А.К. Педенчук полагает, что «эксперт не может совершить процессуальную ошибку, т.к. не является субъектом доказывания <…> нарушение им процессуального режима и процедуры экспертного исследования можно назвать ошибкой процессуального характера»[81]. Соглашаясь с тем, что эксперт не выступает субъектом доказывания, полагаем, что сущность процессуальной ошибки заключается не в совершении ее определенным субъектом. Экспертные ошибки процессуального характера заключаются в нарушении экспертом процессуального режима и процедуры производства экспертизы. К этому классу ошибок относится: выход эксперта за пределы своей компетенции; выражение экспертной инициативы в не предусмотренных законом формах; обоснование выводов материалами дела, а не результатами исследования; самостоятельное собирание материалов и объектов экспертизы; несоблюдение по незнанию

---

[80] См.: Белкин, Р. С. Курс криминалистики: Криминалистические средства, приемы и рекомендации : в 3 т / Р. С. Белкин. — Т. 3. — М. : Юристъ, 1997. С. 337; Белкин, Р. С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики / Р. С. Белкин. — М. : Норма : Инфра-М, 2001. С.172; Галяшина, Е. И., Голикова, В. В., Дмитриев, Е. Н. и др. Судебная экспертиза: типичные ошибки / Е.И. Галяшина, В.В. Голикова, Е.Н. Дмитриев и др.; под ред. Е.Р. Россинской. — М.: Проспект, 2012. — 301 с.

[81] Педенчук А.К. Указ.соч. С.36.

процессуальных требований к заключению эксперта (в том числе отсутствие в заключении необходимых по закону реквизитов) и др.

На наш взгляд, процессуальные ошибки можно подразделить на процессуальные ошибки, ведущие к недействительности содержания экспертного заключения, и процессуальные ошибки, ставящие под угрозу недействительность формы экспертного заключения. Следует согласиться со следующей позицией С.Л. Мельник: «К процессуальным ошибкам относится уничтожение либо существенное изменение свойство объектов без разрешения органа или лица, назначивших судебную экспертизу, ссылки в заключении эксперта на различного рода «акты», составленные по инициативе эксперта специалистами, проводившими лабораторные исследования, а также случаи, когда производство повторной экспертизы проводились тем же экспертом или той же комиссией экспертов, которыми была проведена и первичная экспертиза»[82].

Следует подчеркнуть, что процессуальные экспертные ошибки часто становятся следствием следственных и судебных ошибок, связанных с назначением судебной экспертизы и оценкой ее результатов, а значит, их целесообразно рассматривать во взаимосвязи.

Р.С. Белкин определил природу гносеологических и логических ошибок следующим образом: «Гносеологические ошибки коренятся в сложностях самого процесса экспертного познания. Они могут быть допущены при познании сущности, свойств, признаков объектов экспертизы, отношений между ними, а также при оценке результатов познания, итогов экспертного исследования, их интерпретации. Ошибки гносеологического характера связаны с процессом экспертного исследования, который строится с учетом законов логики и определенных правил. Они делятся на логические и фактические (предметные). Логические ошибки связаны с нарушением в акте мышления законов и правил логики, некорректным применением логических приемов и операций. Такие

[82] Мельник, С. Л. Актуальные вопросы экспертной инициативы : дис. … канд. юрид. наук : 12.00.09 / Светлана Львовна Мельник. — Челябинск, 2005. С. 172.

ошибки обычно связаны с различными логическими операциями и видами умозаключений»[83].

Е.Р. Россинская и Е.И. Галяшина среди логических ошибок также выделяют следующие: «к иным логическим ошибкам, встречающимся в экспертных заключениях, относятся несоответствие вывода осуществленному экспертом исследованию; отсутствие логической обусловленности последовательности стадий экспертного исследования; наличие по одному и тому же предмету двух противоречивых выводов эксперта; наличие внутренних противоречий в заключении эксперта»[84].

Т.В. Аверьянова Р.С. Белкин среди определяют деятельностные (операционные) ошибки так: «деятельностные ошибки связаны с осуществляемыми экспертом операциями (процедурами) и могут заключаться в:

а) нарушении предписанной последовательности этих процедур;

б) неправильном использовании средств исследования или использовании непригодных средств, например, использование аппаратуры, давно не проходившей поверку;

в) получении некачественного сравнительного материала и т.п.»[85].

Анализ значения и содержания термина «ошибка» позволил сформулировать общий тезис, выделив ключевые положения: *экспертная ошибка представляет собой неправильное/не соответствующее действительности суждение/действие эксперта, которое в итоге не приводит к поставленной в рамках экспертного исследования цели, при условии, что такое суждение/действие явилось следствием добросовестного заблуждения эксперта в силу различных обстоятельств, связанных с его познавательной деятельностью*.

---

[83] Белкин Р.С. Криминалистика: проблемы сегодняшнего дня. М., 2001. С. 188.
[84] Россинская Е.Р., Галяшина Е.И. Настольная книга судьи. Судебная экспертиза. М., 2010.
[85] Аверьянова Т. В., Белкин Р. С., Корухов Ю. Г., Россинская Е. Р. Криминалистика. Учебник для вузов. Изд. 4, переработанное и доп. / Т.В. Аверьянова, Р.С. Белкин, Ю.Г. Корухов, Е.Р. Россинская — М.: Норма; ИНФРА-М, 2013. С. 397.

Заблуждение и ошибка обычны и повсеместны, безошибочная деятельность – удел опытных и немногих, которые в свою очередь пришли к этому состоянию также через ошибки и их преодоление[86]. Любая ситуация и содержащаяся в ней ошибка является следствием некоторой причины. То же самое касается и экспертного исследования с экспертной ошибкой. Для того, чтобы понять первоначальную причину экспертной ошибки, представляется обоснованным рассматривать экспертную ошибку с позиции детерминизма, согласно которой ошибка – это развивающаяся система, которой свойственны внутренние противоречия: между стабильностью и изменчивостью, между свойствами целого и отдельных элементов, между стремлением системы к равновесию и так называемыми «возмущающими» воздействиями. Причинные отношения в такой системе отличаются особой сложностью, неустойчивостью, обилием обратных связей[87]. Иными словами, в процессе экспертного исследования все ситуативно связано – все исследуемые объекты, применяемые методики, а это значит, что возникшая в ходе исследования ошибка сама является следствием предшествующей до этого ошибки, т.е. здесь имеет место схема «ошибка от ошибки». Такое прослеживание всей цепочки причин, породивших экспертную ошибку, может привести к многовариантному возможному развитию ситуации и ее разрешению в плане предотвращения всех или хотя бы большинства допущенных ошибок.

Причины экспертных ошибок по своей природе различны и связаны с особенностями познавательной деятельности эксперта, его внутренним (душевным) состоянием, уровнем развития науки и техники, условиями труда, техническим оснащением и многими другими факторами, воздействующими на эксперта как в повседневной жизни, так и в процессе самого экспертного исследования. Исходя из данного положения, мы можем видеть основания для

---

[86] Белкин, Р. С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики / Р. С. Белкин. — М. : Норма : Инфра-М, 2001. С. 83.

[87] Кудрявцев, В. Н. Генезис преступления. Опыт криминологического моделирования : Учеб. Пособие / В. А. Кудрявцев. — М.: Издательская группа «ФОРУМ–ИНФРА–М», 1998. С. 112.

разделения причин экспертных ошибок на две большие группы, хоть и разные, но взаимосвязанные между собой. Экспертная ошибка, с одной стороны детерминируется и объективируется в экспертной ситуации как явлении экспертной практики. С другой стороны, ошибка детерминирована субъективными качествами личности эксперта.

Таким образом, факторы или причины, препятствующие полному и всестороннему исследованию объектов исследования и даче правильных ответов на поставленные вопросы, носят как субъективный, так и объективный характер.

К экспертным ошибкам объективной природы Е.Р. Россинская относит: «отсутствие разработанной и апробированной методики; несовершенство используемой экспертной методики; применение ошибочно рекомендованных либо находящихся в стадии разработки методов; применение неисправного оборудования; применение нелицензионных программ для ЭВМ и др.»[88].

Характеризуя данную группу причин возникновения экспертных ошибок, на наш взгляд, очень важно разъяснить вопрос, касающийся использования в экспертном исследовании различных методов и соответствующего оборудования. По общему правилу судебный эксперт независим в выборе методов и средств экспертного исследования, которые, по его мнению, необходимы для изучения объектов, представленных на экспертизу, при условии отсутствия паспортизированной экспертной методики.

Паспортизация экспертных методик представляет собой деятельность, направляемую межведомственным координационным советом в области судебной экспертизы, по организации единства в систематизации и стандартизации экспертных методик. Целью паспортизации является изложение экспертных методик каждого рода экспертизы по определенной схеме, апробирование методик и их последующее оформление по стандартам паспортов (технологических, технических). Паспортизированные и системно изложенные в справочных

---

[88] Россинская Е.Р., Галяшина Е.И. Настольная книга судьи / Е.Р. Россинская, Е.И. Галяшина. — М. : Судебная экспертиза, 2010. С. 387.

пособиях методики служат методическим пособием для экспертов, пособием по проверке и оценке заключений эксперта лицами, осуществляющими производство по делу[89]. Паспортизированных экспертных методик пока немного, поэтому в большинстве случаев спектр средств и методов эксперт определяет сам.

Судебной экспертологией выработаны основные принципы допустимости использования методов и средств в судебно-экспертных исследованиях, среди которых одним из наиболее важных является научная обоснованность методов и достоверность получаемых с их помощью результатов. Дело в том, что научная природа метода не всегда гарантирует обеспеченную достоверность результатов при условии применения определенной экспертной технологии. В подтверждение данному положению Е.Р. Россинская писала следующее: «в 80-е гг. во ВНИИ МВД СССР был разработан комплекс экспертных методик по исследованию медных проводников в зонах короткого замыкания и термического воздействия. В основе методик лежали методы рентгенофазового структурного анализа (РФСА) и металлографии. Для разработки этих методик проводился широкий спектр модельных экспериментов, они были защищены авторскими свидетельствами, прошли широкую апробацию и начали активно использоваться в экспертных учреждениях разных ведомств. Однако в 90-е г. вместо рентгеновского дифрактометра, который был рекомендован в методиках и позволял снимать весь рентгеновский спектр (хотя использовались для анализа только две линии спектра), для удешевления исследований стали использовать упрощенное оборудование, позволяющее регистрировать только две основные рентгеновские линии, что совершенно недопустимо с точки зрения интерпретации рентгеновского спектра»[90]. Подобная рационализация привела к многочисленным экспертным ошибкам, выявить которые правоприменителю явно не под силу, поскольку он не может разобраться в особенностях оборудования, которое к тому же постоянно

---

[89] Словарь эксперта // НОЧУ ДПО «Институт СЭиК» [Электронный ресурс]. — URL: https://ceur.ru/library/words/page-132/ (дата обращения: 22.12.2023).

[90] Россинская, Е. Р. Судебная экспертиза: типичные ошибки: 2-е издание, монография / под. ред. Россинской Е.Р. — М.: Проспект, 2024. С. 537.

совершенствуется. Таким образом, научность и надежность метода не обязательно означает его пригодность для всех подлежащих исследованию объектов.

При анализе объективных причин экспертных ошибок важно уточнить два ключевых аспекта. Во-первых, объективные причины не обязательно ведут к ошибкам; они только создают условия для их возникновения. Во-вторых, даже при наличии объективных факторов, причина ошибочного вывода эксперта может не заключаться в его собственных ошибках. Экспертное исследование может быть проведено верно, но если исходные данные для экспертизы были неверными, исследуемые объекты не имели отношения к делу или были сфальсифицированы, то заключение эксперта может оказаться ошибочным. В таких ситуациях нельзя говорить об ошибке эксперта: виновными могут быть либо орган, назначивший экспертизу, либо его преднамеренные неверные действия. Такие ошибки чаще всего становятся проблемой при проведении автотехнических и почерковедческих экспертиз.

Второй группой причин экспертных ошибок являются субъективные причины, например, профессиональная некомпетентность эксперта, незнание современных экспертных методик, неумение применять современные экспертные технологии, неправильная оценка признаков и т.д. Субъективными ошибками также являются неполнота исследования, а именно неполное выявление существенных признаков объекта, игнорирование тех или иных свойств объектов, пренебрежение правилами и условиями применения методик экспертного исследования и технических средств и др. В качестве существенной причины дачи экспертом ошибочных заключений также стоит признать имеющее место в ряде случаев небрежно, поверхностно проведенное исследование. В этом, на наш взгляд, заключается некоторое противоречие относительно фактора добросовестности заблуждения эксперта.

Во избежание неправильного толкования вышеуказанных субъективных причин экспертной ошибки, полагаем, стоит добавить разъяснения, в соответствии с которыми небрежно или поверхностно проведенное исследование является

следствием незнания экспертом всех аспектов полного процесса исследования объекта, или, например, правил надлежащего использования технического оборудования, можно признать добросовестным заблуждением, но если в силу знания этих положений, но из-за желания сократить время экспертного исследования или нежелания приложить все возможные усилия, такое исследование было проведено неполно, то добросовестности, по нашему мнению, здесь явно не будет.

Природа субъективных причин, на наш взгляд, несколько сложнее объективных потому, что содержит в себе психофизиологическую составляющую. Одна из причин ошибок при проведении экспертизы – недостаточный учет психологических элементов, которые играют большую роль, особенно в процессах идентификации. Их влияние распространяется на весь процесс исследования: от стадии восприятия до формирования выводов.

Речь идет об определенных чертах личности эксперта, среди которых важными для проведения исследования могут выступать: наличие каких-либо дефектов органов чувств (в данном случае может иметь место генетическая обусловленность причины ошибки в самом субъекте), логические дефекты умозаключений, характерологические свойства личности эксперта (неуверенность в своих знаниях, мнительность, конформизм или пренебрежение мнением коллег в случае проведения комплексной экспертизы).

В.В. Бушуев говорит следующее: «Ошибка может быть заложена в комплексе факторов личностного отражения ситуации – привычках, социальной направленности. В процессе деятельности эксперта может возникнуть проблемная ситуация, когда в его сознании отсутствует способ поиска необходимой ему информации, четко сформулированной программы производства действий»[91]. Например, причиной ошибочного заключения может послужить неординарное психологическое состояние эксперта, усталость, переутомление и т.д.

---

[91] Бушуев, В. В. Экспертные ошибки: причины и профилактика / В. В. Бушуев //Вестник Московского университета МВД России. — 2015. — №3. С. 24.

Ранее нами уже были кратко рассмотрены виды судебных ошибок, однако, это далеко не единственная существующая классификация. Судебные ошибки можно также классифицировать в зависимости от вида производимой экспертизы. Так, ошибки могут быть при производстве судебно-медицинской экспертизы, судебно-баллистической экспертизы, судебно-технической экспертизы документов и т.д. В рамках каждой экспертизы есть как общие ошибки, связанные, например, с правилами действий эксперта на этапе ознакомления с объектами, поступившими на экспертизу, так и частные, отражающие особенности конкретного вида экспертизы. В рамках нашего исследования мы рассмотрим ошибки при производстве судебной фоноскопической экспертизы.

Согласно позиции Е.И. Галяшиной, судебная фоноскопическая экспертиза — род судебной экспертизы, которая проводится в целях установления личности говорящего по голосу и речи, аутентичности фонограмм, диагностики и идентификации записывающих устройств, а также иных фактов, имеющих значение доказательств в судопроизводстве[92].

Фоноскопическая экспертиза – это род судебных экспертиз, направленных на установление обстоятельств (фактов) путем исследования голоса и звучащей речи, звуковой среды, условий, средств, материалов и следов звукозаписей[93]. Звуковые следы человека на сегодняшний день активно используются в судопроизводстве при раскрытии и расследовании различных категорий преступлений, не говоря уже о преступлениях коррупционной направленности, где данное средство доказывания зачастую является практически единственным возможным для получения и исследования. Согласно анализу судебно-следственной практики

---

[92] Галяшина, Е. И. Об истории судебной фоноскопической экспертизы / Е. И. Галяшина // Вестник Университета имени О. Е. Кутафина. — 2014. — №3. С. 186.

[93] Подобное определение приводится на большинстве сайтов организацией, предлагающих проведение альтернативной (несудебной) фоноскопической экспертизы. Центр по проведению судебных экспертиз и исследований автономная некоммерческая организация «Судебный Эксперт» // Автономная некоммерческая организация «Судебный эксперт» [Электронный ресурс] URL: https://sudexpa.ru/. Дата обращения: 05.01.2024 г. АНО ЭКЦ «Судебная экспертиза» [Электронный ресурс]. — URL: https://ekc-se.ru/fobo_ekspertiza?ysclid=m6nmkxayv3104781557 (дата обращения: 05.01.2024).

практически каждое уголовное дело, возбужденное по факту совершения коррупционного преступления, сопровождается назначением фоноскопической экспертизы[94]. Это связано с тем, что подобные преступления нередко находят свое отражение в негласной аудиозаписи бесед между субъектами коррупционных отношений, которая может осуществляться как в ходе проведения оперативно-розыскных мероприятий, так и самостоятельно лицом, у которого вымогают незаконное денежное вознаграждение.

Фоноскопическую экспертизу в силу специфичности объекта исследования, как правило, должен проводить квалифицированный специалист, умеющий в целях исследования фонограммы и дачи ответов на поставленные перед ним вопросы правильно интегрировать знания сразу из нескольких областей науки (криминалистика, акустика и т.д.). Проведение фоноскопической экспертизы необходимо в случаях, когда требуется установление принадлежности записанного голоса и звучащей речи конкретному лицу (идентификация говорящего) или группе лиц, если речь идет о переговорах, имевших место при совершении взятки; выявление возможных признаков монтажа; установление речевого или акустического содержания записи, а также решение некоторых диагностических задач, например, установление состояния говорящего.

Переходя непосредственно к характеристике ошибок, совершаемых в рамках фоноскопической экспертизы, стоит сразу сказать, что все те классификации и причины, которые были рассмотрены нами ранее, а именно субъективные и объективные причины совершения экспертом ошибок и разделение ошибок на процессуальные, гносеологические и деятельностные, проецируются и на фоноскопическую экспертизу, однако с рядом уточнений.

Например, одной из важных предпосылок совершения экспертом ошибки при исследовании фонограммы может послужить субъективный фактор, а именно

---

[94] Ануфриева, Е.А. Особенности методики предварительного расследования и судебного разбирательства по делам о коррупционных преступлениях, совершаемых сотрудниками ОВД : монография / Е.А. Ануфриева — Новосибирск: Изд-во НГТУ, 2014. С. 186.

недостатки слухового восприятия у эксперта. Значимость данного фактора обусловлена спецификой процесса исследования, в рамках которого все необходимые методики осуществляются посредством личного анализа экспертом фонограммы, т.е. собственным слухом. Поэтому уровень чувствительности слухового аппарата эксперта и степень его фонетической подготовки являются очень важными для корректного восприятия и анализа звукосодержащего носителя.

Е.И. Галяшина также отмечает следующее: «Большую роль играет носитель, на который был зафиксирован звуковой след. Такими являются цифровые и аналоговые носители. Аналоговый сигнал представляет собой непрерывный во времени и по амплитуде процесс, а его цифровое представление есть последовательность или ряд чисел, состоящий из конечного числа бит. Поэтому преобразование аналогового сигнала в цифровой состоит из двух этапов: дискретизации по времени и квантования по амплитуде. Это означает, что в отличие от аналогового сигнала, в случае оцифровки, все исследования производятся с сигналом, превращенным в ряд цифр»[95].

На сегодняшний день цифровая запись звука вытеснила аналоговые способы собирания и исследования звуковых следов, а это значит, что экспертам требуется учитывать специфику данного вида носителей. Когда речь идет о цифровом носителе, сразу появляется большой риск возможности внесения в такую запись изменений, которые по разным объективным и субъективным причинам могут быть не обнаружены экспертом. В данном случае имеется в виду монтаж.

В соответствии с ГОСТ 13699-91 «Запись и воспроизведение информации. Термины и определения»: «Монтажом фонограммы называется объединение двух или более частей одной или нескольких ранее записанных фонограмм путем перезаписи, при котором могут вноситься изменения в записываемую информацию

---

[95] Галяшина, Е. И. Современные проблемы экспертного исследования звуковых следов / Е. И. Галяшина // Известия Тульского государственного университета. Экономические и юридические науки. — 2013. — № 4-2. — С. 38.

и может изменяться очередность фрагментов»[96]. Также Е.И. Галяшина говорит: «А природа цифровой записи такова, что сигнал в ней представлен в виде дискретной последовательности значений, не имеющих физической связи с носителем информации. Цифровое представление звуковых данных позволяет производить практически любые манипуляции с ними без выявления первичных признаков монтажа или редактирования. Звуковой сигнал в цифровой форме разбивается на фрагменты, которые состыковываются в необходимой последовательности друг с другом. Далее каждый стык – монтажный переход – и вся фонограмма обрабатываются различными фильтрами и программами редактирования сигналов с целью уничтожения или маскировки следов монтажа»[97]. А это вполне может привести к неверному выводу эксперта, если, например, будет стоять вопрос о факте монтажа звукозаписи.

Аналоговые носители тоже не исключают возможности внесения в запись каких-либо изменений, однако, как нами уже отмечалось, в силу использования сейчас в основном цифровых носителей этот факт не имеет такого большого значения. Такая ошибка эксперта может быть следствием не только специфики цифрового носителя, но и собственной небрежностью в процессе исследования. Речь здесь идет о том, что зачастую экспертами игнорируется факт перезаписи цифровой фонограммы с другого носителя, природа которого может быть даже не установлена, а значит, и необходимое сравнение цифровой записи с оригиналом фонограммы с сопоставлением технических характеристик и содержания записей тоже не осуществляется. В связи с этим эксперт в целях предотвращения экспертной ошибки должен требовать предоставления устройств звукозаписи, сведений о технологической цепочке записи и обстоятельств ее производства. В противном случае будет иметь место процессуальная ошибка.

---

[96] ГОСТ 13699-91 «Запись и воспроизведение информации. Термины и определения». — Москва : Стандартинформ, 2005. — 61 с.

[97] Галяшина, Е. И. Цифровые фонограммы как доказательства / Е. И. Галяшина // Эксперт-криминалист. — 2008. — № 4. С. 46.

К такому же выводу пришел Г.Н. Зубов: «Отсутствие на фонограмме-копии признаков монтажа или изменений, внесенных в процессе записи или после ее окончания, не значит, что указанные признаки отсутствуют на фонограмме-оригинале. Так, например, если оригинальная фонограмма записывается с использованием цифрового магнитофона, а затем монтируется на компьютере, после чего копируется на аналоговый носитель, то получится аналоговая копия цифровой фонограммы, где признаки монтажа или привнесенных изменений будут отсутствовать. В этом случае в итоге получается измененная цифровым способом аналоговая фонограмма, качество записи которой соответствует аналоговому диктофону-магнитофону со следами цифровой обработки речевых сигналов»[98].

В ФЗ «Об обеспечении единства измерений» № 102-ФЗ отмечается следующее: «Как показывает экспертная практика, участники судопроизводства все чаще стали уделять особое внимание техническим средствам и приборам, при помощи которых производятся различные измерения в ходе фоноскопической экспертизы. По мотивам применения приборов, не являющихся сертифицированными средствами измерений, не проверенных в установленном порядке, заключение эксперта признается недопустимым доказательством, полученными с нарушением норм законодательства»[99].

Таким образом, при производстве фоноскопической экспертизы большое внимание должно уделяться природе материалов, представленных на экспертизу. Эксперт должен понимать, что перед ним находится: фонограмма-копия или фонограмма-оригинал (при решении вопроса о возможности факта монтажа этот момент является основополагающим).

---

[98] Зубов Г.Н. «Я не я, и голос не мой»: О возможностях фальсификации фонограмм с помощью современных технологий синтеза устной речи // Сайт «Праворуб» [Электронный ресурс]. — URL: https://pravorub.ru/personal/78856.html (дата обращения: 12.01.2025).

[99] Российская Федерация. Законы. Об обеспечении единства измерений : Федер. закон № 102-ФЗ : принят Государственной Думой 11 июня 2008 г.: одобрен Советом Федерации 11 июня 2008 г. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_77904/ (дата обращения: 13.02.2025).

В век современных технологий, на наш взгляд, эксперт должен всегда держать в уме фразу «технологическая цепочка записи» и никогда не умалять ее значения для процесса исследования. Эксперт в силу специфики проводимого исследования должен уметь отличать понятия «оригинал»/ «дубликат»/ «копия» фонограммы и «оригинал»/ «дубликат» / «копия» файла с фонограммой, что связано, как уже говорилось, с большой вероятностью бесследного или практически не опознаваемого привнесения в запись каких-либо сторонних сведений, первоначально на записи не присутствовавших. В противном случае никаких признаков наличия в записи элементов монтажа экспертом обнаружено не будет, пусть даже в фонограмме-оригинале эти элементы есть: просто в силу того, что представленные записи по внешним и, возможно, внутренним параметрам на взгляд человека, так хорошо в природе цифровых и аналоговых записей не разбирающегося, будут идентичными, эксперт может даже не задуматься о том, что у представленной записи был оригинал, поэтому факт монтажа им установлен, естественно, не будет. Не исключено, что здесь также может иметь место умышленное предоставление уполномоченным лицом эксперту заранее сфальсифицированных объектов, поэтому, на наш взгляд, эксперт, проводящий фоноскопическую экспертизу, должен также обладать хотя бы базовыми знаниями в области цифровой и аналоговой записи, что, конечно же, на практике реализуется не всегда.

Изучив природу причин экспертных ошибок, мы можем смело сказать, что они не являются результатом какого-то одного определенного фактора, что подразумевало бы односторонность экспертной ошибки. Экспертная ошибка, будь она обусловлена как объективными, так и субъективными причинами, происходит в результате стечения ряда определенных обстоятельств, взаимосвязанных друг с другом (например, как мы уже рассматривали, причина объективной ошибки, не обязательно приводящая к её совершению + субъективные факторы личности эксперта = совершение экспертной ошибки). Поэтому, чтобы выявить такие причины, а в дальнейшем и попытаться предотвратить их возникновение,

требуется всестороннее рассмотрение как самого хода экспертного исследования с примененными в его ходе методиками, так и личности субъекта экспертной деятельности.

В самом общем виде *экспертная ошибка представляет собой не соответствующее объективной действительности суждение эксперта и/или его действия, не приводящие к цели экспертного исследования, если искаженное суждение и/или неверные действия представляют собой результат добросовестного заблуждения*.

Для лучшего понимания представленные определения были разобраны на отдельные составляющие, такие как, например, добросовестное заблуждение. Сделано это было в целях грамотного разграничения, на первый взгляд, смежных понятий «экспертная ошибка» и «заведомо ложное заключение эксперта». Фактор добросовестности в данном случае будет решающим. Именно поэтому нами было предложено ввести в практику некоторые правила и способы для установления факта добросовестности заблуждения эксперта. Вместе с этим нами также были представлены некоторые существующие виды и классификации экспертных ошибок, которые в дальнейшем были спроецированы на определенные стороны изученных вопросов.

У каждой ошибки есть предшествующая ей причина, поэтому в рамках исследования экспертной ошибки были проанализированы причины совершения экспертом ошибок. Так, причины экспертных ошибок могут носить как субъективный, зависящий от эксперта и его личности, характер, так и объективный, отражающий наличие несовершенств экспертных методик, специфику используемой техники и некоторые другие положения.

В завершение логической цепочки «ошибка – причина – способы ее устранения» мы рассмотрели способы обнаружения и профилактики экспертных ошибок. Весьма важным здесь является комплексный характер осуществления такой деятельности, а именно участие в ней не только самого эксперта, но и других участников процесса, а также суда и следствия. Это связано с тем, что, во-первых,

риск совершения экспертной ошибки возможен не только на любой стадии экспертного исследования, но и вне его рамок, например, в момент формулировки следователем постановления о назначении судебной экспертизы и определением круга объектов, которые будут представлены на экспертизу; а во-вторых, со значимостью участия в профилактической деятельности экспертного сообщества, которое способно на основании анализа судебной практики и судебных ошибок выдвинуть возможные пути и способы для их устранения.

В осуществлении процесса профилактики ошибок нами было обращено внимание на важность предшествующей ему стадии выявления причины совершенной ошибки, от которой будет зависеть, ту ли ошибку эксперта пытались выявить и предотвратить. Также предлагаем осуществлять профилактику совершения ошибок не только со стороны эксперта, но и лиц, назначающих судебную экспертизу, поскольку, как мы видим, причиной экспертной ошибки могут быть и неправильные действия следователя, например, при формулировании вопросов, поставленных перед экспертом.

Для наглядности изучим практику проявления совершенных экспертных ошибок на примере судебной фоноскопической экспертизы. Конечно, здесь речь не может уже идти только об общей природе экспертной ошибки, поскольку, как и сами эти экспертизы в своем проявлении специфичны, так и ошибки здесь обладают определенными особенностями. В частности, при проведении судебной фоноскопической экспертизы особое внимание должно уделяться наличию возможности практически бессимптомного монтажа оцифрованной записи, что связано с природой такого материалоносителя. Ключевая роль здесь отведена технологической цепочке записи, которая подразумевает под собой весь путь оригинала фонограммы до того вида, в котором его представили на экспертизу, и именно игнорирование данного фактора чаще всего служит причиной совершения экспертной ошибки в рамках фоноскопической экспертизы.

Таким образом, недостаточная компетентность выступает одной из главных причин субъективных ошибок экспертов, осуществляющих различные виды

судебных экспертиз. На наш взгляд, эксперт должен обладать не только знаниями, непосредственно касающимися правил и методик проведения самой экспертизы, но и знаний из смежных областей, без которых не будет складываться общая картина исследования и не могут быть достигнуты его цели и задачи. Это может касаться знаний специальной терминологии, не входящей в рамки экспертной методики, но входящей в область науки, изучающей объект, представленный на исследование, его природу.

Сущность экспертной ошибки сложна и многогранна, и для того, чтобы не только понять ее, но и попытаться предотвратить, требуется приложение совместных усилий, изучение многолетней экспертной практики и скрупулезная работа по устранению причин, способствующих их совершению, а также рекомендаций экспертам в осуществлении ими экспертной деятельности.

1.3. Причины и предпосылки появления новых экспертных ошибок в условиях цифровизации

Работа судебного эксперта сопряжена с определенными быстро изменяющимися внешними факторами, которые необходимо учитывать в процессе выполнения судебных экспертиз во избежание ошибок. Как уже отмечалось, существует множество причин возникновения экспертных ошибок, они могут быть субъективными и объективными. На сегодняшний день учеными и экспертами проведено немало исследований, позволяющих классифицировать ошибки, а также выявлять их причины, возможные пути устранения. Однако человеку не всегда подвластна способность предусмотреть развитие технологического процесса, которое может пошатнуть устоявшуюся систему экспертных ошибок и, более того, спровоцировать их еще большее появление. Речь идет о цифровизации всех сфер человеческой жизнедеятельности, перевода привычных объектов, исследуемых судебными экспертами, в мало изученный цифровой формат.

Характеристики экспертных ошибок на данный момент претерпевают множество изменений и трансформаций в силу цифровизации. Появление новых объектов в цифровой форме требует применения к ним новых подходов, правил и методов исследования. Следовательно, эксперты в процессе работе с новыми объектами допускают качественно новые ошибки, которые нуждаются в системном, видоизмененном устранении.

Принципиально новый характер экспертных ошибок обуславливается, прежде всего, тем, что при работе с объектами в цифровой форме возможны ошибки со стороны эксперта, по причине некачественного программного обеспечения. Помимо этого, имеют значение следующие моменты:

- ошибки в программном обеспечении, используемом для трансформации объектов в цифровую форму, которые могут привести к искажению данных или неправильным результатам;

- использование неповеренного оборудования, нелицензионных программ и приложений, искажающих первоначальные характеристики цифрового объекта и др.

Сложность для экспертов заключается в том, что в силу новизны, отсутствия устоявшейся практики, а также комплексного характера каждого нового цифрового объекта, обладающего целым перечнем дополнительных свойств и параметров, создание грамотной и научно апробированной методики или трансформация уже существующей сильно затрудняется. А.А. Аубакирова обращала внимание на необходимость изучения экспертных ошибок с определенной периодичностью: «Изучение экспертных ошибок должно проводиться с определенной периодичностью, которая зависит от формирования новых родов, видов или подвидов судебных экспертиз. При исследовании новых объектов экспертизы, разработке и использовании новых методов и технических средств, безусловно, могут возникать и экспертные ошибки. Особое внимание следует обратить на широко внедряемые в экспертную практику процессы автоматизации экспертного

производства, внедрение автоматизированного рабочего места и другие»[100]. Таким образом, автор вполне обоснованно полагает, что появление новых экспертных ошибок связано со множеством факторов, среди которых появление новых объектов экспертного исследования выступает особенно значимым.

В этой связи важно обратить внимание на потенциально новые цифровые объекты и предположить на теоретическом уровне, какие ошибки при их исследовании со стороны судебного эксперта могут быть допущены.

Одной из наиболее серьезных и очевидных экспертных ошибок является отсутствие апробированной методики, которая отвечала бы задачам экспертизы при исследовании цифровых объектов. Рассмотрим видоизменение данной объективной ошибки в ракурсе цифровизации на примере такого цифрового объекта, как скриншот. Скриншот представляет собой снимок экрана, фиксирующий то, что в момент снимка находилось на экране устройства (мобильное устройство, компьютер и т.д.). Процесс создания скриншота прост: для этого требуется лишь нажатие 1-2 клавиш и несколько секунд времени. Если говорить о ПК (персональные компьютеры), то на сегодняшний день операционные системы большинства компьютеров предусматривают наличие программного обеспечения либо отдельных программ для быстрого создания скриншота (например, LightShot, ФотоСкрин, Screen Capture, также встроенная в клавиатуру клавиша «PrtSc»).

Простому созданию такого цифрового объекта соответствует такая же легкая и быстрая возможность его видоизменить, внести ложные сведения, сфальсифицировать, причем не только сам скриншот, но и содержащуюся в нем информацию.

Обратим внимание на тот момент, что доказывание фальсификации скриншота схоже с доказыванием фальсификации письменного доказательства –

---

[100] Аубакирова, А. А. Следственные и экспертные ошибки при формировании внутреннего убеждения : дис.... д-ра юрид. наук : 12.00.12 / Аубакирова Анна Александровна. — Челябинск, 2010. С. 354.

будь это поиск ошибок в тексте, логических несостыковок представленного на снимке экрана, противоречивых данных, следов внесения изменений. Если при работе с письменным документом действия эксперта относительно отлажены благодаря перечню «подсказывающих» факторов (следы внесения исправлений, несоответствия шрифта, размеров, оттенков печатного изображения), то в случае с цифровым изображением необходима надежная, научно обоснованная база программ и приложений, позволяющих выявлять следы фальсификации. Особая сложность данной проблемы заключается и в том, что приложения, программные установки очень трудно привести к единому стандарту, который был бы закреплен на уровне ГОСТ, соответствовал целому ряду исходных критериев, был внедрен для использования экспертами повсеместно. На наш взгляд, перечень методов и инструментов должен быть определен и включен в соответствующую методику по исследованию снимков экрана.

Судебная практика по данному вопросу не столь обширна, однако она наталкивает на формулирование вывода о наличии целого ряда проблем при работе со скриншотами. Так, по делу об оспаривании интеллектуальных прав в качестве одного из доказательств была представлена распечатка скриншота страницы архивной копии сайта «Экострада.рф» с содержащейся на ней информацией, имеющей значение для исхода дела. Однако данное доказательство было признано судом необоснованным ввиду следующего: «При этом коллегия судей в результате исследования экземпляров спорного скриншота обнаружила, что указанный скриншот подвергался обработке либо масштабированию при его выводе на печать, в результате чего часть информации, в том числе системные дата и время, отображаемые в области уведомлений панели задач операционной системы, отсутствуют в указанном документе»[101].

[101] Решение Суда по Интеллектуальным правам от 07.12.2020 № 1027_267512 по делу № СИП-311/2020 // Картотека арбитражных дел «Мой арбитр». — URL: https://goo.su/C4Oa (дата обращения: 03.08.2024 г.).

В первую очередь возникает закономерный вопрос, почему решение вопроса о наличии или отсутствии обработки скриншота предоставлено на усмотрение коллегии судей, а не судебного эксперта. Во-вторых, с учетом того, что одна из сторон настаивала на достоверности скриншота, а другая оспаривала этот момент, а также принимая во внимание озадаченность суда при рассмотрении такого доказательства, можно сделать вывод о том, что на данный момент неясно: является ли масштабирование снимка экрана его непосредственной фальсификацией, препятствующей признанию доказательства допустимым. Стоило бы также выяснить, в силу чего произошло изменение масштаба при выводе на печать, поскольку искажение данных может произойти и в результате ошибок оператора, и при сбое оборудования, и в силу целенаправленных действий заинтересованных лиц – в каждом из этих случаев достоверность доказательства должна устанавливаться по-разному[102].

По нашему мнению, исследование скриншота целесообразно поручить судебному эксперту, следует определить, какие именно изменения, привносимые в документ, следует в рамках экспертизы признавать фальсификацией. Решение вопроса о подделке цифрового объекта на сегодняшний день является спорной и сложной задачей даже для экспертов, коллегия судей, несмотря на их опытность, может попросту не обладать необходимым комплексом знаний о цифровой среде. Также не стоит забывать, что достоверность или недостоверность скриншотов, как цифровых документов, схожа с определением достоверности обычных письменных документов. Задача судебного эксперта, как лица, обладающего специальными знаниями, сводится к выявлению, определению и обобщению признаков, указывающих на то, что документ подвергался каким-либо изменениям.

Указанные трудности препятствуют накоплению экспертной практики при работе с цифровыми объектами и, соответственно, выработке надлежащей методики.

---

[102] Осипенко, А. Л. Проблемы вовлечения электронно-цифровых следов в уголовный процесс / А. Л. Осипенко // Научный вестник Омской академии МВД России. — 2009. — №4. С. 33.

Следующая и не менее серьезная проблема – неполное исследование цифрового объекта экспертами. В своей диссертации А.В. Рыбин справедливо отмечает, что для признания цифрового объекта доказательством необходима его конвертация в бумажный носитель для того, чтобы следователь и другие лица имели возможность воспринимать его в привычном виде[103]. Однако исследование судебным экспертом переформатированного в бумажный вариант цифрового объекта не обеспечивает его полноценного изучения и не отвечает задачам судебной экспертизы.

В подтверждение данной точки зрения высказывался в своей диссертации Р.И. Оконенко: «Исследование «цифрового доказательства» — это изучение информационного содержания цифрового носителя информации, связанное с совершением действий в виртуальной среде (открытием папок с файлами, самих файлов, изучением свойств файлов посредством использования иных программ и т.п.). Не может приравниваться к исследованию «цифрового доказательства» внешний осмотр либо иное изучение характеристик электронного носителя информации как реального материального объекта (в частности определение его веса, размера, формы, производителя, модели, других внешних индивидуализирующих признаков)»[104]. По его мнению, исследование цифрового объекта происходит в двух формах: изучение основного содержания файла (например, текста при открытии текстового файла) и изучение сведений, касающихся свойств и характеристик самого файла (время, место создания, расположение в папке и т.д.). Очевидно, что вторая форма исследования невозможна при работе исключительно с материальной копией. Приведенный ранее пример из судебной практики как раз демонстрирует описанную нами

---

[103] Рыбин, А. В. Электронный документ как вещественное доказательство по делам о преступлениях в сфере компьютерной информации (процессуальные и криминалистические аспекты: дис. ... докт. юрид. наук : 12.00.09 / Александр Владимирович Рыбин. — Краснодар, 2005. С. 56.

[104] Оконенко, Р.И. «Электронные доказательства» и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ законодательства Соединенных Штатов Америки и Российской Федерации: дис. … канд. юрид. наук : 12.00.09 / Оконенко Роман Иванович. — Москва, 2016. С. 67.

ошибку – неясность с ролью предоставленного в качестве доказательства снимка экрана является следствием неправильного исследования: объект рассматривался только в бумажном варианте без параллельного изучения самого цифрового файла.

То же самое исследование цифрового объекта в виде текста в рамках автороведческой экспертизы на предмет установления авторства может быть неполным в том случае, если судебный эксперт упустит из виду изучение свойств цифрового файла. Компьютерная система при создании и работе с файлом предусматривает сохранение сведений об источнике документа: в подробных свойствах можно посмотреть, кем он создан документ, каким лицом изменен, количество редакций, дату создания, редактирования, последнего сохранения – и это возможности только базовой операционной системы компьютера. Уточнение таких сведений может быть полезно, например, в ситуациях, когда есть основания полагать, что лицо не является подлинным автором документа[105]. Дата редактирования или печати файла может помочь эксперту в том случае, если два лица настаивают на авторстве одного и того же текста. Однако здесь стоит учитывать необходимость наличия у эксперта-автороведа достаточного уровня знаний в области судебной компьютерно-технической экспертизы, полученных, например, в рамках повышения квалификации или обучения по специальности 40.05.03 «Судебная экспертиза», и позволяющих ему проводить исследование цифровых признаков объекта. В том случае, если для проведения исследования необходимо восстановление файла, определение его формата и метаданных по шестнадцатеричному коду или ASCI, может потребоваться проведение комплексной автороведческой и компьютерно-технической экспертизы.

Наконец, еще один аргумент в пользу обязательного исследования экспертом цифрового объекта в двух формах – это несовершенство ЭВМ. А.Л. Осипенко предлагал дифференцировать цифровые файлы по способу их создания:

---

[105] Шихалиева С.З. Трансформация экспертных ошибок в контексте появления новых цифровых объектов / С. З. Шихалиева // Вестник университета имени О.Е. Кутафина (МГЮА). — 2024. — № 3. С. 172.

- файлы, являющиеся аналогом обычных документов, созданные и сохраненные в компьютере человеком (почтовые сообщения и т.д.);

- файлы, созданные без участия человека: они сгенерированы компьютером автоматически (рассылка от робот-почты);

- файлы гибридного формата, где алгоритмическая часть задается компьютером, а содержимое (вводимые данные) человеком[106]. Данный формат цифровых файлов особенно актуален в рамках проведения экономических экспертиз.

Представленный метод разделения файлов имеет для судебного эксперта следующее значение. Во всех указанных случаях часть файла, выполняемая порождающей программой компьютера, может давать сбой (неправильно заданный код, сбой программы, вредоносный вирус, искажающий выполнение функций, намеренное изменение работы программы заинтересованным лицом). Эксперт должен учитывать возможность такого исхода событий и проявлять осторожность: даже если кажется, что в бумажном и цифровом носителях нет никаких видимых признаков фальсификации данных, необходимо проводить дополнительную проверку. Безусловно, для этих целей требуется разработка системы программного обеспечения, отвечающего целям и задачам судебной экспертизы. Целесообразность разработки стандартизированного и сертифицированного программного обеспечения сбора так называемых «компьютерных доказательств» отмечают ученые. Действительно, «потребность в надежных методиках, гарантирующих достоверность результатов анализа при проведении экспертизы данных на электронных носителях»[107], является значительной.

Причины допущения экспертом ошибок при исследовании цифровых объектов сложны и неоднородны, представляется уместным рассмотреть следующую взаимосвязь. Среди ученых и теоретиков укоренилось точка зрения,

---

[106] Осипенко, А. Л. Проблемы вовлечения электронно-цифровых следов в уголовный процесс / А. Л. Осипенко // Научный вестник Омской академии МВД России. — 2009. — №4. С. 34.
[107] Осипенко А.Л. Указ. соч.

согласно которой следователь или суд в формировании объективных экспертных ошибок играют не последнюю роль. Так, например, Н.С. Неретина описывает существующую взаимосвязь между следственными, судебными и экспертными ошибками: «Обобщение экспертной практики свидетельствует, что многие экспертные ошибки возникают вследствие ошибок или небрежного отношения к своим обязанностям правоприменителя»[108].

Согласно ч.1 ст. 195 УПК РФ следователь или суд при назначении судебной экспертизы обязательно указывает в постановлении (определении) перечень материалов, предоставляемых в распоряжение эксперта[109]. Соответственно, от правильности и полноты отобранных следователем объектов и образцов напрямую зависит качество выполненной экспертизы и корректность сформулированного вывода. Если перечень предоставленных в распоряжение объектов является неполным, качество образцов малоинформативным, а сами объекты были отобраны с нарушениями, то избежать экспертную ошибку крайне сложно.

На наш взгляд, законодателем предусмотрена возможность устранения ошибок на этапе отбора образцов для сравнительного исследования путем выделения в Уголовно-процессуальном кодексе РФ такого участника, как специалист. Согласно ч.1 ст. 58 УПК РФ специалистом является лицо, обладающее специальными знаниями, привлекаемое к участию в процессуальных действиях для содействия в обнаружении, закреплении и изъятии предметов и документов, применении технических средств в исследовании материалов уголовного дела, для постановки вопросов эксперту, а также для разъяснения сторонам и суду вопросов, входящих в его профессиональную компетенцию. Роль специалиста при работе с цифровыми объектами нельзя переоценить, поскольку именно опыт и

---

[108] Неретина, Н. С. Взаимосвязь следственных, судебных и экспертных ошибок / Н. С. Неретина // Вестник Университета имени О.Е. Кутафина (МГЮА). —2024. — №3 (115). С. 101.

[109] Уголовно-процессуальный кодекс Российской Федерации : Федер. закон № 174-ФЗ : принят Государственной Думой 22 ноября 2001 г.: одобрен Советом Федерации 05 декабря 2001 г.: послед. ред. 21.04.2025 г. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_34481/ (дата обращения: 13.02.2025).

компетентность специалиста способны обеспечить успешность процесса отбора сравнительного материала.

В случае с отбором образцов в виде фото- и видеоизображений для проведения судебной почерковедческой, портретной, видеотехнической, компьютерно-технической экспертиз специалист (как предполагается) в силу своей осведомленности о функционале и особенностях работы современных мобильных устройств, будет иметь возможность оказать содействие следователю в грамотном отборе необходимых образцов.

Не стоит забывать, что исключение ошибок должно быть двусторонней инициативой, которая должна исходить как от следователя (суда), так и от эксперта. Иными словами, в том случае, если следователь понимает, что ему предстоит обеспечить эксперта надлежащим материалом для исследования, привлечение специалиста должно быть приоритетным для него. И наоборот, если эксперт на этапе ознакомления и предварительной оценки объектов и сравнительных образцов понимает, что материал был искажен, а действительное отображение внешности/документов видоизменено, его задача – сообщить об этом следователю для устранения допущенных ошибок.

Описанные ошибки составляют небольшую часть из множества примеров неправильной работы следователя при отборе цифровых объектов для назначения судебной экспертизы. Подводя итог всему вышесказанному, можно заключить, что проблема запечатления внешности человека или объектов материального мира на мобильные устройства, заведомо искажающие итоговое отображение всех важных характеристик, способно повлечь за собой целый ряд экспертных ошибок вплоть до формулировки неправильного вывода.

В качестве субъективной ошибки, допускаемой судебным экспертом при производстве исследования цифрового объекта, можно рассматривать неправильную оценку своей компетенции. Опрос среди экспертов позволил сформулировать две противоположные точки зрения относительно того, должен ли эксперт одной специальности обладать также специальными знаниями в области

компьютерно-технической экспертизы при исследовании свойств и признаков цифрового объекта. Одни склоняются к тому, что исследование базовых характеристик цифрового файла, записи является лишь получением сопровождающей информации, а установление таких параметров уже не требует применения специальных знаний и подвластно бытовому пользователю ПК. Другие, напротив, считают, что эксперт обязан владеть соответствующими специальными знаниями в области судебной компьютерно-технической экспертизы.

В подтверждение последней точки зрения можно привести ряд аргументов. Во-первых, конечная цель деятельности эксперта по установлению параметров и свойств файла отличается от той цели, которую ставит перед собой обычный пользователь: эксперт использует данную информацию не опосредованно, а во взаимосвязи с другими признаками объекта, которые позволили бы сформулировать какой-то вывод. Во-вторых, действия эксперта имеют процессуально значимую важность – исследование цифровых свойств файла так же важно, как и изучение «типичных» для объекта признаков, в обоих случаях необходимо наличие специальных знаний в соответствующих областях. Наконец, чтобы понимать значение тех или иных цифровых признаков, уметь выполнять ряд команд и алгоритмов по их выявлению на уровне сведущего лица в аспекте судебно-экспертной деятельности, специальные знания крайне важны.

Таким образом, анализ некоторых разновидностей объективных и субъективных ошибок, допускаемых следователями и экспертами при работе с цифровыми объектами, позволил сделать следующие выводы. В качестве профилактики таких ошибок необходима разработка специализированного курса, реализуемого в рамках подготовки судебных экспертов. Для организации такого курса предлагается скомпилировать уже имеющиеся знания по работе с цифровыми следами для того, чтобы выявить моменты, вызывающие затруднения. На наш взгляд будет полезно привлечение специалистов, в чьи прямые обязанности входит разработка, поверка и изучение характеристик мобильных устройств.

Участие такого специалиста понадобится для разработки вышеуказанного специализированного обучающего курса, где в качестве необходимых знаний будущие следователи и эксперты будут получать сведения, касающиеся характеристик современных мобильных устройств, а также их интерпретаций. Такое обучение позволит устранить пробелы в понимании следователем и экспертом функционала мобильных устройств, а также влияния, которое конкретные функции могут оказать на итоговое отображение характеристик внешности или объектов материального мира.

Не стоит обходить стороной и вопрос грамотной организации обучающего курса. Для того, чтобы и у следователей, и у экспертов в будущем была возможность систематически повышать квалификацию в данной области в рамках дополнительных курсов, необходимо уже на этапе получения высшего образования в вузах внедрить дисциплину, посвященную работе с цифровыми следами, отдельно для следователей и отдельно для экспертов. Такое обучение для будущих следователей в рамках образовательной программы вполне возможно при освоении таких дисциплин, как «Экспертиза в судопроизводстве» или «Криминалистика». А для будущих экспертов – в рамках дисциплин, соответствующих их экспертной специализации.

Процесс цифровизации трансформирует экспертные ошибки ввиду появления новых объектов судебных экспертиз, что требует актуализации требований к их обнаружению, изъятию и упаковке и обновления методического обеспечения экспертного исследования таких объектов с учетом их специфики. Новизна, связанная с природой цифровых объектов судебных экспертиз, не препятствует использованию приведенных выше классификаций экспертных ошибок (исходя из сущности экспертной ошибки и характера причин появления экспертных ошибок) при проведении анализа причин экспертных ошибок при исследовании объектов в цифровой форме и прогнозирования появления связанных с этим новых ошибок, а также для их предотвращения и профилактики.

Изучение теоретических основ сущности, причин возникновения и классификаций экспертных ошибок, а также их трансформации в свете появления объектов судебных экспертиз в цифровой форме позволило сделать следующие выводы:

- сформулировать собственное определение цифрового объекта: цифровой объект – это объект, содержащий в себе криминалистически значимую информацию о предметах или действиях, представленный в цифровой форме, созданный в виртуальной среде либо преобразованный в цифровой формат вспомогательными средствами в результате совместных действий человека и компьютера (иного устройства);

- выделить разновидности цифровых объектов, в соответствии с которыми по структуре цифровые объекты делятся на простые и сложные;

- обозначить некоторые виды объективных и субъективных ошибок, которые допускаются экспертами при работе с цифровыми объектами.

ГЛАВА 2. ТИПИЧНЫЕ ОШИБКИ ПРИ ПРОВЕДЕНИИ РАЗЛИЧНЫХ ВИДОВ ЭКСПЕРТИЗ НОВЫХ ОБЪЕКТОВ: СОВРЕМЕННЫЕ ВОЗМОЖНОСТИ ПРОГНОЗИРОВАНИЯ И ПРОФИЛАКТИКИ

2.1. Процессуальные ошибки судебных экспертиз объектов в цифровой форме

Исследование природы и отличительных особенностей объектов в цифровой форме позволило выделить потенциально проблемные аспекты работы с такими объектами судебного исследования правоприменителем, с одной стороны, и судебным экспертом – с другой. Неправильное изначальное изъятие цифрового следа и последующий перенос на материальный носитель, упущение ключевых сводных данных следа, неправильная упаковка – это лишь некоторые предпосылки, способные привести к допущению множества ошибок.

Рассмотрим варианты ошибок, которые могут быть допущены следователем и экспертом в силу такого качества цифрового следа, как легкоизменяемость. Простота внесения корректировок, умышленное изменение первоначального состояния документа, тем более с учетом современных программ и приложений, на наш взгляд, требует особого внимания и своевременной «ликвидации». Безусловно, речь идет не о том, чтобы направить все усилия на устранение возможности внесения изменений в цифровой файл в принципе. Это необходимо делать лишь в рамках предоставления цифрового объекта на экспертное исследование. Практически любые действия в компьютерной среде приводят к образованию цифрового следа. Аналогично этому процессу, любые операции с цифровым файлом отражаются в его сводных данных – контрольной сумме, или хеш-сумме.

Хеш, хеш-сумма (от англ. hash — путаница, мешанина) — последовательность символов фиксированной длины, полученная путем преобразования произвольных исходных данных (числа, текста, файла и др.) при

помощи специального математического алгоритма, которая однозначно соответствует этим исходным данным, но не позволяет их восстановить[110]. Согласно интернет-источникам, одним из свойств хеш-суммы является ее уникальность. Если хешированию подвергаются разные исходные данные, пусть даже различающиеся незначительно, итоговый хеш будет разным. И наоборот, использование различных алгоритмов и программ для подсчета одних и тех же исходных данных даст один и тот же хеш. Можно сказать, что хеш-сумма представляет собой точно рассчитанный, уникальный математический образ определенного файла. Хеш-сумма, как правило, предстает в виде шестнадцатеричного кода, а этот код в свою очередь соответствует совокупности сведений, из которых состоит цифровой файл.

Хеш-сумма – это математическая единица, следовательно, изменение ее слагаемых неизбежно приведет и к изменению итогового значения их суммы. Значит, любое привнесенное в файл изменение отразится в хеш-сумме, таким образом, она изменится, что будет свидетельствовать обо всех изменениях и трансформациях, которые происходили с файлом. Сравнивая контрольные суммы файла, можно сразу узнать, был он модифицирован или нет. Если есть ошибка контрольной суммы, контрольная сумма не соответствует требуемой или имеющейся, то это значит, что файл был изменен.

Полагаем, следует рассматривать хеш-сумму файла как значимую характеристику при работе с объектами в цифровой форме. В первую очередь, стоит сразу оговориться, мы не заявляем о том, что контрольная хеш-сумма файла является его идентификатором, она не указывает на оригинальность следа сама по себе. В рамках судебного-экспертного исследования хеш-сумма лишь подтверждает, что экспертом на исследование был получен именно тот файл, который ему направил правоприменитель. Таким образом, соответствие хеш-

---

[110] Энциклопедия «Касперского». URL: https://encyclopedia.kaspersky.ru/glossary/hash/?ysclid=m5crbl0myp242650144 / (дата обращения: 12.01.2025).

суммы файла свидетельствует о том, что в первоначальное содержание цифрового файла не вносилось никаких изменений.

Обратим внимание на то, что мы говорим о соответствии хеш-суммы. Хеш-сумма файла сама по себе не даст ни следователю, ни эксперту никакой информации. Для того, чтобы она начала иметь смысл, таких контрольных сумм обязательно должно быть две. С одной стороны, эксперт при получении цифрового следа на материальном носителе должен самостоятельно проверить хеш-сумму файла. Сопоставлять получившийся код он должен с той хеш-суммой, которая указана в постановлении/определении о назначении судебной экспертизы следователем/судом. На данном этапе и начинается большинство проблем, поскольку, как показывает практика, данное условие лицами, назначающими судебную экспертизу, не соблюдается, хотя должно.

В целях выяснения мнения следователей и судей относительно целесообразности и практики подсчета хеш-суммы файла при назначении судебной экспертизы и описании цифрового следа, содержащегося на носителе, нами была разработана анкета, макет и примеры ответов представлены в Приложениях № 1 и 2.

По данным анкетирования, 40% опрошенных отметили, что в своей практике им неоднократно приходилось назначать судебную экспертизу цифровых объектов. На вопрос «Считаете ли Вы необходимым предпринимать меры по защите содержания цифрового следа от изменений?» 88,9% опрошенных из 100% ответили утвердительно, 11,1% - отрицательно. 37% респондентов не знают, что из себя представляет хеш-сумма файла, лишь 1 респондент отметил подсчет хеш-сумму как способ защиты файла от внесения изменений в качестве применяемого им инструмента.

Такая статистика, на наш взгляд, является негативной, однако 77,8% опрошенных считают указание хеш-суммы файла надежным способом защиты содержания цифрового файла. Наконец, только 22,2% респондентов осуществляли подсчет хеш-суммы в своей практике.

Для уточнения сложившейся статистики нами также были выяснены причины отрицательного ответа на данный вопрос. Среди наиболее частых причин были названы следующие: 22,2% не считают это необходимым вообще, 33,3% анкетируемых отметили, что не знают техники подсчета хеш-суммы и не уверены в правильности сведений, 14,8% опрошенных отметили, что не имеют понятия о том, что такое хеш-сумма и для чего она нужна.

Для сопоставления мнения лиц, назначающих судебную экспертизу, с мнением судебных экспертов была создана аналогичная анкета, макет и примеры ответов представлены в Приложениях № 3 и 4. В анкетировании приняли участие эксперты – сотрудники государственных, негосударственных судебно-экспертных учреждений, частных экспертов различных экспертных специальностей. 66,67% респондентов отметили, что принимали к производству экспертизу цифровых объектов хотя бы раз, у многих экспертов такими объектами выступает от 70% объектов в настоящий момент, что как раз обусловлено повсеместной цифровизацией.

77,4% опрошенных знают, что такое хеш-сумма файла, 69,8% экспертов считают ее надежным способом отслеживания изменений файла, оставшиеся 30,2% предпочли иные способы, о которых будет подробно рассказано позднее. Подсчет хеш-суммы файла осуществляет лишь 39,6 % из 100% опрошенных, что сами эксперты объяснили помимо прочих причин тем, что данный показатель им попросту не с чем сравнивать, поскольку изначально правоприменителем он не предоставляется, а осуществлять подсчет просто так нет смысла. На наш взгляд, такая точка зрения является оправданной, поскольку сама хеш-сумма, посчитанная экспертом, без заданной хеш-суммы от следователя/суда и без возможности их сравнения не даст никакой полезной информации.

Таким образом, параллельный анализ и сопоставление результатов обеих анкет позволили нам выявить довольно важную проблему. С одной стороны, следователи не считают необходимым направлять в качестве характеристики цифрового файла контрольную хеш-сумму, а с другой стороны, эксперты не имеют

возможности проверить аутентичность полученного для исследования объекта, поскольку рассчитанную ими хеш-сумму сравнивать не с чем. Отметим, что со слов самих опрошенных, такая практика является следствием двух факторов: непонимания сущности хеш-суммы и смысла ее подсчета, а также незнания процедуры.

Проведенный анализ позволяет заключить следующее. Как уже было сказано, хеш-сумма сама по себе – это не гарант того, что файл был не тронут, видоизменен, модифицирован. Данный показатель работает в совокупности, иными словами, здесь срабатывает правило простого равенства двух показателей. Если у одного и того же файла на стадии предоставления объекта на экспертизу и на этапе получения его экспертом при двухстороннем подсчете получается один и тот же контрольный код, значит, можно с большой вероятностью полагать, что эксперт на исследование получил ровно то, что ему было направлено. Безусловно, хеш-сумма не является единственно верным и абсолютно надежным показателем, однако природа цифровых следов очень сложна, каждый из них уникален, обладает отличными от других характеристиками, и при таком раскладе хеш-сумма выступает как один из показателей, который может быть общим для всех.

Рассмотрим, какие здесь могут быть допущены ошибки со стороны следователя и эксперта. В первой главе мы отмечали, что следственные и экспертные ошибки непременно взаимосвязаны между собой, именно поэтому мы беремся исследовать не только экспертные ошибки, но и следственные. Соответственно, каждому ошибочному действию следователя можно подобрать коррелирующую с ней экспертную. Например, выход эксперта за пределы своей компетенции может заключаться в решении им вопросов, для ответов на которые требуются специальные знания, которыми он не обладает: «Включение подобных вопросов в постановление (определение) о назначении судебной экспертизы – это

следственная (судебная) ошибка. Но если эксперт отвечает на подобный вопрос, а не отказывается от его решения – это уже экспертная ошибка»[111].

Итак, со стороны следователя будет ошибкой не рассчитать хеш-сумму цифрового следа, который будет в дальнейшем направлен на исследование эксперту на объекте-носителе. Ошибкой это будет потому, что в случае отсутствия базового описания следа, у эксперта не будет возможности на самом деле проверить, что именно он получил в распоряжение. Здесь можно провести аналогию с обычным объектом, например, при направлении на исследование объекта почерковедческой экспертизы, обычно указывается, на скольких страницах представлен объект, где расположены спорные подписи/записи, подлежащие исследованию. Или, например, аудиофайл, подлежащий исследованию в рамках фоноскопической экспертизы, должен быть подробно описан: какова продолжительность аудиодорожки, размер файла и т.д. Таким образом, указание хеш-суммы, как качественного признака, будет свидетельствовать о том, что в файл не были привнесены никакие изменения.

Перед тем, как раскрыть сущность самой ошибки, следует обратить внимание на следующий момент. В классификации экспертных ошибок отсутствие хеш-суммы мы относим к процессуальным ошибкам, однако такое разделение является весьма условным и делается нами с акцентом на будущее. Экспертные ошибки сами по себе достаточно трудно отнести к конкретно определенному виду, многие из них являются ошибками смешанной природы. Например, одна и та же ошибка может быть как гносеологической, так и операционной.

Аналогичная ситуация разворачивается с ошибкой в отсутствии описания хеш-суммы. Будет справедливо считать ее как гносеологической, так и процессуальной. В первом случае первопричиной будет являться незнание или непонимание следователем особенностей цифровых следов, значимости хеш-

---

[111] О судебной экспертизе по уголовным делам : Постановление Пленума ВС РФ № 28 : принято Пленумом ВС РФ 21 декабря 2010 г.: послед. ред. 29.06.2021 г. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_108437/ (дата обращения: 13.02.2025).

суммы, как индивидуализирующей характеристики, незнание о последствиях, к которым может привести отсутствие такого показателя. Это может быть также следствием некомпетентности. В любом случае, с такой точки зрения ошибка будет являться гносеологической. Процессуальной она в полной мере станет в том случае, если положение о необходимости указывать хеш-сумму цифрового следа будет закреплено на нормативном уровне. В таком случае следователь не будет выполнять предписанный процессуальный порядок при изъятии и фиксации цифрового следа. Таким образом, к процессуальным данную ошибку мы относим с перспективой на ее будущее нормативное закрепление.

Положения о хеш-сумме будут соответствовать действительности только в том случае, если создается дубликат/оригинальная копия цифрового следа, а не его конвертированный/переформатированный вариант. На это обращает внимание Е.И. Галяшина: «Фонообъект, полученный в результате конвертации аудиофайла, является не дубликатом или копией оригинального звукового следа, а новым объектом. Специфика конвертации заключается в том, что звуковой след, закодированный по одному алгоритму в цифровом записывающем устройстве, преобразуется в новый звуковой сигнал, закодированный по другому алгоритму. Только дубликат цифрового доказательства полностью воспроизводит оригинальный звуковой след»[112]. Также она отмечает значимость хеш-суммы, как индивидуального свойства, устраняющего сомнения в доказательственном значении цифрового следа: «Неизменность цифрового звукового следа может быть проверена с использованием расчета контрольных сумм (хеша) файла до и после каждого его воспроизведения, репродуцирования, передачи и т.п.»[113]

На целесообразность идеи применения хеш-кода обращает внимание в своих исследованиях цифровых следов И.Н. Подволоцкий отмечая, что он будет подчеркивать достоверность изучаемых фактов с момента изъятия цифрового

---

[112] Галяшина, Е. И. Судебная фоноскопическая экспертиза: проблемы диагностики аутентичности фонограмм / Е. И. Галяшина // Вестник Университета имени О. Е. Кутафина. — 2014. — №3. С. 17.
[113] Там же. С. 19.

следа до направления в суд. «Постоянство суммы цифровых значений определенного электронного объекта в процессе расследования будет указывать на сохранность первоначального состояния. В процессе дальнейшей работы с представленным объектом создается его копия, которую эксперт обрабатывает в зависимости от предполагаемого методикой исследования алгоритма. Все изменения, сделанные в копии файла, эксперт фиксирует в сопроводительном протоколе к своему заключению. При соблюдении данных процедур сохраняется возможность проверки правильности действий специалиста»[114].

Такое положение нашло свое отражение и в зарубежной практике. В частности, в январе 2023 года в Великобритании был разработан и введен в действие «Forensic Science Regulator code of practice» – Кодекс практики регулятора судебной экспертизы. Указанный кодекс практики касается осуществления судебно-экспертной деятельности в Англии и Уэльсе, документ на 364 страницы размещен на официальном сайте правительства Великобритании[115]. В частности, на страницах 185-186 данного кодекса содержится перечень действий, выполняемых в рамках сбора, обработки и анализа данных с цифровых устройств», куда входят также способы анализа цифровых данных. Согласно концепции Кодекса, «анализ – это ориентация на цифровые данные посредством применения заранее определенной и предписывающей стратегии изучения с помощью переданных/изъятых устройств»[116]. В частности, к методам анализа цифровых данных, изъятых из различных устройств/серверов, относится анализ файловых данных, например, идентификация файлов путем сравнения известных хешей. Также на страницах 298-299 указаны правила контроля сведений, составляющих объект исследования, при их переносе на объект-носитель, например, диск: «Однако, если намерение состоит в том, чтобы использовать USB-накопитель или

---

[114] Подволоцкий, И. Н. Использование цифровых технологий в деятельности экспертов / И. Н. Подволоцкий // Вестник криминалистики. — 2023. — № 4. С. 52.

[115] Forensic Science Regulator code of practice // Gov.UK. URL: https://www.gov.uk/government/publications/forensic-science-regulator-code-of-practice (дата обращения: 26.12.2024).

[116] Там же.

CD/DVD только в качестве носителя, то методология потребует проверенных шагов для демонстрации того, что цифровые данные остаются в том виде, в котором они были перенесены. Это может включать сопоставленные значения хеш-функций»[117].

Еще одним значимым документом, указывающим на необходимость хешировать цифровое доказательство в зарубежной практике, является Федеральные правила доказывания. Впервые принятые в 1975 году, Федеральные правила доказывания кодифицируют доказательственное право, применяемое в федеральных судах Соединенных Штатов Америки. Структура документа включает в себя 68 правил. Интересующие нас положения находятся в разделе №9 «Аутентификация и идентификация»: Правило 901. Установление подлинности или идентификация доказательств; Правило 902. Доказательства, подтверждающие сами себя. В частности, нас интересует Поправка № 902(14), согласно которой аутентифицировать копии данных можно с помощью процесса цифровой идентификации, обычно с использованием хеш-значений. Как и поправка № 902(13), это правило требует сертификации квалифицированным лицом, которое может подтвердить целостность процесса, используемого для копирования данных[118]. Полный текст Правил находится в открытом доступе на официальном сайте «Federal rules of Evidence: 2024 edition», в самом кратком виде выжимка касательно хеширования цифровых доказательств выглядит следующим образом:

- данные, копируемые с электронных устройств, носителей информации и электронных файлов, обычно аутентифицируются с помощью «хеш-значения»;

- если значения хеша для оригинала и копии различны, то копия не идентична оригиналу. Если значения хеша для оригинала и копии одинаковы, то крайне маловероятно, что оригинал и копия не идентичны;

---

[117] Forensic Science Regulator code of practice // Gov.UK. URL: https://www.gov.uk/government/publications/forensic-science-regulator-code-of-practice (дата обращения: 26.12.2024).

[118] Federal Rules of Evidence. URL: https://www.rulesofevidence.org/fre/article-ix/rule-902/ (дата обращения: 12.01.2025).

- при сборе цифровых доказательств из исходных данных генерируется хеш-значение с использованием функции хеширования, например, SHA-256. Это хеш-значение действует как уникальный цифровой отпечаток для этого конкретного доказательства;

- цифровые доказательства уязвимы для подделки, как преднамеренной, так и непреднамеренной. Значения хеш-функции обеспечивают надежный механизм для обнаружения любых изменений в доказательствах. Даже самое незначительное изменение файла приведет к совершенно другому значению хеша;

- генерация хеш-значения выполняется быстро и легко (при наличии подходящего инструмента). Размер файла также не имеет значения — генерация хеш-значения для большого файла так же проста, как и для маленького;

- если доказательство было правильно собрано и обработано, любой, кто впоследствии использует тот же алгоритм для его аутентификации, увидит точно такое же значение хеша[119].

Таким образом, изучение вышеуказанных документов позволяет говорить о том, что закрепление необходимости подсчета хеш-суммы при изъятии и сбор цифровых доказательств для последующего указания полученных сведений на уровне нормативного правового акта способно благоприятно повлиять на единообразие практики работы с такими объектами и обеспечить минимальный уровень надежности. Стоит отметить, что было бы не лишним рассмотреть возможность внедрения подобных правил и в отечественную нормативную базу, о чем будет сказано позднее.

На сегодняшний день положения о функции хеширования содержат только некоторые документы, одним из которых является ГОСТ Р 34.11-2012 — российский криптографический стандарт на хеш-функцию, введенный 1 января

---

[119] Why Hash Values Are Crucial in Digital Evidence Authentication // Pagefreezer Blog. URL: https://blog.pagefreezer.com/importance-hash-values-evidence-collection-digital-forensics#fre902 (дата обращения: 11.12.2024).

2013 года вместо устаревшего ГОСТ Р 34.11-94[120]. Областью определения данного ГОСТ, согласно самому документу, является: «определение алгоритма и процедуры вычисления хеш-функции для любой последовательности двоичных символов, которые применяются в криптографических методах обработки и защиты информации, в том числе для реализации процедур обеспечения целостности, аутентичности, электронной цифровой подписи (ЭЦП) при передаче, обработке и хранении информации в автоматизированных системах»[121]. Однако, поскольку данный документ носит рекомендательный характер и на деятельность следователей не распространяется, фактически его положения для следователей не представляют практической значимости, что в целом и является проблемой ГОСТов.

Другой вопрос – в какой момент следователь должен посчитать хеш-сумму для того, чтобы она сама по себе была достоверной. В силу того, что такой показатель способен измениться даже после незначительного, единичного видоизменения, мы полагаем, что для того, чтобы хеш-сумма обладала признаком достоверности, имеет смысл ее рассчитывать в момент первоначального обнаружения цифрового следа. Об этом также говорит Е.И. Галяшина: «Расчет контрольной суммы необходимо производить в тот момент, когда непосредственно регистрируется исходный цифровой звуковой сигнал, поскольку полученное значение является ориентиром при последующих операциях с сигналограммой. После расчета контрольной суммы любое, даже самое незначительное, изменение файла будет легко установлено»[122].

---

[120] ГОСТ Р 34.11-2012. «Информационная технология. Криптографическая защита информации. Функция хеширования» // [Электронный ресурс] URL: http://docs.cntd.ru/document/gost-r-34-11-2012.

[121] ГОСТ Р 34.11-2012. «Информационная технология. Криптографическая защита информации. Функция хеширования» // [Электронный ресурс] URL: http://docs.cntd.ru/document/gost-r-34-11-2012.

[122] Галяшина, Е. И. Проблемы использования в доказывании по уголовным делам фонограмм, получаемых по результатам оперативно-розыскных мероприятий / Е. И. Галяшина // Судебная власть и уголовный процесс. — 2018. —№2. С. 45.

Следователь может это сделать самостоятельно либо при помощи специалиста. Если не выполнить данное действие в первый момент осмотра и копирования цифрового следа, в дальнейшем не будет никаких гарантий того, что подсчитанная хеш-сумма соответствует действительности. Будь то некомпетентность или умысел следователя заменить файл или случайное изменение внутренних характеристик следа при переносе на флеш-накопитель, диск или иной носитель, промедление с подсчетом хеш-суммы будет помехой для установления ее достоверности. Иначе говоря, коэффициент доверия к такому показателю будет весьма низким.

Отдельное внимание стоит уделить тому, где целесообразно указывать хеш-сумму изъятого файла. В разработанных нами анкетах экспертами были предложены свои варианты, часть из которых уже применяется на практике. Так, контрольное значение цифрового следа предлагается указывать:

- в протоколе осмотра места происшествия, в рамках которого осуществляется непосредственное изъятие цифрового следа с последующим переносом на материальный носитель;

- в постановлении/определении о назначении судебной экспертизы.

На наш взгляд, хеш-сумму необходимо указывать в обоих случаях: первоначально в протоколе осмотра места происшествия, затем это же значение обозначить в постановлении о назначении экспертизы, чтобы цепочка передаваемых сведений была достоверной и надежной.

Не секрет, что сама идея анализа изменений файла благодаря отслеживанию хеш-суммы не является новой, она была предложена еще в начале 2000-х годов. Однако, как можно заметить, подобного рода предложения до сих пор не нашли никакого закрепления на законодательном уровне. Отсюда можно сделать вывод, что идеи без четкого алгоритма реализации в практике мало чем полезны. И хотя отчасти указание на необходимость делать запись о технических особенностях работы с электронным носителем информации при его изъятии в протоколе

следственного действия содержится в ст. 164.1 УПК РФ, важность описания всех характеристик цифрового следа, включая его хеш-сумму, никак не оговаривается.

В связи с этим нами предлагается рассмотреть возможность разработки Инструкции, содержащей правила и процедуру изъятия и фиксации цифровых доказательств и следов в ходе следственных действий, куда можно было бы включить следующие положения:

- указание на обязательность участия специалиста при осуществлении подобных операций с цифровыми следами. Данное положение обусловлено тем, что специфика работы с цифровыми следами предполагает знание всех особенностей техники изъятия, фиксации и переноса таких объектов, поскольку даже одно неосторожное действие может привести к утрате части свойств следа либо его полному уничтожению. В подтверждение этому можно привести следующую точку зрения: «Ключевым этапом в выстраивании стратегии доказывания фактов на основе цифровых следов являются их поиск и сохранение способами, обеспечивающими относимость, допустимость и полноту доказательств. Цифровые следы порождаются самыми разными процессами. Они могут представлять собой сетевые временные файлы с расширениями html, текстовые документы txt, docx, журналы системы, почтовые архивы и т. д. Их можно умышленно или неумышленно скрыть, уничтожить, изменить, зашифровать. Поиск цифровых следов необходимо проводить при содействии специалиста с профильным образованием и опытом»[123].

На это также обращают внимание В.А. Попов и А.А. Рудавин, отмечая: «Специалист, входящий в состав следственно-оперативной группы, решает более узкие задачи, связанные с использованием технико-криминалистических средств. В качестве примера обратимся к такой распространенной на практике ситуации, когда изъять тот или иной носитель информации не представляется возможным

---

[123] Особенности криминалистической фиксации цифровых доказательств и следов // Официальный сайт «Закон.ру». URL: https://zakon.ru/blog/2022/08/09/osobennosti_kriminalisticheskoj_fiksacii_cifrovyh_dokazatelstv_i_sledov / (дата обращения: 12.01.2025).

ввиду объективных причин. В подобной ситуации специалисту, участвующему в следственном действии, рекомендуется подготовить соответствующий образ файловой системы»[124].

О.Б. Дронова указывает на недостаток в сформировавшейся практике привлечения специалиста субъектами назначения экспертизы, который заключается в следующем: «Нивелирование и пренебрежение сотрудниками следственных подразделений возможностью постоянной координации с профильным сотрудником ЭКП при изучении криминалистически значимой информации, планировании хода расследования, оценки имеющейся материально фиксированных данных создает предпосылки для усложнения хода расследования, затягивания установленных законом сроков, утраты значимых сведений. Даже если расследование конкретного преступления в сфере информационно-коммуникационных технологий не предусматривает необходимость формирования специализированной следственной группы следователю при установлении ключевых обстоятельств совершения противоправного деяния целесообразно вести прямой диалог со специалистом отдела компьютерных экспертиз»[125].

На практике также возможно клонирование (посекторное копирование) информации с ее носителя. Основное отличие будет заключаться в том, что в специализированном оборудовании предусмотрена функция аппаратной блокировки, а также автоматизирован процесс определения аутентичности имеющейся и создаваемой информации. В случае использования иных средств создания посекторной копии или образа носителя информации, специалисту необходимо обеспечить запрет записи на носитель, с которого осуществляется получение данных и возможность осуществления контроля аутентичности

---

[124] Попов, В. А., Рудавин, А. А. Современные особенности технико-криминалистического обеспечения практики работы с цифровыми следами преступлений / В. А. Попов, А. А. Рудавин // в сб.: Технико-криминалистическое обеспечение раскрытия и расследования преступлений. Сб. науч.тр. всеросс. научн.-практ. конф., проводимая в рамках деловой программы Международной выставки средств обеспечения безопасности государства «Интерполитех-2022». — 2022. С. 182.
[125] Дронова, О. Б., Кочкин А. В. Доэкспертная оценка вещественных доказательств как средство оптимизации назначения и производства компьютерных экспертиз / О. Б. Дронова, А. В. Кочкин // Судебная экспертиза. — 2025. — № 1. — С.23.

имеющейся и создаваемой информации. Контроль аутентичности имеющейся и создаваемой информации можно осуществлять путем расчета хеш-функций (контрольных значений). В протоколе должны быть отражены способы создания и контрольные значения»[126];

- обязательное указание всех важных характеристик изъятого цифрового следа, включая его размер, разрешение, а также хеш-сумму;

- установить точный момент для подсчета хеш-суммы. Подсчет хеш-суммы копируемого и фиксируемого цифрового следа должен осуществляться исключительно в момент его первоначального обнаружения. Желательно, чтобы обнаружение и копирование файла выполнялись одномоментно в целях избегания образования временного провала между тем, когда след был обнаружен, и тем, когда он фактически был скопирован на носитель, поскольку на исследование эксперт получит именно последний вариант файла. Таким образом, следователь совместно со специалистом обнаруживает цифровой след, который необходимо извлечь для последующего исследования, фиксирует его хеш-сумму, далее переносит копию на нужный носитель. В таком случае хеш-сумма будет оставаться одинаковой, условие достоверности будет соблюдено. Та же самая хеш-сумма будет указана и в постановлении о назначении судебной экспертизы.

В ходе анкетирования нами была выявлена еще одна проблема у следователей, связанная с затруднениями при осуществлении подсчета хеш-суммы: 85,2% опрошенных отметили, что хотели бы получить инструкцию по осуществлению подсчета хеш-суммы.

Данная проблема может быть решена следующим образом:

---

[126] Попов, В. А., Рудавин, А. А. Современные особенности технико-криминалистического обеспечения практики работы с цифровыми следами преступлений / В. А. Попов, А. А. Рудавин // в сб.: Технико-криминалистическое обеспечение раскрытия и расследования преступлений. Сб. науч.тр. всеросс. научн.-практ. конф., проводимая в рамках деловой программы Международной выставки средств обеспечения безопасности государства «Интерполитех-2022». — 2022. С. 184.

- привлекаемый специалист обладает достаточным уровнем знаний в рамках своей компетенции, поэтому подсчет хеш-суммы не будет вызывать никаких затруднений;

- совместно со специалистами в области компьютерно-технической экспертизы может быть разработана инструкция по подсчету хеш-суммы. На сегодняшний день существует перечень надежных и апробированных алгоритмов, например, SHA-1, CRC32, SHA-2 и SHA-256. Более того, в некоторые операционные системы компьютеров уже включена функция автоматического подсчета данного показателя, например, в Windows 10 с помощью встроенной утилиты certutil с параметром -hashfile.

Безусловно, наше предложение нуждается в обсуждении перед внедрением его в практику. Стоит учитывать возможность появления трудностей при составлении таких рекомендаций, поэтому разрабатываться они должны совместно при участии специалистов и сотрудников различных ведомств. Чем больше ведомств будет принимать участие, тем легче будет такие рекомендации внедрить в повседневную практику. Таким образом, мы считаем разработку Правил изъятия и фиксации цифровых следов в ходе следственных и оперативно-розыскных действий необходимым шагом к минимизации допущения ошибок следователями и экспертами.

Отчасти указанные положения содержатся в ГОСТ Р ИСО/МЭК 27037-2014 Национальный стандарт Российской Федерации «Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме». Данный стандарт составлен по примеру международного стандарта ISO/IEC 27037:2012 «Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence». Он содержит в себе правила и рекомендации по идентификации, сбору, получению и

сохранению потенциальных свидетельств, представленных в цифровой форме[127]. Сфера применения стандарта следующая: он предназначен для предоставления руководства лицам, отвечающим за идентификацию, сбор, получение и сохранение потенциальных свидетельств, представленных в цифровой форме. Можно сказать, что данный стандарт вполне мог бы использоваться руководителями различных ведомств и их сотрудниками, однако, как мы уже отмечали, ГОСТ носит лишь рекомендательный характер. В любом случае, полное игнорирование положений, содержащихся в указанном стандарте, может повлечь за собой множество ошибок со стороны следователей и затруднить процесс исследования для экспертов.

В связи с этим, можно полагать, что самым действенным вариантом будет закрепление подобных положений на государственном уровне. Размышляя глобально, формирование единой следственной и экспертной практики при работе с цифровыми следами служит цели качественного обеспечения процесса судопроизводства и отправления правосудия. Нам представляется весьма актуальной идея Ю.В. Гаврилина о создании государственной научно-технической политики в области криминалистического обеспечения правоохранительной деятельности. Так, автор размышляет о том, что создание такой политики не менее важно, чем реализация единой уголовной политики государства как деятельности по обеспечению безопасности общества от криминальных посягательств, основанной на использовании уголовно-правовых, процессуальных, уголовно-исполнительных и других средств. Автор также отмечает следующее: «Очевидно, что криминалистическое обеспечение вносит значительный вклад в правоохранительную деятельность, содействуя борьбе с преступностью. Приведенные положения позволяют констатировать наличие оснований для формирования государственной научно-технической политики в области криминалистического обеспечения правоохранительной деятельности, или,

[127] ГОСТ Р ИСО/МЭК 27037-2014 «Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме». — Москва : Стандартинформ, 2014. — 47 с.

другими словами, криминалистической политики, содержание которой является неотъемлемым элементом единой государственной политики, отражающей систему идей и взглядов стратегического характера в сфере борьбы с преступностью (уголовной политики)»[128].

В качестве объекта такой политики выступает криминалистическое обеспечение выявления, раскрытия и расследования преступлений. Не будем забывать, что судебная экспертология выделилась в свое время из теории криминалистики. Более того, судебно-экспертная деятельность наряду с криминалистическим обеспечением способствует раскрытию и расследованию преступлений, а также отправлению правосудия. Полагаем, что положения о работе с цифровыми следами должны войти в состав указанной научно-технической политики.

Об этом также упоминает Ю.В. Гаврилин: «Цифровая трансформация механизма большинства преступлений требует совершенствования технических средств, предназначенных для обнаружения, фиксации и изъятия орудий, следов преступления, других вещественных доказательств в различных средах. В свою очередь, развитие средств криминалистической техники, их усложнение и расширение функциональных возможностей требует разработки рекомендаций по практическому ее использованию, включая криминалистические технологии решения конкретных тактических и экспертных задач, возникающих в процессе расследования отдельных видов преступлений. Кадровый компонент включает в себя особенности подготовки высококвалифицированных специалистов, обладающих компетенциями в области криминалистики и уголовного процесса, имеющих представление о современных возможностях криминалистического обеспечения и перспективах его развития»[129].

---

[128] Гаврилин, Ю. В. О понятии и содержании государственной научно-технической политики в области криминалистического обеспечения правоохранительной деятельности / Ю. В. Гаврилин // Труды Академии управления МВД России. — 2022. — №2 (62). С. 97.
[129] Там же. С. 100.

Наконец, следует признать, что сами по себе знания, оформленные в качестве рекомендаций, не способны в полной мере оказывать влияние на процесс судопроизводства, практику работы следователей, прокуроров. Для того, чтобы эти положения начали действовать, они должны быть доведены до правоприменителей, постоянно обновляться, а также быть реально применимыми с учетом существующих правовых и ресурсных ограничений.

Подытожим вышесказанное: для того чтобы рекомендации по работе с цифровыми следами начали действовать на практике, они должны быть утверждены на межведомственном и государственном уровнях. С учетом этого предлагается внести предложение о формировании Правил изъятия и фиксации цифровых следов в ходе следственных и оперативно-розыскных действий и предоставить это на решение Правительственной комиссии о координации судебно-экспертной деятельности в Российской Федерации (далее – Комиссия).

Согласно Постановлению Правительства РФ от 08.12.2018 № 1502 (ред. от 17.07.2019) «О Правительственной комиссии по координации судебно-экспертной деятельности в Российской Федерации» деятельность указанной комиссии направлена на формирование единой государственной политики и совершенствования законодательства Российской Федерации в сфере судебно-экспертной деятельности[130]. В пункте 4 Положения о Комиссии прописана следующая функция: комиссия координирует деятельность заинтересованных органов, а также межведомственных комиссий (советов, рабочих групп) в области судебно-экспертной деятельности. Также согласно пункту 8 в состав Комиссии с правом совещательного голоса могут включаться:

---

[130] О Правительственной комиссии по координации судебно-экспертной деятельности в Российской Федерации» (вместе с «Положением о Правительственной комиссии по координации судебно-экспертной деятельности в Российской Федерации») : Постановление Правительства РФ № 1502 : Утв. постановлением Правительства РФ 8 декабря 2018 г.: послед. ред. 17.07.2019 г. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_313162/7a2c590847c9cbfad23ff1b746f51a027d8e47e9/ (дата обращения: 13.02.2025).

а) руководители (заместители руководителей) иных государственных органов;

б) руководители (заместители руководителей) структурных подразделений заинтересованных органов государственной власти и учреждений, подведомственных указанным органам[131].

Поскольку данная Комиссия действует в интересах судебно-экспертной деятельности и направлена на ее совершенствование, а также с учетом того, что в состав Комиссии могут входить и представители органов государственной власти, полагаем, что решение о повышении качества деятельности следователей при работе с цифровыми объектами может входить в область интересов Комиссии. Также не стоить забывать, что следственные ошибки тесно связаны со следственными, таким образом, нам кажется вполне разумным поручить вопрос о внедрении Правил по работе следователей с цифровыми объектами данной Комиссии.

В соответствии с Распоряжением Правительства Российской Федерации от 20.07.2019 г. № 1618-р (ред. от 10.10.2024 № 2804-р) в состав Комиссии входят следующие представители ведомств:

- Министр юстиции Российской Федерации;
- Заместитель Министра внутренних дел Российской Федерации;
- руководитель Научно-технической службы ФСБ России;
- заместитель Министра обороны Российской Федерации;
- заместитель руководителя Федеральной таможенной службы;

---

[131] О Правительственной комиссии по координации судебно-экспертной деятельности в Российской Федерации» (вместе с «Положением о Правительственной комиссии по координации судебно-экспертной деятельности в Российской Федерации») : Постановление Правительства РФ № 1502 : Утв. постановлением Правительства РФ 8 декабря 2018 г.: послед. ред. 17.07.2019 г. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_313162/7a2c590847c9cbfad23ff1b746f51a027d8e47e9/ (дата обращения: 13.02.2025).

- заместитель Председателя Следственного комитета Российской Федерации и др.[132]

Как мы видим, среди задействованных лиц есть представители основных ведомств, регулирующих деятельность следователей в том числе, что подтверждает возможность рассмотрения предложенных нами положений. Наиболее действенным вариантом будет обсуждение и принятие таких положений самими представителями ведомств для того, чтобы избежать разногласий и достичь максимального единства в практической составляющей. В результате такого мероприятия может быть разработан Межведомственный приказ, утверждающий «Правила изъятия и фиксации цифровых следов в ходе следственных и оперативно-розыскных действий», которая впоследствии будет адаптирована под следователей.

Нами предлагается проект Правил изъятия и фиксации цифровых следов в ходе следственных и оперативно-розыскных действий[133]. Среди положений, выносимых на обсуждение, будет обращено внимание на необходимость расчета хеш-суммы, привлечения специалиста при изъятии и фиксации цифровых следов, соблюдения правил при осмотре и обыске и др.

Осуществить данную идеи можно следующим образом: Комиссия в лице представителей основных ведомств, регулирующих деятельность следователей, разрабатывает предложение о внедрении Правил изъятия и фиксации цифровых следов в ходе следственных и оперативно-розыскных действий. Далее это предложение направляется в ведомства, которые разрабатывают приказ о его принятии и внедрении.

Возможен и другой вариант: ведомства согласованно могут каждый для себя разработать и принять приказ, регламентирующий деятельность следователей по

---

[132] Об утверждении состава Правительственной комиссии по координации судебно-экспертной деятельности в Российской Федерации : Распоряжение Правительства РФ № 1618-р : принято Правительством РФ 20 июля 2019 г. // Официальное опубликование правовых актов : сайт. URL: http://publication.pravo.gov.ru/document/0001201907230021 (дата обращения: 13.02.2025).

[133] Проект Правил представлен в Приложении № 7.

работе с цифровыми следами. Например, по образу Приказа Министерства юстиции РФ от 28 декабря 2023 г. № 404 «Об утверждении Инструкции по организации производства судебных экспертиз в федеральных бюджетных судебно-экспертных учреждениях Министерства юстиции Российской Федерации».

Как верно указывает Е.Р. Россинская, типичной экспертной ошибкой процессуального характера является отсутствие в заключении подробного описания объектов, представленных на экспертизу[134]. Следовательно, со стороны судебных экспертов ошибка может проявляться в следующем:

- эксперт получил сведения о хеш-сумме, но не провел самостоятельный расчет показателя, в силу чего нельзя говорить со стопроцентной уверенностью о том, что эксперт исследует ровно то, что ему прислали на экспертизу;

- эксперт не получил никаких сведений о хеш-сумме цифрового следа, находящегося на носителе, однако, он не сделал об этом никакой пометки в ходе своего исследования.

Безусловно, контроль за тем, чтобы обеспечить неприкосновенность цифрового следа лежит на лице, назначающем судебную экспертизу, но не стоит забывать об обязанности эксперта перед началом исследования полностью осмотреть полученные на экспертизу объекты и полноценно их описать.

Тем не менее, подсчет хеш-суммы является не единственной мерой отслеживания изменений в цифровом следе. Например, существует довольно надежная и распространенная технология блокчейна.

Блокчейн (англ. «blockchain», «block» - блок, «chein» - цепь) – это распределенная база данных, состоящая из «цепочки блоков», устройства хранения блоков не подключены к общему серверу, база данных позволяет контролировать достоверность транзакций без надзора каких-либо финансовых регуляторов. Проверкой транзакций занимаются так называемые майнеры – участники системы,

---

[134] Россинская, Е. Р. Судебная экспертиза: типичные ошибки: 2-е издание, монография / под. ред. Россинской Е.Р. — М.: Проспект, 2024. С. 512.

которые подтверждают подлинность совершенных действий, а затем формируют из записей транзакций блоки. Реестр хранится одновременно у всех участников системы и автоматически обновляется при малейшем изменении. Каждый имеет доступ к информации о любой транзакции, когда-либо осуществленной. Пользователи выступают в качестве коллективного нотариуса, который подтверждает истинность информации в базе данных[135]. Разработка криптовалюты (биткоин) программистом Сатоши Накамото в 2009 г. положила начало развитию блокчейн-технологии (БТ)[136]. В технологии блокчейна также упоминается и хеширование: «Неизменность связей между блоками обеспечивается за счет того, что каждый последующий блок при хешировании своих данных использует данные предыдущего блока, например, их хеш. Наиболее частой причиной такого является то, что одному хешу соответствует бесконечное множество входных данных»[137].

Блокчейн, как надежный, достоверный и прозрачный способ защиты, представляется наиболее подходящим использовать в отношении объектов экономических экспертиз – криптовалют и т.д. Такая точка зрения была выражена и экспертами в ходе нашего анкетирования. На вопрос «Считаете ли Вы создание блокчейна хорошим способом защиты содержания цифрового следа от изменений?» 54,29% опрошенных ответили утвердительно. Эксперты отмечают, что создание блокчейна – это хороший способ защиты содержания цифрового следа от изменений.

Однако у применения такой технологии есть и ряд недостатков, среди которых эксперты выделили следующие:

- для большинства цифровых следов использование блокчейна часто избыточно из-за высокой сложности реализации, значительных затрат на

---

[135] Федотова, В. В., Емельянов, Б. Г., Типнер, Л. М. Понятие блокчейн и возможности его использования / В. В. Федотова, Б. Г. Емельянов, Л. М. Типнер // European science. — 2018. — №1 (33). С. 46.

[136] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system // Bitcoin.org. URL: https://bitcoin.org/bitcoin.pdf (дата обращения: 01.01.2025).

[137] Балдов, Д. В., Петрова, С. Ю., Лебедев, А. А. Использование технологии блокчейн для защиты данных / Д. В. Балдов, С. Ю. Петрова, А. А. Лебедев // International Journal of Open Information Technologies. — 2021. — № 9. С. 28.

вычисления и хранения, а также отсутствия необходимости в распределенной инфраструктуре в условиях, где стандартные механизмы проверки целостности (хеширование, цифровые подписи) способны обеспечить адекватную защиту;

- требует создания соответствующей системы, для создания частного блокчейна требуется также ответственное лицо.

Многие эксперты сходятся во мнении о том, что на данном этапе развития технологий при наличии иных способов отслеживания изменений применение блокчейнов попросту излишне. В рамках судопроизводства, с учетом огромного массива цифровых следов, использование блокчейна будет финансово затруднительным. Тем не менее использование технологии блокчейна весьма перспективно для экономических экспертиз, хотя ее применение на этом не ограничивается.

Также при работе с цифровыми доказательствами предлагается обращаться к «цепи законных владений». В частности, о такой технологии известно следующее: «Соблюдение «цепи законных владений» обеспечивает достоверность доказательства, указывающего на его внутреннюю доброкачественность через формальную сторону, что и отличает это свойство от допустимости. Судами не берется во внимание «цепь законных владений» которая подразумевает, что доказательство, в частности аудио-, видеозапись для приобретения ей такового статуса должна иметь как реквизиты, так и законный путь вовлечения в материалы уголовного дела указывающий на ее подлинность и позволяющий проверить достоверность и неизменность записанной информации. Зачастую доказательства описываются без соблюдения рекомендаций как при изъятии и осмотрах, так и в дальнейшем экспертом. В случае небрежного описания мобильных устройств, дисков и иных носителей информации правоприменители зачастую рассчитывают, что допущенные ошибки будут признаны судом техническими. Наиболее типичные цепочки передачи: направление результатов ОРД от сотрудников, проводивших ОРМ к лицу, ведущему расследование; передача изъятых предметов от лица, ведущего расследование, к эксперту. Ошибки допускаются и их можно

найти, проверяя описание упаковки, количества, фасовки в протоколах изъятия (осмотра, обыска), акте первоначального исследования, постановлении о назначении экспертизы, заключении экспертизы»[138].

Отметим, что помимо описания самого цифрового файла обращается внимание и на важность правильного описания упаковки с объектом-носителем. Это подводит нас к выделению следующей процессуальной ошибки при работе уже с цифровыми объектами, которыми, как мы определили, являются цифровой след и объект-носитель. Речь идет об ошибках упаковки цифровых объектов и ее грамотного описания.

Обеспечить отслеживание изменений в цифровом следе – важно, однако, не стоит забывать, что цифровой объект мы рассматриваем в совокупности с материальным носителем (флеш-накопителем, диском и т.д.), и для его защиты нужно предпринимать такие же меры по упаковке и описанию, как и для стандартного объекта.

Уже сегодня можно обнаружить ошибки, допускаемые экспертами в связи с неполноценным описанием упаковки цифрового объекта. Последствия таких ошибок негативны, они могут привести к решению о признании заключения эксперта недопустимым доказательством. Приведем пример из судебной практики. В рамках апелляционного представления государственного обвинителя А.Н. Бурыкина на приговор Кунцевского районного суда г. Москвы от 14 июня 2019 года были предъявлены следующие требования. В апелляционных жалобах осужденный К.А.В., выражая несогласие с состоявшимся судебным решением, считает его незаконным и необоснованным, а выводы, изложенные в нем, составленными на недопустимых доказательствах, поскольку:

- «описание изъятого мобильного телефона отличается в ряде процессуальных документов, в частности, в протоколе личного досмотра вообще не указаны какие-либо отличительные особенности данного телефона, в протоколе

[138] Ушаков, О. М. Процедура доказывания и «цепь законного владения» / О. М. Ушаков // Право и государство: теория и практика. — 2021. — №12 (204). С. 272.

осмотра предметов, он указан, как телефон черного и желтого цвета с повреждением экрана, в сопроводительном письме, как телефон черного цвета, а в постановлении о приобщении к материалам дела вещественных доказательств, указан лишь имей телефона. Указанные разночтения, по мнению автора жалоб, не позволяют сделать вывод, что в материалах дела фигурирует один и тот же, изъятый у него мобильный телефон. Кроме того, в постановлении о назначении экспертизы указано, что на экспертизу представлен конверт с обозначением № 1, в котором находится сверток из полимерного материала с веществом, в то время, как эксперт в описательной части ссылается лишь на пакет из бумаги белого цвета, не ссылаясь на обозначение № 1, при этом, эксперт никак не индивидуализирует поступившие ему конверты, описывая их одинаково в каждой из 4-х экспертиз. При таких обстоятельствах полагает, что невозможно установить, что конкретно поступило на экспертизу, и что исследовалось при ее производстве»[139]. По результату разбирательства апелляционная жалоба была удовлетворена.

Для того, чтобы требования по полноценному описанию упаковки цифрового объекта, поступившего на экспертное исследование, были выполнены, эксперт должен:

- полностью описать, во что упакован объект, цвет, форму, размеры и габариты самой упаковки, подписи/иные рукописные/печатные записи/обозначения при наличии, целостность упаковки, если она была вскрыта – указать, как и где именно;

- если объект не упакован, обязательно отметить это в своем заключении.

Помимо неполного или неграмотного описания объекта-носителя или упаковки цифрового объекта, экспертные ошибки могут возникать и как следствие необеспечения надежной упаковки как таковой. На практике привести в негодность носитель цифровой информации относительно несложно: случайно прогнуть или

---

[139] Апелляционное определение Московского городского Суда от 28.10.2019 по делу № 10-16047/2019 г. [Электронный ресурс]. — Доступ из справ.-правовой системы «КонсультантПлюс».

сломать пополам CD-диск, вовсе заменить флеш-карту или сам диск на другой с целью фальсификации доказательств, если упаковка это позволяет. Е.С. Лапин пишет: «Если в ходе следственного действия имело место копирование данных с изымаемого электронного носителя информации, то существенным нарушением требований ч. 3 ст. 164.1 УПК РФ станет отсутствие в качестве приложения к протоколу следственного действия самого электронного носителя информации, на который были скопированы данные, в пригодной, опечатанной и подписанной понятыми и следователем (дознавателем) упаковке. Важно, чтобы изъятый носитель информации и содержащиеся на нем цифровые следы как вещественное доказательство сохранялись при материалах уголовного дела без какой-либо порчи или утраты вследствие воздействия окружающей среды»[140].

К сожалению, лицом, назначающим экспертизу, не всегда обращается должное внимание на упаковку, например, CD или DVD дисков, содержащих аудио- или видеозапись, как цифровой файл. Например, в рамках апелляционного определения на приговор Мещанского районного суда г. Москвы от 2 мая 2017 года защитниками осужденных было заявлено требование признать представленные для фоноскопического исследования DVD-диски с аудиофайлами недопустимыми доказательствами на основании следующего:

- «значимая для исхода дела аудиозапись с диктофона Олимпус была перенесена Ф. на СД-диск, суду представлен DVD-диск, который не совпадает ни по серийному номеру, указанному в акте, ни по техническим характеристикам. Упаковка другого DVD-диска также была отличной от ранее заявленной»[141]. В результате рассмотрения апелляционной жалобы требования были удовлетворены, а дело направлено на новое судебное рассмотрение.

Кроме очевидного упущения следователя, эксперты также нередко не уделяют внимания отсутствию должной упаковки, дабы избежать лишней

---

[140] Лапин, Е. С. Вопросы, возникающие при работе с цифровыми следами в ходе расследования преступлений / Е. С. Лапин // Правовая политика и правовая жизнь. — 2021. — №2. С. 177.

[141] Апелляционное определение Московского городского Суда от 29.11.2017 по делу № 10-15114\17. [Электронный ресурс]. — Доступ из справ.-правовой системы «КонсультантПлюс».

волокиты и затягивания самого процесса экспертного исследования. Между тем, ненадлежащая упаковка может привести:

- к утере материального носителя, флеш-накопителя, диска;

- поломке диска;

- целенаправленной подмены объекта-носителя на иной, схожий по внешним характеристикам и т.д.

Существует несколько способов обеспечения надежной упаковки цифрового объекта. Например, в качестве обеспечения минимальной защиты от несанкционированного вскрытия можно запечатывать цифровые объекты в так называемые невскрываемые конверты. По сути, их, конечно, можно вскрыть, иначе как бы эксперт смог извлечь содержимое такого конверта, однако при их использовании факт вскрытия непременно будет известен. Это могут быть, например, конверты серии «Security», которые предназначены для максимальной защиты вложения от перлюстрации и несанкционированного доступа. Для этого под клапаном конверта нанесены специальные просечки, по которым бумага рвется при попытке вскрытия клапана. Запечатка со специальным рисунком – защитная просечка или пин-запечатка, которая обеспечивает улучшенную защиту содержимого конверта от чтения на просвет[142].

Помимо конвертов цифровые объекты можно направлять на экспертизу в сейф-пакетах. Сейф-пакеты – это вид упаковки, которая герметично закрывается и предназначена для отправки и транспортировки ценных грузов, денежных средств, документов. На клапане пакета нанесена специальная защитная полоса. Е.В. Меланич, говоря о сейф-пакетах, как средстве защиты особых ценностей и документов, пишет следующее: «В настоящее время средством идентификации и контроля доступа могут быть сигнальные устройства в виде наклеек, которые используются в таможенном деле для идентификации документов, а также сейф-

[142] Конверт С4 (229х324мм) Security с защитными просечками, стрип. URL: https://www.kanctanta.ru/catalog/9249/41311/ (дата обращения: 25.01.2025).

пакеты (пластиковые пакеты), применяемые в таможенном деле для идентификации документов и в банковском деле — для перевозки наличности»[143].

Сейф-пакет отличается тем, что обладает несколькими ступенями защиты:

- специальная надпись – Stop/Void, Вскрыто. Даже если заново заклеить пакет, она не исчезнет. При попытке заморозить клей и вскрыть упаковку – надпись не исчезнет;

- покрытие, которое при воздействии химических растворителей изменяет цвет;

- нижний край пакета специально делается бесшовным. Это позволяет избежать несанкционированного вскрытия;

- боковые швы имеют двойную сварку. Это позволяет защитить пакет от вскрытия путем подрезания швов;

- края пакета имеют рельеф, который исключает попытку вскрытия упаковки путем разрезания.

- каждый пакет имеет индивидуальный номер и штрихкод. Это исключает подмену пакета. Уникальный номер дублируется также на внутренней стороне клапана пакета. Даже если удалить номер на внешней стороне, он останется на внутреннем клапане[144]. Такой номер сейф-пакета следователь или суд могут указать в постановлении о назначении экспертизы при описании упаковки.

Наконец, не менее надежным способом защиты является наличие подписи/грифа следователя/суда, а также печати учреждения. Помещать такие подписи или печати целесообразно на местах, потенциально подходящих для вскрытия конверта, пакета, бумажного конверта и т.д. То есть не будет надежным проставить печать или разместить подпись на лицевой поверхности конверта, которая при вскрытии может остаться нетронутой, лучше делать это на боковых, верхних и нижних краях.

---

[143] Меланич, Е.В. Печати: семь тысяч лет. Профилактика правонарушений : Издание 1-е / Е.В. Меланич. — Москва, 2021. С. 50.

[144] Сейф-пакет – что это такое и где применяется. URL: https://em-pack.ru/sejf-paket-chto-eto-takoe-i-gde-primenyaetsya/ (дата обращения: 17.02.2025).

Кроме указания всех характеристик цифрового файла, описания упаковки цифрового объекта и обеспечения защиты упаковки необходимо уделять внимание и самому объекту-носителю, ведь перед тем, как запечатать цифровой объект в упаковку, цифровой файл на носителе, допустим, диске, его можно подменить. Для этого существуют неизменяемые носители, например, CD-R (Compact Disc Recordable) диски. Они представляют собой одноразовые CD-диски без возможности перезаписи. Информация на них записывается один раз и навсегда. Любая попытка перезаписи приведет к повреждению диска и потере данных.

Следственная ошибка может быть допущена при копировании цифрового файла на материальный носитель неизвестной природы, например, если следователь принес на место происшествия личный флеш-накопитель.

Иные следственные ошибки могут допускаться на любом этапе осмотра средств вычислительной техники. Данное мероприятие состоит из следующих действий:

- внешний осмотр компьютерной техники;

- проверка наличия активных сетевых подключений;

- осмотр компьютерной информации (установленных и использующихся приложений, файловой системы, запущенных процессов);

- снятие копии (дампа) содержимого оперативной памяти;

- выключение компьютера и создание копии жесткого диска;

- отсоединение кабелей и внешних устройств (в случае изъятия взаимосвязанных объектов необходимо промаркировать имеющиеся кабельные соединения);

- составление протокола и упаковка изъятого[145].

О необходимости участия специалиста было сказано ранее, помимо того, что специалист может помочь следователю зафиксировать и изъять цифровой след

---

[145] Россинская Е.Р., Семикаленова А.И., Рядовский И.А., Сааков Т.А. Теории информационно-компьютерного обеспечения криминалистической деятельности : монография / под. ред. заслуженного деятеля науки РФ, доктора юридических наук, профессора Е.Р. Россинской. — М.: Проспект, 2022. С. 92.

правильно, его участие исключает возможность уничтожения самого цифрового следа. Особенно часто это происходит в том случае, если ~~одиноко~~ стоящий компьютер включен и его система активна. Следователь может не знать о том, что выключение компьютера без создания копии диска может стереть находящиеся на нем сведения. Например, на некоторых персональных компьютерах диспетчер учетных данных теряет учетные данные после выхода из системы или перезагрузки компьютера. В таком случае по ошибке следователя цифровой след, содержащий потенциально значимую криминалистическую информацию, может быть бесповоротно утерян.

Ошибкой следователя при осмотре и обыске включенного компьютера будет также следующее:

- следователь создал копию жесткого диска, скопировал находящуюся на нем информацию, но не проверил наличие активных сетевых подключений;

- следователь произвел неполноценный осмотр компьютерной информации (установленных и использующихся приложений, файловой системы, запущенных процессов). В данном случае речь идет о фиксации дерева/каталога программ, что по природе является как процессуальной, так и операционной ошибкой.

Еще одна следственная ошибка связана с неполным отражением действий специалиста в протоколе осмотра места происшествия, поскольку следователь должен зафиксировать не только сам ход действия и полученные результаты, но и указать наименование примененных специалистом технических и программных средств. Кроме того, помимо обыска и изъятия, специалист в отдельных случаях для полного сбора сведений может произвести исследование работающей компьютерной системы.

Достаточность компетентности привлекаемого к осмотру и обыску цифровых устройств специалиста должна особо тщательно проверяться следователем. При недостаточной внимательности к наличию у специалиста

необходимых компетенций есть риск упустить важные информационные объекты или не сохранить надлежащим образом цифровые следы[146].

Помимо непосредственного изучения цифрового устройства и изъятия цифрового следа следователь вместе со специалистом должен учитывать важность осмотра внешней обстановки места происшествия. Например, исходный код вредоносной программы может быть обнаружен в распечатанном либо даже рукописном виде, как и записи, подтверждающие неправомерный доступ к компьютерным системам, пароли к заблокированным компьютерным устройствам, реквизиты доступа к облачным сервисам, схемы сетевой инфраструктуры, используемой при совершении преступлений и т.п.[147]

По результатам проведенного нами анкетирования эксперты предлагают использовать следующие профилактические меры для устранения как следственных, так и экспертных ошибок при работе с цифровыми следами и объектами:

- в рамках экономических экспертиз возможно использование специального программного обеспечения 1С, функции которого позволяют блокировать внесение изменений. Если эксперту представляется электронный документ, он должен быть защищен криптографией, подписан УКЭП (усиленной квалифицированной электронной подписью). Если представляется база данных, то в нее должны быть вшиты логи обо всех операциях, произведенных с этой базой данных, которые не могут быть изменены, а если изменяются, то база данных должна становится недоступной (битой);

- осуществление доступа к цифровому следу по цифровому ключу;

---

[146] Россинская Е.Р., Семикаленова А.И., Рядовский И.А., Сааков Т.А. Теории информационно-компьютерного обеспечения криминалистической деятельности : монография / под. ред. заслуженного деятеля науки РФ, доктора юридических наук, профессора Е.Р. Россинской. — М.: Проспект, 2022. С. 96.

[147] Аверьянова Т. В., Белкин Р. С., Корухов Ю. Г., Россинская Е. Р. Криминалистика. Учебник для вузов. Изд. 4, переработанное и доп. / Т.В. Аверьянова, Р.С. Белкин, Ю.Г. Корухов, Е.Р. Россинская — М.: Норма; ИНФРА-М, 2013. С. 912.

- использование технологии «USB Data Blocker» и иных блокираторов. Запрет на осуществление любых манипуляций с носителями без средств блокирования записи;

- для объектов автороведческих и лингвистических экспертиз возможно нотариальное заверение содержания сайта/переписки/скриншота перед выведением на печать и переносом на бумажный носитель;

- применение электронных подписей (ЭЦП);

- обязательно использовать фото/видеотехнику с возможностью и включенной функцией записи метаданных создаваемых фото/видео файла;

- фиксация в заключении эксперта метаданных файла, размера и сравнение их с данными, приведенными в постановлении о назначении экспертизы (формат, размер, использованная техника, хеш-сумма и т.д.).

Таким образом, описанные выше проблемы при работе с цифровыми следами – объектами судебных экспертиз – позволили нам проложить вектор развития следственных и экспертных ошибок, которые, как показывает судебная практика, могут привести к отмене судебного решения, построенного на основании судебной экспертизы, выполненной с нарушением процессуальных норм.

Обнаружение экспертных ошибок и осуществление профилактических мер – два основных направления, в рамках которых возможно добиться минимизации процессуальных ошибок экспертов.

Экспертные ошибки могут быть обнаружены следующими способами:

1) при проверке самим экспертом хода и результатов проведенного им исследования;

2) при анализе и обсуждении результатов экспертного исследования, осуществляемого комиссией экспертов при производстве комиссионной и комплексной экспертиз;

3) при анализе экспертом или специалистом заключений предшествующих экспертиз – в данном случае если эксперт обнаруживает ошибку в заключении предшествующей экспертизы, то он принимает все возможные меры для

недопущения подобной ошибки в своем исследовании и учитывает ее при объяснении различий между своими и предыдущими выводами;

4) при контроле хода и результатов экспертного исследования руководителем экспертного учреждения;

5) следователем, присутствующим при производстве экспертизы: если ошибка замечена следователем, присутствующим при производстве экспертизы, то он немедленно ставит об этом в известность эксперта (однако стоит сказать, что на практике подобные случаи практически не встречаются);

6) при оценке заключения эксперта следователем или судом (первой, апелляционной, кассационной, надзорной инстанций) – если ошибка не влияет на выводы эксперта, она может быть нейтрализована или устранена путем допроса эксперта или назначения дополнительной экспертизы. В противном случае может быть назначена повторная экспертиза (такое обнаружение экспертных ошибок встречается значительно чаще);

7) в процессе обобщения экспертной практики, осуществляемом в практических или научных целях – по поводу этого пункта точки зрения ученых несколько разнятся. Например, И.О. Перепечина пишет следующее: «Следует признать, что объективно оценить положение, связанное с качеством судебной экспертизы в отечественной практике, в настоящее время не представляется возможным. В отличие от зарубежной литературы, в которой проблема ошибок при производстве экспертиз исследована весьма обстоятельно и широко обсуждается на страницах печати, в отечественной литературе этой теме посвящено весьма незначительное число публикаций; проверки экспертной деятельности носят сугубо внутриведомственный характер, практика внешнего аудита отсутствует»[148]. Привлечение адвокатами специалистов для оценки экспертных заключений хоть и

[148] Перепечина, И. О. Экспертные ошибки в контексте профессиональной деятельности экспертов / И. О. Перепечина // Вестник Московского университета МВД России. — 2015. — №3. С. 35.

осуществляется, однако зачастую полученные рецензии игнорируются судом/следователем и не приобщаются к материалам уголовного дела.

Описанное сделало сферу экспертной деятельности закрытой не только для общества в целом, но и для специалистов. Таким образом, «истинное положение дел в экспертной сфере – реальная квалификация экспертов, уровень ошибок в целом и в том или ином экспертном подразделении и т.д. – неизвестно»[149]. Однако в современной научной литературе, например, монографии «Судебная экспертиза: типичные ошибки» (2024) под ред. Е.Р. Россинской уже приведен довольно широкий перечень вопросов, требующих внимания ученых и экспертов, и создающих условия для экспертных ошибок. Необходимо учитывать моменты, свидетельствующие о недостаточной подготовке экспертов: необоснованность выводов по причине ошибок в расчетах, выборе параметров и коэффициентов, использование устаревших методик, коэффициентов и формул, неверный выбор схемы или методики исследования, несоблюдение ее требований, неприменение рекомендованной методики, неполнота исследования, халатное отношение к своим обязанностям.

Профилактические меры по предотвращению экспертных ошибок также можно условно разделить на несколько групп:

1) меры, предпринимаемые экспертными учреждениями: совершенствование методического и технологического обеспечения экспертизы, создание надежной системы контроля за результатами исследования, разработка эффективной системы подготовки экспертных кадров и контроля их квалификации. Одной из наиболее значимых мер профилактики также является внутреннее рецензирование экспертными учреждениями[150]. Об этом пишет О.Г. Дьяконова, в частности, отмечая рецензирование как одну из функций руководителя экспертного учреждения: «Приказ МВД России от 29.06.2005 № 511 (ред. от 12.11.2024)

[149] Там же. С. 37.
[150] Дьяконова, О. Г. Организация профессионального сообщества судебных экспертов на основе судебной экспертологии / О. Г. Дьяконова // Судебная экспертиза. — 2023. — № 1 (73). С. 13.

предусматривает возможность со стороны руководителя организовывать выборочное письменное рецензирование заключений экспертов. Контрольная функция руководителя охватывает как судебно-экспертную деятельность организации в целом, так и действия по контролю проведения конкретных экспертиз»[151]. Суть внутреннего рецензирования отмечается в следующем: «Судебно-экспертные организации (СЭО) проверяют качество подготовленных экспертами заключений. Такое рецензирование осуществляется в рамках системы контроля за качеством экспертиз и выражается в проверке компетентными субъектами выбранной экспертом методики, ее научной обоснованности, полноты, всесторонности и логики проведенного исследования, что можно оценить положительно»[152];

2) меры со стороны субъектов доказывания: тщательная оценка результатов исследования и экспертных выводов. В грамотно составленном заключении эксперта должны присутствовать все необходимые реквизиты (дата, время и место производства судебной экспертизы; основания производства судебной экспертизы; вопросы, объекты и т.д.), выводы эксперта должны вытекать из проведенного исследования и подтверждаться им, примененные методы и методики не должны вызывать сомнений, все объекты должны быть всесторонне исследованы, а ответы эксперта должны быть исчерпывающими и не содержать двусмысленных трактовок и т.д. Также сюда входит активное привлечение специалистов, а при необходимости – назначение повторных экспертиз;

3) меры со стороны профессионального экспертного сообщества: создание независимых комиссий, наделенных правомочиями систематически проводить внешний аудит деятельности экспертных лабораторий с целью проверки

---

[151] \Дьяконова, О. Г., Иванова, Е. В. О некоторых функциях руководителя судебно-экспертной организации, связанных с назначением и проведением судебной экспертизы / О. Г. Дьяконова, Е. В. Иванова // Известия Тульского ГУ. Экономические и юридические науки. — 2022. — Вып.2. С. 29.

[152] Дьяконова, О. Г. Рецензия специалиста на заключение судебной экспертизы и консультация специалиста: понятие, сущность, нормативное регулирование / О. Г. Дьяконова // Журнал российского права. — 2023. — Том 27. №4. С. 91.

экспертных заключений, а также соответствия квалификации персонала установленным требованиям, которые должны быть жестко регламентированы.

Мы поддерживаем предложение, сформулированное Ф.Г. Аминевым относительно создания специализированной палаты для создания подобных комиссий: «В целях повышения уровня профессиональной подготовки необходимо создание единой вневедомственной Высшей федеральной квалификационной комиссии судебных экспертов с филиалами в территориальных округах Российской Федерации. В состав органа по подготовке и проведению квалификационных экзаменов, наряду с представителями государственных судебно-экспертных организаций и наиболее известных судебных экспертов, обязательно участие профессорско-преподавательского состава вузов, осуществляющих подготовку по специальности «Судебная экспертиза» и т.д.[153].

Перечисленные меры профилактики экспертных ошибок могут применяться в рамках исследования всех видов объектов судебных экспертиз. Что касается профилактики экспертных ошибок при работе с объектами в цифровой форме, можно сказать однозначно, что устранение таких ошибок, так же, как и всех остальных, требуется рассматривать комплексно. Например, если ошибка связана с описанием объекта, то здесь должны соблюдаться меры описания и со стороны следователя, и со стороны эксперта; если ошибка кроется в неправильной упаковке и ее описании, профилактические меры также должны соблюдаться обеими сторонами. Таким образом, устранение ошибок – это всегда результат совместных усилий, некоторые из рекомендаций были предложены нами выше.

Следующей немаловажной проблемой, требующей серьезного рассмотрения в контексте появления новых цифровых объектов, является вопрос компетенции судебного эксперта. Для начала стоит сказать, что фактически цифровые следы уже являются объектом судебно-экспертного исследования на протяжении двух

---

[153] Аминев, Ф. Г. О проблемах судебно-экспертной деятельности в Российской Федерации и путях их решения / Ф. Г. Аминев // Пробелы в российском законодательстве. Юридический журнал. — 2017. — № 3. С. 390.

последних десятилетий. Исследуются они, в основном, в рамках компьютерно-технических экспертиз, хотя могут встречаться и в других видах (фоноскопической, портретной и т.д.). Соответственно, исследование всех характеристик и свойств таких объектов, само собой разумеется, осуществляется экспертом в области компьютерной техники и технологий и по большому счету не требует наличия каких-либо дополнительных знаний.

Согласно позиции А.И. Усова, основу судебных компьютерно-технических экспертиз составляют следующие виды: «судебная аппаратно-компьютерная экспертиза; исследование технических (аппаратных) средств компьютерной системы; судебная программно-компьютерная экспертиза; исследование программного обеспечения; судебная информационно-компьютерная экспертиза (данных); судебная компьютерно-сетевая экспертиза, которая основывается на функциональном предназначении компьютерных средств, реализующих какую-либо сетевую информационную технологию»[154].

Однако, как показывает практика, цифровые следы уже вышли за рамки исследования только компьютерно-технической экспертизы. Подменяя традиционные формы объектов, они стали исследоваться в рамках и речеведческих, экономических, традиционных криминалистических экспертиз и других. Следовательно, ситуация здесь меняется на абсолютно противоположную, ведь не всегда эксперт, обладая, допустим, компетенцией в области судебной экономической экспертизы, способен самостоятельно провести исследование цифрового объекта, не упустив из виду важных деталей и не навредив самому объекту по собственному незнанию.

В условиях цифровизации с изменением объектов заметно меняется и компетенция судебных экспертов. Судебные эксперты, исследующие цифровые следы, должны обладать навыками использования современных компьютерных технологий. Многие виды экспертиз уже требуют от эксперта наличия

---

[154] Усов, А. И. Концептуальные основы судебной компьютерно- технической экспертизы : дис. ... докт. юрид. наук : 12.00.09 / Александр Иванович. — М., 2002. С. 127.

определенных навыков в области IT-технологий из-за своей специфики. Это касается, например, фоноскопической, видеотехнической и фототехнической экспертиз, а также решения некоторых задач в портретной экспертизе.

Все это не могло не повлечь за собой негативные последствия в виде теоретических, правовых и организационных проблем. Представляется важным разобраться, в каких случаях эксперт способен произвести исследование цифрового объекта, не выходя за пределы своей основной компетенции, а в каких случаях его действия будут нарушением процессуальной нормы.

Для начала возьмем на рассмотрение уже описанный нами момент, когда эксперту нужно рассчитать хеш-сумму полученного файла для сверки с хеш-суммой, указанной в постановлении о назначении экспертизы. Если исходить из самого определения компетенции, то она состоит из определенного комплекса специальных знаний. В свою очередь, противоположностью специальных знаний являются общеизвестные, доступные большому массиву лиц без необходимости приобретать их посредством дополнительного образования и т.д. Входит ли в область специальных знаний подсчет хеш-суммы файла? На наш взгляд, не входит, что объясняется следующим.

Как мы уже отмечали, на сегодняшний день расчет хеш-суммы файла уже внедряется в операционные системы компьютеров, становясь частью базовых настроек. Отчасти способность вычислить данную характеристику можно приравнивать к владению стандартным пакетом офисных программ, например, пакета Microsoft. В наше время владение офисными программами даже на продвинутом уровне – требование, которое предъявляется к перечню навыков большого количества работников, сотрудников, педагогов и т.д. Можно говорить о том, что для современного человека умение пользоваться базовыми функциями компьютерных систем – само собой разумеющееся. Следовательно, для того, чтобы посчитать хеш-сумму цифрового файла, наличие дополнительной квалификации не требуется. Более того, мы уже говорили, что этим должны заниматься и следователи при назначении экспертизы, что еще раз доказывает исключение

расчета хеш-суммы из области специальных знаний в области компьютерно-технической экспертизы.

Таким образом, если при работе с цифровым объектом эксперт помимо решения задач, входящих в его основную компетенцию, рассчитывает хеш-сумму файла, за рамки своей компетенции он не выходит, следовательно, процессуальные нормы не нарушает[155]. В рамках анкетирования для выяснения мнения экспертов по данному поводу мы также задали вопрос «Как Вы считаете, необходима ли эксперту дополнительная квалификация (помимо основной) в области судебной компьютерно-технической экспертизы для работы с цифровыми следами? Укажите, в каких случаях». Примечательно, что вопрос касался всех аспектов работы с цифровыми следами, однако частью экспертов самостоятельно был оговорен данный момент, некоторые из них сошлись с нами в мнении о том, что исключительно для подсчета хеш-суммы наличие дополнительных знаний не требуется.

Выше мы осветили вопрос о необходимости применения дополнительных специальных лишь на этапе описательной части, однако реальные проблемы возникают при непосредственном исследовании новых объектов, а также при их изъятии самим экспертом. Во многих родах судебных экспертиз на первоначальной стадии экспертного исследования судебный эксперт выявляет следы, обнаружение которых невозможно без использования специальных (инструментальных) методов. Отметим, что в целом при исследовании цифровых объектов возможно развитие двух вариантов:

1) либо цифровой объект с уже изъятым цифровым следом поступает на исследование на отдельных носителях, например, на жестком магнитном диске, флеш-накопителе и т.д.;

---

[155] Шихалиева С.З. Отсутствие хэш-суммы как процессуальная ошибка, возникающая в судебной экспертизе при исследовании объектов в цифровой форме / С. З. Шихалиева // Правовое государство: теория и практика. — 2025. — №1 (79). С. 261.

2) либо пока еще цифровой след находится в компьютерных системах, на серверах, соответственно, перед тем, чтобы приступить к непосредственному исследованию, эксперт первым делом должен этот след изъять. Рассмотрим такое развитие событий подробнее.

Все больше случаев, когда объектом экспертного исследования выступает цифровой след, который существует исключительно в компьютерной среде, создан в ней, использован для осуществления определенной операции именно в ней, и для того, чтобы такой след изъять в привычной для восприятия экспертом форме, компетенции самого эксперта может быть недостаточно. Возьмем в качестве примера судебные экономические экспертизы. С учетом цифровой трансформации исследование объектов данного рода экспертиз представляется слабо возможным без использования знаний в области IT-технологий. Так, в рамках судебной финансово-экономической экспертизы сформировался новый вид судебных экономических экспертиз — судебная экспертиза операций с цифровыми финансовыми активами.

В.В. Блажеев отмечает следующее: «Операции с цифровыми финансовыми активами осуществляются исключительно в сети Интернет и носят транснациональный характер. Специфика экспертных исследований здесь такова, что для проведения исследования эксперт должен обладать не только экономическими знаниями, но и знаниями в области IT-технологий. При этом в судебной экспертизе операций с криптоактивами все объекты представляют собой цифровые следы»[156].

Как отмечает Д.О. Буйнов, «одной из наиболее широко распространенных систем автоматизированного бухгалтерского учета в России является система «1С: Предприятие». В процессе пользования данной системы для ведения бухгалтерского либо налогового учета создается база данных в виде файла

[156] Блажеев, В. В., Алтухов, А. В., Андреев, Л. В. Право и общество в эпоху социально-экономических преобразований XXI века: опыт России, ЕС, США и Китая: коллективная монография / Под общей редакцией профессора В. В. Блажеева и профессора М. А. Егоровой — М.: Проспект, 2021. С. 208-221.

1Cv8.CD. В данном файле могут храниться различные данные информационной системы, например, конфигурация, база данных и т.д. Посредством исследования данных файлов и содержащихся в них баз данных возможно получить информацию о различных операциях, сформировать бухгалтерские регистры либо бухгалтерскую отчетность, что позволяет установить интересующие следствие факты»[157]. С учетом всей специфики и сложной структуры данной системы и хранящихся в ней цифровых следов, самостоятельно эксперт в области экономической экспертизы извлечь правильно и без потерь такой объект пока не может. На наш взгляд, в таких случаях необходимо привлечение специалиста.

Объекты подобной природы могут быть изъяты специалистом напрямую либо скопированы так, чтобы у эксперта был полноценный образ системы. В первом случае привлечение специалиста нужно потому, что эксперт-экономист не всегда способен самостоятельно получить бухгалтерские документы и отчетности, хранящиеся в базах данных (например, в случае некорректной работы файла либо носителя компьютерной информации).

Д.О. Буйнов в этой связи говорит: «Одним из способов копирования цифровых следов является создание образа операционной системы. Данный прием позволяет осуществить полное копирование не только самой операционной системы, но и всех настроек, файлов, программ, конфигураций и т.д. Создав образ, специалист в области IT-технологий дает возможность анализировать документы бухгалтерского и налогового учета и отчетности, не подвергая риску сам носитель информации и содержащиеся на данном носителе цифровые следы»[158].

Таким образом, если задача привлечения специалиста заключается лишь в том, чтобы грамотно изъять цифровой след оттуда, откуда это не может сделать сам эксперт, такое процессуальное решение абсолютно оправдано. При таком

---

[157] Буйнов, Д. О. Назначение комплексных судебных экспертиз при исследовании цифровых следов в расследовании экономических преступлений / Д. О. Буйнов // Полицейская деятельность. — 2022. — №4. С. 21.

[158] Буйнов, Д. О. Назначение комплексных судебных экспертиз при исследовании цифровых следов в расследовании экономических преступлений / Д. О. Буйнов // Полицейская деятельность. — 2022. — №4. С. 25.

раскладе эксперт снимает с себя ответственность за нарушение процессуальных норм производства экспертизы, более того, он также ограждает себя от ответственности за возможную порчу цифрового следа или приведение его к негодности.

По-другому обстоят дела в том случае, если в компетенцию эксперта входит работа с цифровыми следами изначально и изъять цифровой след он может самостоятельно. Известно, что объектами таких экспертиз, как фоноскопическая и видеотехническая, преимущественно являются цифровые следы – аудио- или видеофайлы. Например, на фоноскопическую экспертизу цифровые следы направляются на отдельных носителях. Использование IT-технологий является неотъемлемой частью экспертной методики, а эксперт-фоноскопист обладает в соответствии со своей специализацией необходимыми компетенциями, поскольку он получил высшее образование по специальности «судебная экспертиза», специализация «судебные речеведческие экспертизы», либо прошел профессиональную переподготовку. В таких экспертизах используется комплексная методика экспертного исследования и, соответственно, комплекс различных компетенций, но это наблюдается далеко не во всех родах (видах) судебных экспертиз.

Таким образом, при решении вопроса о том, выходит ли эксперт за пределы своей компетенции при необходимости изъятия цифрового следа, если это является частью экспертного исследования, необходимо исходить из того, входит ли изучение подобных следов в принципе в его компетенцию, а также где именно располагается требуемый цифровой след. Если изъятие цифрового следа находится за пределами компетенции эксперта, целесообразно привлечение специалиста в этих целях.

Возможен и другой подход, когда сначала проводится технико-криминалистическая экспертиза цифрового следа, а затем полученный цифровой объект направляется на исследование эксперту другой области. Например, по делу о крупном мошенничестве необходимо было провести судебную строительно-

техническую экспертизу, сами документы — цифровые следы — находились в сети строительной организации. Сначала необходимо было провести судебную компьютерно-техническую экспертизу для выявления файлов, содержащих эти документы, преодоления действия специальных программ защиты файлов путем их быстрого уничтожения, установления времени создания и происхождения этих файлов, а затем уже по полученным расшифрованным документам производилась судебная строительно-техническая экспертиза.

По-другому обстоят дела в том случае, если перед экспертом ставится задача не исследовать непосредственно характеристики самого объекта, аудиозаписи, провести анализ отчетных документов, а решить вопрос о факте видоизменения/фальсификации программы, в которой цифровой след находился, или установить факт наличия признаков, указывающих на видоизменение цифрового следа. В таком случае, например, если мы говорим об эксперте-экономисте, в его компетенцию не входит решение данных задач.

Д.О. Буйнов описывает процедуру исследования подобных цифровых следов следующим образом: «Сначала они должны быть исследованы экспертом в области судебной компьютерно-технической экспертизы для легитимного получения цифровых следов, например, установить, имеется ли на данном компьютере система «1С-бухгалтерия», является ли она лицензионной, получены ли массивы бухгалтерской информации с помощью этой версии программы или привнесены в компьютер как-то иначе и пр., а затем, скопированы на внешний носитель или представлены в бумажном варианте для производства судебно-бухгалтерской экспертизы. В противном случае эксперт судебно-бухгалтерской экспертизы, даже если он владеет необходимыми технологиями, не имеет права ими воспользоваться, поскольку это находится вне пределов его компетенции»[159].

[159] Буйнов, Д. О. Назначение комплексных судебных экспертиз при исследовании цифровых следов в расследовании экономических преступлений / Д. О. Буйнов // Полицейская деятельность. — 2022. — №4. С. 26.

Т.А. Сааков, рассуждая о вопросах компетенции эксперта при исследовании цифровых следов, говорит: «Также возможны случаи, когда выход за пределы своей компетенции при работе с цифровыми следами будет в принципе маловероятен. Например, такое может встречаться в рамках автороведческих экспертиз блогов и других материалов социальных сетей для решения идентификационных задач (отождествления автора) или диагностических задач, связанных с личностными характеристиками автора»[160].

А.И. Семикаленова также пишет: «Возможность решения поставленных задач в рамках комплексной экспертизы также не стоит исключать, однако, это необходимо устанавливать для каждого случая отдельно. Примером комплексной судебной экспертизы является судебная компьютерно-техническая и судебная товароведческая экспертизы при решении задачи установления стоимости работ по созданию и внедрению программного продукта с точки зрения формирования его потребительских характеристик, потребительских свойств и потребительской стоимости»[161].

В ряде случаев участие специалиста по обнаружению, изъятию и обеспечению сохранности цифровых следов может быть обусловлено тем, что при выявлении таких объектов необходимы не только специальные знания в области IT-технологий, но и другие специальные знания, связанные со спецификой программного обеспечения. Например, при изъятии и последующем исследовании с удаленного сервера данных о финансовых операциях, осуществляемых с помощью специальных программ, разработанных для банковской сферы, необходимо совместное участие экспертов в области судебных компьютерно-технической и финансово-экономической экспертиз, поскольку судебный

---

[160] Сааков, Т. А. Письменные речевые следы, оставленные в цифровой среде, как источник значимой информации о личности неизвестного / Т. А. Сааков // Законы России: опыт, анализ, практика. — 2021. — № 3. С. 57.

[161] Семикаленова, А. И. Проблемы определения потребительской стоимости программного продукта / А. И. Семикаленова // Теория и практика судебной экспертизы. — 2018. — Том 13. № 4. С. 131.

компьютерно-технический эксперт может затрудниться с выбором цифровых следов, не зная специфики финансовых операций.

Следует подчеркнуть, что при любой ситуации при исследовании объектов, являющихся цифровыми следами, судебный эксперт должен представлять себе технологии изъятия криминалистически значимой информации в виде определенных цифровых следов, уметь оценивать легитимность, пригодность и достаточность этих объектов для проведения судебной экспертизы и получения обоснованного вывода.

Резюмируя вышеизложенное, стоит признать, что вопрос выхода за пределы компетенции при работе с цифровыми объектами на данный момент не решен даже приблизительно, новых объектов очень много, каждый из них уникален, и как с ними грамотно работать – все еще неясно. Возьмем, например, цифровые объекты почерковедческих экспертиз. Некоторые исследователи, например, В.Э. Яскина, П.И. Лакеев и Л.М. Круглов выделяют два вида таких объектов: «На основании вышеизложенного полагаем, что способы получения рукописей, поступающих на экспертизу в электронном виде, можно подразделить на оцифровывание и рукописный ввод. Так, под оцифровыванием подразумевается получение цифровой копии (сканирование, фотографирование) с рукописи, выполненной преимущественно при помощи традиционных материалов и инструментов письма. А рукописный ввод предполагает выполнение рукописи с помощью программно-технических средств (инструментов рукописного ввода) непосредственно в электронном документе»[162]. В связи со спецификой подписей, выполненных указанными способами, авторы выделяют необходимость более основательной теоретической и методической разработки проблемных аспектов по следующим вопросам: «В связи с этим у специалистов возникают следующие вопросы:

[162] Яскина, В. Э., Лакеев, П. И., Круглов, Л. М. О некоторых вопросах исследования почерковых объектов, представленных на экспертизу в электронном виде / В. Э. Яскина, П. И. Лакеев, Л. М. Круглов // Теория и практика судебной экспертизы. — 2023. — Т. 18. № 2. С. 56.

– Насколько простым для обычного пользователя ПК является комплекс действий, направленных на установление факта применения устройств рукописного ввода, оригинальности представленного файла?

– Возможно ли проведение почерковедческого исследования без применения специальных знаний в области компьютерно-технической экспертизы?

– Не выходят ли данные действия за пределы компетенции эксперта-почерковеда?»[163].

Несмотря на большое количество спорных моментов, одно можно утверждать точно – привлечение специалиста в области компьютерно-технических экспертиз позволит снизить процент допускаемых ошибок как минимум вдвое. А.И. Семикаленова, рассуждая на данную тему, приводит лишь небольшой перечень экспертных ошибок, совершаемых экспертами из-за отсутствия необходимых компетенций. Так, она пишет следующее: «Просматривая экспертную практику назначения судебной компьютерно-технической экспертизы мы увидели большие пробелы у экспертов, чаще всего у частных экспертов, в наборе компетенций»[164].

Обратим внимание, что она рассматривает только ошибки экспертов в области СКТЭ, не говоря о том, какие еще ошибки могут быть допущены экспертами в других областях, в то время как перечисленные ею объекты могут вполне исследоваться в рамках той же судебной бухгалтерской экспертизы. Это наталкивает на логичный вывод о том, что даже для экспертов по СКТЭ цифровые объекты – «непаханое поле», поэтому эксперты других областей в одиночку с такими объектами справиться пока просто не в состоянии.

Автор также не зря делает акцент на необходимости регулирования вопроса компетенций среди частных экспертов, и действительно, не стоит забывать, что сегодня практически половина всех экспертных исследований выполняется

---

[163] Там же. С. 59.

[164] Семикаленова, А. И. Судебная компьютерно-техническая экспертиза: проблемы компетенций экспертов / А. И. Семикаленова // Вестник криминалистики. — 2020. — № 2 (74). С. 71.

негосударственными экспертами. В качестве возможных способов решения данной проблемы предлагается следующее: «В первую очередь необходимо принять нормативные акты, регулирующие деятельность частных экспертов, создать орган или систему контроля наличия компетенций у экспертов СКТЭ, разделить возможности решения экспертом задач в зависимости от наличествующих у него компетенций, создать единый реестр экспертов, позволяющий субъектам, участвующим в назначении экспертизы, получать максимально полную информацию об эксперте»[165].

Каким образом можно преодолеть препятствия, возникающие в рамках компетенции эксперта не из области судебной компьютерно-технической экспертизы? На наш взгляд, уже сейчас имеет смысл вводить в систему базового экспертного образования курсы или дисциплины по теории цифровизации судебно-экспертной деятельности, возможно, разработать и изучать методические правила работы с цифровыми следами, поскольку в будущем такие знания будут необходимы для экспертов любых областей.

В рамках анкетирования был поставлен соответствующий вопрос следователям и экспертам. На вопрос «Как Вы считаете, необходима ли эксперту дополнительная квалификация (помимо основной) в области судебной компьютерно-технической экспертизы для работы с цифровыми следами? Укажите, в каких случаях» следователи ответили следующим образом: 66,7% считают это необходимым, оставшиеся 33,3% не видят в этом особой нужды. Практически так же сложилась картина среди экспертов: 64,29% экспертов видят смысл в дополнительном повышении квалификации, 35,71% не видят в этом смысла. Те, кто на данный вопрос ответил отрицательно, ссылаются на то, что вопрос компетенции решается назначением комплексной экспертизы. Однако, как мы установили ранее, назначение именно комплексной экспертизы не всегда оправдано, в большинстве случаев вопрос решается привлечением специалиста, который восполняет отсутствующие у эксперта знания в области IT-технологий.

---

[165] Там же. С. 73.

Также эксперты, ответившие утвердительно, отмечают, что повышение квалификации необходимо в целом и для того, чтобы понимать более четко сущность цифровых следов, механизм их образования, значимые характеристики, да и в принципе повышение квалификации для эксперта должно организовываться непрерывно, в течение всего срока экспертной деятельности, так как информационные объекты и способы противоправного применения информационных технологий постоянно и быстро эволюционируют. Некоторые эксперты обуславливают необходимость владения дополнительными компетенциями и тем, что в случае, например, допроса в суде, эксперт должен дать квалифицированные ответы на вопросы о том, как именно он осуществлял работу с цифровым объектом: при помощи каких инструментов осуществлял изъятие цифрового следа и т.д.

58,5% экспертов выбрали повышение квалификации в качестве приоритетного способа приобретения необходимых знаний по работе с цифровыми объектами, однако, с оговоркой на то, что повышение квалификации возможно только в том случае, если такие знания были даны экспертам в рамках базового образования. Как отмечалось ранее, мы считаем такую точку зрения правильной, потому нами и предлагается первостепенно обеспечить специализированные курсы и дисциплины по работе с цифровыми следами в рамках направления обучения «40.05.03. Судебная экспертиза».

Таким образом, можно сказать, что обнаружение и профилактика экспертных ошибок играют очень важную роль для судебной экспертизы и экспертного сообщества в целом. Как и в любой другой сфере, предотвращение ошибок возможно только путем их тщательного разбора и поиска новых путей осуществления конкретной деятельности и устранения всех предпосылок совершения таких ошибок снова. Значимость профилактики экспертных и следственных ошибок обусловлена и тем, что на сегодняшний день заключение эксперта активно используется в качестве одного из доказательств по делу. Поэтому крайне важно сделать так, чтобы такое заключение отвечало критериям

достоверности, обоснованности и объективности. Также стоит отметить комплексный характер ответственности лиц, участвующих в процессе выявления и профилактики экспертных ошибок. Как было указано ранее, в этом участвует не только эксперт, участники процесса, в том числе следователь и суд, но и экспертное сообщество. Поэтому деятельность по профилактике субъективных и объективных экспертных ошибок должна осуществляться систематически и иметь комплексный характер.

Подводя итоги, можно с уверенностью сказать, что на данном этапе развития судебной экспертологии и частной теории цифровизации судебно-экспертной деятельности неразрешенных вопросов все еще много. Эксперты в совокупности с правоприменителями должны уделять как никогда много внимания каждому этапу производства судебной экспертизы: на этапе изъятия, если это является частью судебной экспертизы, здраво оценивать свои возможности по осуществлению изъятия цифрового следа, на этапе описания объекта не упускать ни одной качественной или количественной характеристики, на этапе решения экспертных задач опираться на собственные специальные знания и допускать возможность их нехватки.

Что касается профилактических мероприятий для предотвращения ошибок со стороны следователей, то нами предлагается рассмотреть следующее предложение. С учетом того, что многие ошибки допускаются из-за недостаточного уровня знаний в какой-либо области, в том числе в отношении цифровых следов, представляется необходимым ликвидировать пробелы и непонимания природы и особенностей цифровых следов, что может быть реализовано в рамках специальной рабочей программы, внедренной в учебный план следователей.

Кафедрой судебных экспертиз Московского государственного юридического университета имени О.Е. Кутафина (МГЮА) в рамках Проекта по реализации Стратегии института прокуратуры была разработана рабочая программа дисциплины Б1.В.ДВ.02 «Использование специальных знаний при расследовании

преступлений и судебном рассмотрении дел в цифровой среде». Данная рабочая программа была разработана для обучения прокуроров, принята в рамках указанной Стратегии и утверждена Ученым советом Университета имени О.Е. Кутафина 27 января 2024 года. Составителями рабочей программы являются Е.Р. Россинская и Н.С. Неретина.

Рабочая программа была разработана в целях приобретения практических навыков об использовании специальных знаний при расследовании преступлений в цифровой среде, формирование компетенций в области использования современных IT-технологий в производстве судебных экспертиз, понимание основных категорий и положений цифровизации судебно-экспертной деятельности, основных представлений о цифровых следах, их материальной сущности, технологической природе, механизме формирования. Как мы видим, многое из перечисленного подходит и для следователей, в связи с чем мы предлагаем модифицировать и персонифицировать программу для следователей, однако, расширив ее путем включения еще нескольких разделов, касающихся ошибок, правил проведения следственных действий и т.д.

Опираясь на вышеуказанную рабочую программу, мы разработали макет программы для следователей, основные разделы которой приведены в Приложении № 5.

Следует отметить, что в некоторых образовательных учреждениях, выпускающих следователей, стали добавлять в список дисциплин курсы, частично излагающие обучающимся положения теории цифровизации. Например, за кафедрой информационных технологий и организации расследования киберпреступлений Московской Академии Следственного Комитета закреплены следующие учебные дисциплины:

- Информатика и информационные технологии в профессиональной деятельности следователя;

- Информационно-компьютерное обеспечение следственной деятельности;

- Цифровые следы преступлений против личности;

- Расследование киберпреступлений.

Для будущих экспертов также предусмотрены следующие дисциплины: цифровые следы преступлений, компьютерно-технические экспертизы, расследование преступлений, совершенных с использованием информационных технологий, специальные знания при расследовании преступлений в сфере компьютерной информации.

Что касается профилактики экспертных ошибок, то здесь ситуация решается следующим образом. По мнению О.Г. Дьяконовой, подготовка судебного эксперта должна включать в себя следующее:

«а) знания в одной или нескольких областях специальных знаний;

б) знания в области судебной экспертологии, включая концептуальные основы судебной экспертологии, правовое и организационное обеспечение применения и использования специальных знаний в юрисдикционной деятельности, а также судебно-экспертные технологии;

в) знания в области цифровых технологий, в число которых входит не только владение компьютерно-техническими средствами и программным обеспечением, но и знания об изменяющейся природе объектов под влиянием цифровизации и о новых методах их исследования»[166].

В рамках подготовки по специальности 40.05.03 «Судебная экспертиза» уже внедрены базовые знания в области развития общей теории судебной экспертологии, а также частной теории цифровизации судебно-экспертной деятельности. Таким образом, будущие эксперты уже получают необходимые знания о цифровых следах, а для практикующих экспертов возможна организация повышения квалификации. Например, на кафедре судебных экспертиз МГЮА имени О.Е. Кутафина уже реализована программа повышения квалификации

[166] Дьяконова, О. Г. Специальные знания в судебной и иной юрисдикционной деятельности государств-членов ЕАЭС: теория и практика : дис.... д-ра юрид. наук : 12.00.12 / Дьяконова Оксана Геннадьевна. — М., 2021. С. 328.

«Цифровые следы как объекты судебных экспертиз»[167]. Полагаем, что подобные программы повышения квалификации могут быть реализованы и для экспертов различных ведомств. В содержательной части программ должны быть отражены ключевые положения о цифровых следах, цифровых объектах, видах материальных носителей, особенностей исследования цифровых объектов, видах ошибок, допускаемых при работе с ними, и т.д.

Таким образом, в рамках обобщения и анализа экспертной и следственной практики были спрогнозированы процессуальные ошибки, допускаемые как экспертами, так и следователями, а также предложены профилактические меры для их предотвращения.

2.2. Гносеологические и операционные ошибки судебных экспертиз объектов в цифровой форме

В судебно-экспертной деятельности цифровизация изменила не только привычные нам объекты экспертного исследования, но и повлияла на методы, применяемые экспертами для решения задач. Эксперты сейчас находятся в сложном положении, когда с одной стороны от них требуется соблюдение методологических приемов работы с объектами исследования, а с другой стороны качественные особенности цифровых объектов не позволяют ограничиваться уже привычным инструментарием. В результате складывается ситуация, где эксперт должен в сжатые сроки и в «полевых» условиях реагировать на трансформации объектов исследования и вооружаться теми инструментами и методами, которые бы отвечали уровню сложности цифровых объектов. В такой ситуации, к сожалению, очень легко оступиться и допустить ошибку, используя сомнительное программное обеспечение и неапробированный инструментарий.

---

[167] Кафедра судебных экспертиз // Официальный сайт Университета имени О.Е. Кутафина (МГЮА). URL: https://msal.ru/structure/kafedry-obshcheakademicheskie/kafedra-sudebnykh-ekspertiz/?ysclid=mahc6cisv0554799660 (дата обращения: 23.02.2025).

Предположим, эксперт на исследование получил новый цифровой объект, который ранее в практике ему не встречался. В данном случае, скорее всего, подходящей методики не оказывается, и эксперт исходит из принципа наибольшей схожести: исследование нового объекта производится на основании методики исследования подобного объекта. Такая практика отчасти объясняется тем, что методическое обеспечение судебно-экспертной деятельности не может поспевать за каждодневно изменяющимся технологическим прогрессом, ведь процесс принятия новой методики не быстрый. Практикующие эксперты в такой ситуации зачастую могут прибегать к использованию сторонних программ, методов, что чревато тем, что они неадекватно понимают работу аппаратного и программного обеспечения. В свою очередь, это приводит к неправильной интерпретации данных, полученных в результате работы программного обеспечения. Если учесть также тот фактор, что не верифицированные, малоизвестные среди экспертного общества программы обладают неизвестной долей погрешности, то выходные данные, извлекаемые экспертом после изучения объекта через какую-то программу, могут оказаться с вероятностью ошибочными.

Следовательно, эксперты могут в значительной степени полагаться на инструменты для обработки данных, не принимая во внимание ограничения и присущие им ошибки. Все это может приводить к последующей чрезмерной зависимости от подобных инструментов и программ. Эксперт, постепенно вводя в привычной обиход те или иные программы, привыкает к ним, начиная принимать полученные результаты за верные, поскольку практика еще не успевает проанализировать систему допускаемых им ошибок. Описанное также усугубляется высокодинамичной технической и операционной средой быстро развивающихся технологий и возросшей распространенностью цифровых технологий, используемых при осуществлении преступной деятельности. Рассмотрим данные положения на примерах.

Наиболее распространенной ошибкой среди экспертов является конвертирование, кадрирование, обрезка аудио- и видеодорожек в приложениях на

мобильных устройствах, а также посредством использования интернет-сайтов. Предположим, эксперту нужно изменить формат файла из pdf в jpg или из pdf в txt. Сразу оговоримся, что такое можно делать исключительно для облегчения выполнения каких-то текущих задач при исследовании, если эксперту на экспертизу направили файл формата «pdf», то и использовать в заключении он везде должен его. Допустим, файл содержит большое количество текста, цифровых записей, которые нужны эксперту для заполнения реквизита документов. Ситуация является более-менее приемлемой, если конвертация из одного формата в другой была произведена с помощью программ, входящих в пакет офисных «Microsoft» или, например, выпускаемых компанией «Adobe Systems» – это Adobe Acrobat, или ABBYY FineReader. Данные программы лицензированы, устанавливаются официально на многие операционные системы (Windows, macOS), сертифицированы. По-другому складывается ситуация в том случае, если для этих целей эксперт использует интернет-сайты, например, «ilovepdf.com». Данный сайт может за считанные секунды произвести конвертацию даже многостраничных документов, тогда как, например, в том же ABBYY FineReader этот процесс может растянуться на несколько минут. Однако, на этом преимущества использования подобных сайтов заканчиваются. Не стоит забывать, что все pdf-файлы можно условно разделить на два вида:

- созданные изначально в формате word, а затем конвертированные;
- являющиеся фактически сканом документа.

Если скан документа в формате pdf с текстовыми или цифровыми записями, рукописными подписями, рисунками и иными символами переформатировать через сторонний сайт, высока вероятность того, что программа в силу имеющихся погрешностей считает символы неверно. Данное положение легко проверить опытным путем – на выходе вместо текста получится просто набор символов, причем не обязательно на русском языке. При должной внимательности эксперт может заметить данную ошибку и быстро ее ликвидировать, однако, в потоке большого количества работы, документов, он может разместить такое изображение

в иллюстрационной таблице или же не глядя скопировать текст и вставить в описательную часть документа.

Аналогичная ситуация ожидает эксперта также в том случае, если он будет производить исследование и анализ аудио- или видеодорожки через сторонние сайты либо вовсе мобильные приложения. Известно, что современные мобильные устройства оснащены большим количеством различных приложений, которые значительно упрощают и ускоряют процесс обрезки и иной обработки аудио- и видеофайлов. За этими удобствами эксперт и рискует проглядеть те изменения, которые на первый взгляд неочевидно привнесет неизвестное приложение в исследуемый файл. Например, эксперт для своего удобства обрезает часть фонограммы, не имеющей моментов переговоров двух лиц, чьи голоса и слова он должен транскрибировать либо исследовать. Мобильное приложение либо сайт позволяют ему это сделать достаточно быстро, однако, например, в таком приложении может быть включена автоматическая подчистка дорожки от сторонних шумов, звукоизоляция, шумоподавление, изменение тональности и настройка чистоты голосов, что в свою очередь может привести к потере части значимых признаков.

Ситуация может усугубиться и тем, что эксперт не посчитает нужным отображать в ходе своего исследования осуществленные им не имеющие, на его взгляд, значения технические процедуры, поэтому условно к его заключению не будет никаких претензий. Однако само исследование будет построено на основании инструментальных методов и средств, не прошедших апробацию и искажающих сущностные характеристики цифрового следа. Таким образом, эксперт допускает сразу несколько ошибок, которые ко всему прочему будет очень сложно выявить.

Говоря об использовании мобильных приложений и мобильных устройств в целом, стоит сказать, что их использование как следователем, так и экспертом в принципе не должно рассматриваться, на что есть целый ряд веских причин. И.Н. Подволоцкий пишет: «Использование бытовых устройств в судопроизводстве –

сомнительное достижение. Во-первых, информация, записанная с помощью бытового мобильного устройства, теряет свою достоверность, так как первоначально фиксируемое событие или объект на месте происшествия обрабатывается встроенными в мобильное устройство «интеллектуальными помощниками» и в результате получается отображение объекта с измененными свойствами и характеристиками. Во-вторых, из-за неквалифицированных действий оператора в настройке фотосъемки, информация может быть изменена и стать недостоверной. В-третьих, есть вероятность умышленного искажения исходной видеозаписи или создания поддельной видеозаписи. Например, видеоредакторы на мобильных устройствах оснащены профессиональными инструментами, позволяющими оператору удалять фрагменты видеозаписи, вставлять изображения, изменять фон и т.д. По-видимому, эти и другие скрытые возможности мобильных устройств серьезно подрывают полноту и достоверность фиксируемой криминалистической информации и, следовательно, ее доказательную ценность»[168]. Мы полностью согласны с выдвинутыми опасениями.

К примеру, в качестве цифрового объекта в рамках судебной почерковедческой экспертизы нередко используются сканы или PDF-файлы документов, цифровые изображения подписей, рукописных записей. В рамках судебной портретной экспертизы цифровыми объектами выступают фотоизображения внешности человека. Поскольку природа объекта совершенствуется, меняется с традиционной на цифровую, правила работы с ними тоже требуют изменения. Рассмотрим особенности отбора объектов для назначения судебной портретной экспертизы.

Судебная портретная экспертиза является одним из наиболее традиционных видов криминалистических экспертиз. В рамках данной экспертизы решается задача установления личности по признакам внешности.

---

[168] Подволоцкий, И. Н. Использование цифровых технологий в деятельности экспертов / И. Н. Подволоцкий // Вестник криминалистики. — 2023. — № 4. С. 53.

Портретная экспертиза — это вид криминалистической экспертизы, проводимой в соответствии с положениями процессуального законодательства, в целях установления личности по признакам внешности, зафиксированным на различных объективных отображениях, и выполняемой с помощью специализированных методов исследования. Решаемые в рамках портретной экспертизы задачи могут носить как идентификационный (отождествление личности по изображениям), так и диагностический характер (установление расово-этнической принадлежности, возрастной группы, половой принадлежности и т.д.). Среди объектов, исследуемых экспертом при производстве экспертизы, выступает как внешность человека, так и ее различные отображения объективного и субъективного характера. При проведении криминалистической идентификации по признакам внешности в качестве отождествляемого объекта выступает личность человека. Идентификация производится с использованием различных отображений внешнего облика (фотоснимков, видеокадров и пр.). Эти отображения выступают в качестве отождествляющих объектов, носителей информации о признаках внешности[169].

К основным трудностям, связанным с отбором фотоснимков для портретной экспертизы, ученые относят низкое качество изображения, неподходящий ракурс, неправильный наклон головы, отсутствие необходимого освещения и т.д. В тех случаях, когда предоставленные в распоряжение эксперта изображения недостаточны или малоинформативны, следователь должен самостоятельно при возможности сделать фото- и видеоизображения с учетом всех требований. На данном этапе и допускается, на наш взгляд, одна из наиболее серьезных и злободневных следственных ошибок, приводящих к формированию экспертных.

Для проведения качественного исследования фотоизображение должно максимально качественно отображать все имеющиеся идентифицирующие и

---

[169] Акишин, Д. Г. Особенности подготовки и назначения судебной портретной экспертизы. URL: http://www.proexpertizu.ru/theory_and_practice/portret/713/?ysclid=lydeludx6k781410013 (дата обращения: 05.07.2024 г.).

диагностически значимые признаки внешности – шрамы, морщины, пигментные пятна, рубцы, родинки, родимые пятна, оттенок кожи, наличие румянца, кожных заболеваний (например, розацеи) и т.д. Современные технические средства позволяют запечатлеть все вышеуказанные особенности внешности с высокой точностью.

На сегодняшний день человечество перешло от традиционных фотоаппаратов и профессиональных видеокамер к более простому и удобному варианту – мобильному устройству. Мобильное устройство в силу своей компактности и простоты использования более предпочтителен для использования в повседневной жизни. Однако, как показывает практика, не только простые обыватели, но и следователи, дознаватели, судьи и иные лица, вовлеченные в процесс отправления правосудия, а также сам судебный эксперт зачастую предпочитают в качестве камеры использовать именно камеру мобильного устройства, предусматривающего возможность в считанные минуты сделать готовые фото- и видеоснимки, что представляется нам крайне сомнительным не только из-за недопустимости использовать камеры мобильных устройств вместо фотокамеры, но и из-за технических особенностей, кроющихся в настройках современных мобильных устройств.

Согласно данным из различных интернет-источников, а также основываясь на визуальном анализе основных характеристик, на сегодняшний день разрешение камеры мобильного устройства составляет диапазон от 12 до 108 мегапикселей, в ряде случаев – до 200 мегапикселей, разрешение современных фотоаппаратов зависит от физического размера матрицы. Например, полнокадровые матрицы встречаются с разрешением от 16 до 60 Мп, разрешение матриц среднего формата может достигать до 150-200 Мп. Может показаться, что, поскольку мегапиксели у камеры телефона и фотоаппарата примерно одинаковые, то и качество снимков будет одним и тем же, что объясняет выбор в пользу мобильных устройств. Однако это не совсем соответствует действительности.

Ключевой деталью любой камеры, от которой напрямую зависит разрешение и качество полученных фотографий, является матрица. Она есть и у современных мобильных устройств, и у фотокамер, но у последних она по техническим характеристикам больше, что и играет ключевую роль в качестве. Матрица смартфона в несколько раз меньше матрицы фотоаппарата, даже несмотря на разрешение. Иными словами, размер одного пикселя у фотоаппарата в десятки раз больше – а поскольку фотография основана на фиксации света, то и света такой сенсор получает тоже больше.

Вместе с тем, камеры современных мобильных устройств всё ещё способны фотографировать и снимать видео на достаточно хорошем уровне, но не стоит забывать, что с качеством снимков, сделанных на фотокамеру, никогда не сравнится.

Однако, наряду с возможностью делать высокодетализированные снимки, у современных мобильных устройств есть и противоположная функция – встроенная ретушь или «face retouch». Такая функция предусмотрена для того, чтобы мобильное устройство автоматически при создании фотокадра «сгладил» некоторые неровности и несовершенства внешности. Данная проблема активно изучается специалистами в области габитоскопии, учеными и экспертами. А.М. Зинин, размышляя об этом вопросе, пишет: «Однако необходимо иметь в виду, что современная практика применения программных средств для обработки изображений, в том числе полученных при фотографировании, позволяет с помощью как встроенных в съемочную аппаратуру микропроцессоров, имеющих целью улучшать качество изображения, так и с помощью компьютерных редакторов, изменять размерные характеристики, пропорции частей лица человека и т.п.»[170].

Полный перечень возможностей встроенного редактора варьируется от конкретной модели мобильного устройства, однако все они в определенной

[170] Зинин, А. М. Нейросети и судебно-портретная экспертиз / А. М. Зинин // Вестник криминалистики. — 2020. — № 2 (74). С. 67.

степени видоизменяют внешность человека. Например, проведенное мини-исследование обывателя интернета показало, насколько сильно функция ретуши («украшение», «преображение», название может также варьироваться в зависимости от модели мобильного устройства), меняет черты лица, «стирая» большое количество индивидуализирующих признаков. В своем аккаунте на форуме «Пикабу» он опубликовал несколько коллажей, содержащих по две фотографии одного и того же человека со встроенной ретушью и без нее, со следующим текстом: «Мы взяли портреты известных мужчин и сфотографировали их еще раз мобильное устройство «Huawei Honor 6 Plus» с включенной функцией «Украшение»[171]. Проведенное исследование показывает, что на изображениях с ретушью отсутствуют такие значимые для эксперта черты внешности, как морщины, складки, шрамы, рубцы, «синяки» под глазами и т.д., а сами фотографии обладают довольно низким качеством.

Серьезность проблемы также обусловлена тем, что количество моделей мобильных устройств, обладающих встроенной функцией «face retouch», довольно велико. По результатам запроса «Все мобильные устройства с функцией ретуши лиц на фото (face retouch) «sravnismart» выдал 2014 моделей мобильных устройств, среди которых мобильные устройства таких широкоиспользуемых марок, как «Iphone», «Samsung» и т.д.[172] Ситуация осложняется также тем, что несмотря на указание о наличии функции ретуши в мобильном устройстве, многие работники и специалисты по различным причинам не обращают на это должного внимания. Более того, зачастую функция ретуши заложена в заводские настройки мобильного устройства и включена по умолчанию, а для того, чтобы ее выключить, человек должен хотя бы озадачиться данным вопросом. Таким образом, качество снимков,

---

[171] Мы взяли портреты известных мужчин и сфотографировали их еще раз мобильное устройствоом Huawei Honor 6 Plus с включенной функцией «Украшение // Официальный сайт форума «Пикабу». URL: https://pikabu.ru/story/vstroennoy_funktsiey_retushi_v_smartfonakh_obyichno_polzuyutsya_devushki_interesno_kak_ona_rabotaet_na_sereznyikh_muzhchinakh_3423505#comments (дата обращения: 05.07.2024).

[172] Все мобильное устройства с функцией ретуши лиц на фото (face retouch) // Сайт «Сравни.ру». URL: https://sravnismart.ru/camera_extra_functions/face-retouch/ (дата обращения: 05.07.2024).

а также диагностически значимых и идентификационных признаков внешности заведомо будет искаженным, не позволяющим провести экспертное исследование на должном уровне.

Существует и другая погрешность, неминуемо допускаемая при фотографировании внешности лиц на мобильные устройства. Речь идет о фокусном расстоянии, напрямую влияющем на то, как именно на фото будут отображены пропорции лица. Данное суждение также подтверждается исследованием, проведенным пользователем платформы «AndroidInsider», посвященной статьям, обзорам, новостям, экспериментам и аналитике мобильных устройств на базе Android. Так, исследование показало, как внешность одного и того же человека может кардинально поменяться в зависимости от фокусного расстояния, на котором были сделаны фотоснимки. По результатам исследования был сделан следующий вывод: «Основная камера современных мобильных устройств имеет фокусное расстояние 24-28 мм. Если фотографировать на нее человека вблизи, то неминуемо будут искажены пропорции лица. А по мере увеличения фокусного расстояния объект постепенно начнет выглядеть более естественно. Чтобы не искажались пропорции лица во время съемки вблизи, рекомендуется использовать фокусное расстояние 70-135 мм[173].

Такие же требования могут быть предъявлены и при съемке рукописных документов со спорной подписью или рукописью в рамках почерковедческой экспертизы. В том случае, если настройки камеры будут искажать изображение документа, и следователь, и эксперт потеряют такие значимые для исследования признаки, как оттенок бумаги, цвет пишущего прибора, наличие загрязнений и иных частиц на бумаге, наличие заломов, линий сгиба и т.д.

Очевидное влияние следственных ошибок объясняется тем, что именно следователь решает, какие именно объекты будут предоставлены в распоряжение

---

[173] Почему камера телефона искажает лицо и как это исправить. URL: https://androidinsider.ru/polezno-znat/pochemu-kamera-telefona-iskazhaet-liczo-i-kak-eto-ispravit.html?ysclid=lydgdclnrl936468974 (дата обращения: 05.07.2024 г.).

эксперта. Например, эксперт обнаруживает, что предоставленных объектов оказалось недостаточно, а имеющиеся фотографии лица сильно устарели и сделаны в неверный идентификационный период и сообщает об этом следователю. В таком случае следователю нужно сделать дополнительные снимки внешности, которые он снимает на свое мобильное устройство со встроенной ретушью и на неправильном фокусном расстоянии. В таком случае объект будет подходить по временному критерию, поскольку будет сделан в нужный идентификационный период, однако качество отображенных признаков будет как минимум сомнительным, как максимум – недостоверным, как и само техническое оборудование, на которое были сделаны снимки[174].

Помимо следователей мобильные устройства в качестве фиксирующего устройства используют также сотрудники ГИБДД во время осмотра дорожно-транспортного происшествия, что влечет за собой ряд затруднений и ошибок. Так, на практике был случай, когда при дорожно-транспортном происшествии сотрудник ГИБДД зафиксировал на мобильное устройство следы повреждений на шинах, а затем на исследование эксперту в рамках судебной трасологической экспертизы направил ксерокопии сделанных фотографий. Перед экспертом была поставлена задача провести по этим ксерокопиям идентификационное исследование, чего делать было нельзя, однако, эксперт провел экспертизу и сформулировал ответ по поставленному вопросу. В дальнейшем на данное экспертное заключение была подготовлена рецензия специалиста, в которой были указаны совершенные ошибки.

Отчасти негативный фактор использования в ходе следственных и оперативно-розыскных мероприятий камер мобильных телефонов мы объясняем сильным искажением черт внешности, характеристик объектов окружающей действительности и т.д. Вместе с тем, справедливо отметить, что искажения во внешности практически невозможно преодолеть даже при использовании

---

[174] Шихалиева С.З. Модификация объективных ошибок судебного эксперта в контексте цифровизации / С. З. Шихалиева // Судебная экспертиза. — 2025. — № 3 (79). С. 149.

фотоаппаратов. Так, об этом частично упоминается в Национальном стандарте Российской Федерации ГОСТ Р ИСО/МЭК 19794-5-2013 «Информационные технологии. Биометрия. Форматы обмена биометрическими данными. В части 5 «Данные изображения лица» установлены требования к фотографированию лица и криминалистические рекомендации по фотографированию лиц, которые необходимо соблюдать по причине возможности искажения черт внешности из-за фотографирующего устройства[175]. Таким образом, если даже с применением фотоаппаратов искажения устранить сложно, об использовании камер мобильных устройств, на наш взгляд, не может быть и речи. Кроме того, могут возникнуть сомнения в формировании доказательств (фотографий, видеозаписей, аудиозаписей) законным способом при использовании должностными лицами личных мобильных устройств.

И.Н. Подволоцкий пишет следующее: «Настало время критически пересмотреть практику использования бытовых устройств в судопроизводстве. Экспертную и криминалистическую работу следует адаптировать для использования специальных много функциональных мобильных устройств, предназначенных для криминалистических исследований и оснащенных сертифицированными программами работы с цифровой фото- и видеоинформацией»[176]. Таким образом, в качестве решения проблемы несанкционированного использования бытовых устройств (мобильных устройств, планшетов и т.д.), для фиксации, обработки и работы с цифровыми файлами автор предлагает разработать специальные мобильные устройства, которые будут обладать необходимым функционалом и сертифицированными программами. Такая идея, конечно, может быть оценена положительно, потому что она могла бы разом решить половину проблем и предотвратить множество описанных нами

---

[175] ГОСТ Р ИСО/МЭК 19794-5-2013 «Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица». — Москва : Стандартинформ, 2015. — 117 с.

[176] Подволоцкий, И. Н. Использование цифровых технологий в деятельности экспертов / И. Н. Подволоцкий // Вестник криминалистики. — 2023. — № 4. С. 53.

ошибок. Однако, как мы уже отмечали, любая идея хороша до тех пор, пока не заходит речь о ее реализации. Это представляется не только сложным технически, но и неподъемным в финансовом плане: чего будет стоить только сама разработка программ, мобильных устройств, сертификация, лицензирование. Помимо этого, нужно снабдить такими устройствами всех экспертов, хотя бы государственных. К тому же, нельзя не учитывать необходимость оснащения данными устройствами частных экспертов.

В дополнение к предложенному способу решения проблемы нами предлагается другой вариант: создать примерный перечень базовых программ, которые уже имеются в свободном доступе в программном обеспечении большинства компьютеров, для работы с цифровыми объектами. Обратим внимание, что речь не идет о мобильных устройствах вообще, одобрение их использования в экспертной и следственной деятельности на данный момент видится нам невозможным. Рассмотрим плюсы и минусы данной идеи.

Для выяснения мнения экспертов мы задали вопрос «На Ваш взгляд, каким критериям должно соответствовать программное обеспечение судебного эксперта?» Среди наиболее распространенных характеристик качественного программного обеспечения эксперты выделили следующие:

- простота использования;
- надежность;
- доступ к многократному использованию;
- эффективность;
- открытость (opensource);
- наличие лицензии и сертификации;
- апробированность:
- обновляемость и т.д.

Кроме того, эксперты выделили среди необходимых качеств программного обеспечения возможность применять большинство методик экспертного исследования для всех видов традиционных и новых объектов, полное

исследование поступающих объектов, правомерность для легитимного использования, соответствие функционала программы методическим рекомендациям Минюста, возможность поддержки обратной связи с разработчиком, вычисления не должны перегружать рабочую станцию эксперта. Как мы видим, список требований достаточно большой, более того – не всегда реализуемый, поскольку даже не все наиболее распространенные программы отвечают хотя бы большей части перечисленных критериев.

На необходимость создания программного обеспечения применительно к цифровым объектам обращают внимание многие исследователи. Например, в рамках судебной трасологической экспертизы объектами исследования все чаще выступают не объемные гипсовые слепки следов обуви, шин, а их цифровые фотоизображения. Качук А.В. отмечает следующее: «Исследование следа, зафиксированного на цифровом фотоизображении, показало, что в настоящее время отсутствует единое программное обеспечение для осуществления исследования по фотоизображениям, однако при необходимости можно использовать существующие программы. В перспективе рассматривается разработка программного обеспечения, включающего в себя возможности исследования метаданных изображения, измерения размеров сфотографированных следов и их особенностей, а также отображения протокола внесения изменений»[177].

Среди программ, которые применимы к изучению свойств фотоизображений, автор выделяет «ShowEXIF», «XnView MP», «Adobe Photoshop CS5», «PhotoPro», разработанной отечественной компанией ООО «ЛСРМ» (лаборатория спектрометрии и радиометрии), созданной в рамках АРМ «Эксперт».

На вопрос «По вашему мнению, возможно ли создание единого, установленного ГОСТ перечня программ, необходимых судебному эксперту для работы с цифровым объектом?» ответы получились неоднозначными: 39,13% «за»

---

[177] Качук, А. В. Особенности трасологического исследования следов, зафиксированных на цифровых фотоизображениях / А. В. Качук // Право, общество, государство: проблемы истории, теории и практики. Сборник материалов Всероссийской научно-теоретической конференции. Составитель С.Г. Куликова. — 2023. С. 504.

и 60,87% «против». В качестве основных причин отрицательной позиции эксперты отметили следующие:

- скорость развития технологий не сопоставима с возможностью быстрого внесения изменений в ГОСТ или иной унифицированный перечень;

- быстрота видоизменения цифровых следов, и для их исследования необходимо в каждом отдельном случае применять новые программы;

- невозможность создания единого перечня всех экспертных методов и технических средств, развитие техники всегда будет опережать документ;

- трудоемкость.

Как мы видим, в основном сомнения вызывает именно консервативность развития и изменения ГОСТ или реестра программ и его невозможность «идти в ногу» с быстро изменяющимися технологиями, экспертными задачами, цифровыми объектами. Однако, не все эксперты отозвались так категорично, для определенной части эта идея кажется реализуемой при соблюдении некоторых оговорок. Например, вместо ГОСТ предлагается просто вести постоянно пополняемый реестр унифицированных программ, подходящих для исследования большинства объектов. Также можно создать перечень минимально необходимых базовых программ, при этом не ограничивая эксперта в выборе программного обеспечения, поскольку есть нестандартные задачи, для решения которых ограниченного функционала может быть недостаточно. Некоторые эксперты отмечают положительный аспект создания реестра программ для работы с цифровыми объектами, объясняя это тем, что в таком случае появится регламентированный подход. Также эксперты говорят, что ГОСТ – это общее требование, которое носит рекомендательный характер, а предполагаемые программы просто должны ему соответствовать. Если программа соответствует ряду прописанных в ГОСТ требований, то она вносится в сертификационный список.

Безусловно, нельзя обязать всех экспертов использовать только четко обозначенный список программ и приложений, поскольку, как верно было

отмечено, ГОСТ не устанавливает общеобязательных норм. Нам пока неясно, в каком формате возможна реализация данной идеи, возможно, термин «реестр» действительно является более подходящим. Одним из опрошенных была предложения идея разработать единый стандарт: «Необходим стандарт, устанавливающий общие положения для любого программного обеспечения для экспертов. По типу ГОСТ Р 54593-2011 Информационные технологии (ИТ). Свободное программное обеспечение. Общие положения». Согласимся, что нечто подобное, как приведенный выше ГОСТ, уже существует, и ГОСТ для экспертов можно было бы сделать по его образу и подобию, однако, необходимо помимо соответствующей сферы применения учитывать следующее. ГОСТ Р 54593-2011 «Информационные технологии (ИТ)» предполагает возможность использования именно свободного программного обеспечения для различных структур и компаний. Для экспертов же такая политика представляется не совсем корректной, поскольку программное обеспечение экспертов должно быть лицензированным и сертифицированным.

Таким образом, проанализировав все вышесказанное, мы приходим к выводу о том, что наиболее рациональным может быть вариант разработать единый перечень/реестр базовых программ для работы с цифровыми объектами, где к программам должны предъявляться следующие требования:

- апробированность;
- сертифицированность;
- обслуживание большинства традиционных и цифровых объектов;
- надежность и точность результатов.

Такой перечень программ не обязательно должен включать в себя все существующие проверенные программы, он может состоять из набора базовых программ, которые подходят для работы с большинством объектов и решения типичных задач. Как правильно отмечают эксперты, предугадать, какие именно программы нужны будут в ближайшем будущем для решения задач при исследовании новых цифровых объектов, неизвестно, экспертам необходимо

оставлять возможность пользоваться сторонними программами в соответствии с поставленными задачами. Однако здесь опять встает вопрос о легитимности такого программного обеспечения, ведь, как мы выяснили, отвечать задачам могут и мобильные устройства, и программы, размещенные в сети Интернет, но критериям достоверности они вряд ли соответствуют. Безусловно, говорить об обязательности не приходится: такой характер любому реестру (перечню) может придать только официальное признание ведомственными управлениями и т.д.

Поиск на зарубежных серверах показывает, что в иностранных организациях также предпринимаются определенные попытки создать специальную платформу, реестр программ для работы с цифровыми доказательствами в целом. Например, существует «List of digital forensics tools» – Список инструментов цифровой криминалистики. Программы в нем подразделяются по виду лицензии (общая публичная лицензия, проприетарная лицензия), по операционной системе (Linux, Windows, macOC). Так, уже разработана Платформа цифровой криминалистики, Forensic Toolkit, или FTK – программное обеспечение для компьютерной криминалистики, сканирующее жесткий диск в поисках различной информации. С его помощью можно, например, находить удаленные электронные письма и сканировать диск на наличие текстовых строк. Также был разработан «Digital Forensic Framework» (Платформа цифровой криминалистики) – это пакет программного обеспечения для компьютерной криминалистики с открытым исходным кодом. Она используется для сбора, сохранения и раскрытия цифровых доказательств без ущерба для систем и данных[178].

Обзор отечественных источников позволил выявить на данный момент лишь авторские перечни программ по работе с цифровыми доказательствами, созданные пользователями интернета или иными неспециалистами в данной области.

[178] 46 инструментов судебной экспертизы информационной безопасности. URL: https://waksoft.susu.ru/2018/01/18/podborka-besplatnyih-utilit-kompyuternoy-kriminalistiki-forenziki/ (дата обращения: 12.01.2025).

Например, на одном сайте есть «46 инструментов судебной экспертизы информационной безопасности», среди которых приводятся следующие:

- дисковые инструменты сбора данных (Arsenal Image Mounter — утилита для работы с образами дисков в Windows, доступ к разделам и томам и т. д.; EnCase Forensic Imager — утилита для создания доказательных файлов EnCase; FTK Imager — просмотр и клонирование носителей данных в среде Windows и т.д.);

- программы по работе с объектами на серверах электронных почт (Mail Viewer — утилита для просмотра файлов Outlook Express, Windows Mail/Windows Live Mail, базы данных сообщений Mozilla Thunderbird и отдельных файлов EML и др.);

- программы для работы с файлами и данными (Crowd Inspect — утилита для получения информации о сетевых процессах, перечислении двоичных файлов, связанных с каждым процессом; Defraser — утилита для обнаружения полных и частичных данных о мультимедийных файлах в нераспределенном пространстве; Encryption Analyzer — утилита для анализа защищенных паролем и зашифрованных файлов, анализирует сложность шифрования отчетов и варианты дешифрования для каждого файла; ExifTool — утилита для чтения и редактирования данных Exif в большом количестве типов файлов; MetaExtractor — утилита для извеления мета-информации из офисных документов и pdf; Shadow Explorer — утилита для просмотра и извлечения файлов из теневых копий)[179].

Очевидно, что приведенный перечень носит по меньшей мере «любительский» характер, какие-то программы, возможно, и отвечают требованиям достоверности и безопасности, и могут вполне пригодиться эксперту/специалисту при изъятии и исследовании цифровых объектов, однако, такой перечень не может рассматриваться серьезно и отвечать методологическим

[179] 46 инструментов судебной экспертизы информационной безопасности. URL: https://waksoft.susu.ru/2018/01/18/podborka-besplatnyih-utilit-kompyuternoy-kriminalistiki-forenziki/ (дата обращения: 12.01.2025).

требованиям судебно-экспертного обеспечения. Он был приведен в качестве ознакомительного примера.

Таким образом, предложенная идея создать единый перечень базовых программ для работы с цифровыми объектами имеет право на существование: ее создание при соблюдении строгих правил смогло бы улучшить качество проведения экспертных исследований и минимизировать совершение экспертных ошибок. Как и прежде, препятствиями к реализации остаются сложности технического и финансового обеспечения. Руководствуясь вышенаписанным, мы разработали примерный перечень программ, которым могут пользоваться эксперты при необходимости исследовать цифровые следы. Отметим, что в силу постоянного обновления ПО и появления новых объектов исследования перечень не является окончательным и закрытым, мы подразумеваем, что он должен постоянно обновляться и пополняться. Примерный перечень программ представлен в Приложении №6.

Стоит отметить, что большинство из перечисленных ранее программ на сегодняшний день недоступны для использования, продление или покупка официальной лицензии для конкретной программы также невозможны. Вследствие этого возникает следующая проблема: в качестве альтернативы для замены недоступных программ эксперты прибегают к использованию отечественных аналогов. Такие программы находятся в открытом доступе и зачастую являются нелицензионными и недостаточно апробированы, не адаптированы для решения экспертных задач. Подобная практика вызывает сомнения в соответствии методическим рекомендациям, поскольку в каждом случае эксперт должен быть уверен, что функционал и специфика заменяющей программы соответствуют тем же показателям той программы, которая была указана в методике, как пригодная для работы с конкретным объектом. В данном случае эксперт допускает деятельностную ошибку.

Перейдем к рассмотрению других экспертных ошибок, связанных с непосредственным использованием экспертами результатов технологий ИИ в

своих исследованиях. На данный момент прослеживается тенденция пополнения инструментария судебного эксперта технологиями ИИ, что имеет как плюсы, так и минусы. Рассмотрим положительные аспекты применения ИИ при производстве судебных экспертиз.

Использование технологий ИИ может значительно улучшить качество и эффективность судебных экспертиз, а также ускорить процесс принятия решений. Среди очевидных плюсов использования ИИ можно выделить:

- возможность осуществления анализа большого массива данных: ИИ способен обрабатывать и анализировать огромные объемы данных, что позволяет экспертам быстрее находить необходимые доказательства и факты. Например, алгоритмы машинного обучения могут выявлять закономерности в данных, которые могли бы остаться незамеченными при традиционном анализе;

- автоматизация рутинных задач: многие процессы в судебной экспертизе, такие, как сбор и систематизация документов, могут быть автоматизированы с помощью ИИ. Это экономит время и ресурсы экспертов для более трудоемких задач, требующих непосредственного «человеческого» анализа и интерпретации;

- компьютерное зрение: технологии компьютерного зрения могут использоваться для анализа изображений и видео. Например, ИИ может помочь в распознавании лиц, идентификации объектов на фотографиях или видео и даже в анализе следов на месте преступления;

- обработка естественного языка: ИИ может быть использован для анализа юридических документов, контрактов и других текстов. Алгоритмы обработки естественного языка (NLP) могут извлекать ключевую информацию, выявлять противоречия и помогать в составлении юридических заключений.

Среди современных технологий ИИ, применяемых сегодня в судебной экспертизе, можно выделить следующие:

1) Компьютерное зрение «OpenCV» – это библиотека для компьютерного зрения, которая может использоваться для анализа изображений и видео, например, для распознавания лиц или анализа следов на месте преступления;

2) «Gephi» – это программа для анализа социальных сетей. Она может использоваться для визуализации и анализа сетей, что помогает в расследованиях, связанных с преступлениями с организованной преступностью или киберпреступлениями.

3) Системы для анализа аудиозаписей по типу «Veritone». Платформа, использующая ИИ для анализа аудиозаписей, позволяя извлекать ключевую информацию и автоматически транскрибировать важные фрагменты – особенно актуально для фоноскопических экспертиз и другие.

Таким образом, технологии ИИ имеют потенциал значительно изменить судебную экспертизу, повысив ее эффективность и точность. Однако, важно подходить к этому процессу с осторожностью, учитывая возможные риски и этические аспекты. В частности, при неосторожном использовании технологий ИИ, недостаточно апробированных, не поверенных, не унифицированных, а также чрезмерное полагание на те решения и ответы, которые нейросети предлагают на поставленные задачи, эксперт рискует выработать у себя привычку необдуманно доверять ИИ, не проверяя самолично полученные результаты и фактически не решая ничего самостоятельно. Здесь и кроется потенциальная опасность в действиях эксперта, поскольку подмена собственного экспертного исследования исключительно результатами работы технологий ИИ будет очевидной ошибкой. Справедливо замечание А.А. Аубакировой: «Несмотря на внедрение высоких технологий, в процессе познания главенствующая роль остается за человеком»[180].

На сегодняшний день учеными проводятся исследования, в рамках которых изучаются погрешности, допускаемые технологиями ИИ при обеспечении компьютерно-технического оснащения экспертного исследования. Например, в своей работе Газизов В.А., Заварихина Е.О. и Бондаренко Д.М. рассказывают об особенностях 3D-сканирования в аспекте габитоскопических исследований. В частности, новейшие технологии, позволяющие на основе 2D-изображений

[180] Аубакирова, А.А. Интеллектуальные ошибки эксперта при формировании его внутреннего убеждения : монография / А.А. Аубакирова. — М. : Юрлитинформ, 2012. С. 98.

построить объемную, трехмерную модель лица и головы необходимого лица представляются шагом к совершенствованию экспертной методики идентификации внешности человека[181]. Такие технологии применимы сразу к нескольким видам исследований, особую актуальность они представляют, конечно же, для судебной портретной экспертизы. Сама технология, именуемая «ВОКОРД видеоэксперт» работает следующим образом: «Расставленные точки на изображении объекта (лицо, номерной знак автомобиля и др.) позволяют математическому алгоритму программы «ВОКОРД Видеоэксперт» проводить измерения, определять угол поворота изображения и при необходимости повернуть его в нужное положение.

Например, привести изображение лица к положению для сигналетической фотосъемки, предложенной еще А. Бертилионом в XIX в., в настоящее время для биометрической идентификации используется термин «фронтальное положение»[182]. Нужна такая система хотя бы потому, что нередко объектами судебно-портретного исследования выступают изображения с записей камер видеонаблюдения, где, естественно, изображение лица объемное.

В качестве сравнительных образцов наоборот чаще всего предоставляют двухмерные, «плоские» фотоизображения – фото из паспорта, водительского удостоверения и т.д. В таком случае проведение сравнительного исследования требует приведения изображений к единому ракурсу, соответственно, необходимо будет отбирать дополнительные образцы, делать фотографии. Альтернативой такому процессу может выступить как раз выстраивание объемного изображения, где при желании можно подобрать любой требуемый ракурс при помощи 3D-моделирования.

---

[181] Газизов, В. А., Заварихина, Е. О., Бондаренко, Д. М. 3D-сканирование и совершенствование методов габитоскопических исследований в условиях цифровой трансформации криминалистики / В. А. Газизов, Е. О. Заварихина, Д. М. Бондаренко // Технико-криминалистическое обеспечение раскрытия и расследования преступлений: Сб. науч. трудов. — 2022. С. 69.

[182] Программа «ВОКОРД» Видеоэксперт. Регистрационный номер в едином реестре российского ПО – 3294. Производитель: ООО «Вокорд Софтлаб» // Сайт «Целевые технологии». URL: http://aimtech.ru/catalog/152 (дата обращения: 21.02.2025).

В качестве технического инструментария здесь выступает 3D-сканер – это устройство, производящее трехмерное сканирование материального объекта для создания его цифровой 3D-модели. Трехмерное или 3D-сканирование – это копирование объемных объектов. Для этого обеспечивается точное измерение всех геометрических параметров, а их обработка позволяет построить цифровую модель (полигональная модель или облако точек). Далее она может выводиться на экран компьютера (гаджета) или на 3D-принтер для материального воспроизводства[183]. Следует отметить, что подобные технологии могут применяться не только относительно внешности человека, но и для моделирования места происшествия. Э. Курбанаева, И. Степанова, М.Г. Чепрасов отмечают актуальность таких технологий: «Перспектива применения 3D-сканирования при раскрытии и расследовании уголовных дел такова: на смену фотографиям и ручным измерениям в следственных процессах и судебной экспертизе приходит лазерное 3D-сканирование. Приборы создают трехмерные модели мест происшествия с точной фиксацией расположения объектов и расстояний между ними. Данные используют в процессе досудебных и судебных разбирательств»[184]. Таким образом, практическое использование трехмерного сканирования – это уже реальность сегодняшнего дня.

Авторы отмечают возможность внедрения технологии трехмерного сканирования в программное обеспечение судебного эксперта следующим образом: «В настоящее время с переходом на использование российского программного обеспечения и создания условий для использования открытого программного обеспечения возникает возможность при производстве судебных экспертиз применять программное обеспечение на условиях открытой лицензии. А

---

[183] Газизов, В. А., Заварихина, Е. О., Бондаренко, Д. М. 3D-сканирование и совершенствование методов габитоскопических исследований в условиях цифровой трансформации криминалистики / В. А. Газизов, Е. О. Заварихина, Д. М. Бондаренко // Технико-криминалистическое обеспечение раскрытия и расследования преступлений: Сб. науч. трудов. — 2022. С. 72.

[184] Курбанаева, Э., Степанова, И., Чепрасов, М. Г. Значение 3D-технологий в науке «Криминалистика» / Э. Курбанаева, И. Степанова, М. Г. Чепрасов // Вестник казахско-русского международного университета. — 2015. — № 4 (13). С. 94.

для работы с изображениями в области судебной экспертной деятельности может быть использован графический редактор GIMP, при условии выполнения вышеуказанных постановлений правительства. GIMP свободно распространяемый графический редактор, предназначенный для широкого спектра потребителей, но при этом позволяет применять методы и приемы габитоскопических исследований согласно действующей методике 2010 г. «Идентификация личности по признакам внешнего облика (прижизненное изображение)»[185].

Таким образом, при наличии очевидных плюсов использования технологий трехмерного моделирования внешности человека, существуют и неоспоримые минусы, которые при отсутствии должного внимания могут привести к тому, что часть важных признаков внешности может быть попросту «стерта». Также исследователи указывают на одновременно преимущество и недостаток применения трехмерных моделей объектов малых размеров, которая выражается в следующем: «Небольшие по размеру доказательства могут быть распечатаны в большем масштабе, чтобы показать детали. Объект может быть увеличен для изучения деталей, которые трудно увидеть невооруженным глазом, и могут быть использованы для демонстрации в зале суда. Однако, при всех достоинствах, в настоящее время еще не проведено достаточное количество исследований, посвященных оценке полноты и точности передачи мелких особенностей объектов, практическая сфера применения пока что ограничена»[186].

Отметим, что мы не отрицаем положительных аспектов внедрения 3D-моделирования для постоянного использования внешности, однако, это должно быть организовано лишь при условии устранения всех описанных недостатков. Также не стоит забывать, что на данном этапе развития судебной экспертологии

---

[185] Газизов, В. А., Заварихина, Е. О., Бондаренко, Д. М. 3D-сканирование и совершенствование методов габитоскопических исследований в условиях цифровой трансформации криминалистики / В. А. Газизов, Е. О. Заварихина, Д. М. Бондаренко // Технико-криминалистическое обеспечение раскрытия и расследования преступлений: Сб. науч. трудов. — 2022. С. 75.

[186] Полякова, А. В. Формирование и развитие 3D-технологий в судебно- экспертной деятельности: методологические и организационные аспекты : дис. …канд. юрид. наук : 5.1.4 / Полякова Анастасия Васильевна. — Уфа, 2023. С. 67.

все технологии ИИ целесообразно рассматривать лишь как дополнительный, ориентирующий инструмент. Разработанные методы могут использоваться в специализированных программных комплексах эксперта-криминалиста, результаты применения будут являться дополнительной информацией для идентификации личности[187].

Помимо технологии трехмерного моделирования в настоящий момент в судебной портретной экспертизе рассматривается возможность применения достижений нейросетей. Работают алгоритмы нейросетей следующим образом: специально разработанную систему, ориентированную на распознавание лица/внешности человека по определенным критериям, обучают на образцах фотоснимков. Далее в процессе обучения такую систему тренируют выявлять доминирующие, устойчивые индивидуализирующие признаки внешности одного человека среди массива фотоизображений разных лиц. В дальнейшем на основании такой схемы систему доводят до автоматизма, когда она учится самостоятельно выстраивать взаимосвязь между найденными признаками для того, чтобы потом узнавать среди имеющегося множества предъявляемые новые изображения[188].

Механизмы нейросетей способны осуществлять автоматизированный поиск изображений среди баз данных зарегистрированных лиц, причем в ближайшем будущем все препятствия в виде различных ракурсов, плохого освещения на записях с камер видеонаблюдения и т.д. могут быть преодолены. Рассуждая на эту тему, А.М. Зинин поднимает вопрос о возможности замены криминалистической портретной экспертизы подобным процессом распознавания лиц. Он отмечает, что при наличии такой возможности перед нейросетями все еще стоит целый ряд спорных моментов: умышленное или случайное изменение характеристик внешности при фотографировании, плохие, некачественные условия, в которых

---

[187] ГОСТ Р ИСО/МЭК 19794-5-2013 «Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица». — Москва : Стандартинформ, 2015. — 117 с.

[188] Друки А. А. Системы поиска, выделения и распознавания лиц на изображениях / А. А. Друки // Известия Томского политехнического университета. — 2011. —№ 5. С. 68.

были сделаны снимки (освещение, неоднородно фиксирующее черты внешности, осуществление видеосъемки в затруднительных условиях, через стекло автомобиля и т.д.)[189]. Естественно, сама нейросеть не способна фильтровать все указанные условия, она будет работать лишь по заданному алгоритму, в котором учет сопутствующих негативно влияющих на качество снимков обстоятельств не предусматривается.

Примечательной является следующая статистика, приведенная на сайте Русского общества содействия биометрическим технологиям, системам и коммуникациям: в разных странах, заинтересованных в активном продвижении и внедрении таких технологий, уже были зафиксированы случаи ошибочного совпадения выявляемых лиц при проведении массовых мероприятий, зафиксированных в базах данных[190]. О.Г. Дьяконова и А.М. Зинин пишут о том, что большая часть методов распознавания лиц сводится к успешному анализу изображений, полученных в одинаковом ракурсе с изображений анфас. Однако при использовании измененного ракурса, различных видов освещения, изображении с невысокой разрешающей способностью применение методов оказывается мало результативным[191].

Еще одним аргументом в противовес идее замены фигуры эксперта технологиями нейросетей является положение, которое А.М. Зинин упоминает в своей работе. Это касается того, что нейросети при исследовании изображений работают с фотоснимками определенной давности, исходя из этого изменения во внешности, обусловленные истечением времени, наличием травм или хирургических вмешательств игнорируются, что значительно снижает качество применения подобных нововведений. Наконец, автор приходит к выводу о том, что

---

[189] Зинин А.М. Нейросети и судебно-портретная экспертиз // Вестник криминалистики. 2020. № 2 (74). С. 66-69.

[190] Некоммерческое партнерство "Русское общество содействия развитию биометрических технологий, систем и коммуникаций". URL: http://www.rusbiometrics.com/ (Дата обращения 06.05.2020).

[191] Зинин А.М., Дьяконова О.Г. Мышление человека и ИИ в аспекте сравнительного исследования внешнего облика человека по его изображениям // Эксперт-криминалист. 2023. №3. С.2-5.

что применение нейросетей при распознавании лиц среди больших массивов изображений не может заменить практику назначения и выполнения судебных портретных экспертиз[192].

Помимо судебной портретной экспертизы, существуют и другие виды, где эксперту приходится сталкиваться с качественно новыми цифровыми объектами, которые требуют мобильности и обновления методико-технического обеспечения. Рассмотрим сложности, обусловленные цифровыми объектами в рамках судебной фоноскопической экспертизы. Как мы знаем, объектом судебной фоноскопической экспертизы чаще всего выступает фонограмма. Сегодня наиболее распространенным способом записи устной речи является именно цифровая фонограмма.

Как отмечает А.К. Лебедева, «сложность проверки и оценки достоверности информации, запечатленной в устной речи на цифровой фонограмме, заключается в принципиальной возможности редактирования и монтажа фонограммы без оставления видимых следов манипуляций»[193]. Среди фонограмм, в том числе цифровых, выделяют аутентичные и неаутентичные. Последние, согласно позиции Е.И. Галяшиной, могут быть получены следующими способами: «уменьшение количества информации (выборочная фиксация, остановки во время записи, ее прерывание, отключение микрофона, стирание и т.д.); увеличение количества информации (дополнение фонограммы в любом ее месте, наложение дополнительной информации на существующую, искусственное формирование вербальной составляющей диалога и т.д.); замена информации, одних фрагментов фонограмм или записанных речевых и неречевых сигналов другими и т.д.; подбор

---

[192] Зинин, А. М. Нейросети и судебно-портретная экспертиз / А. М. Зинин // Вестник криминалистики. — 2020. — № 2 (74). С. 69.

[193] Лебедева, А. К. Особенности судебно-экспертного исследования голоса, измененного при помощи компьютерно-технических средств / А. К. Лебедева // Известия Тульского государственного университета. Экономические и юридические науки. — 2016. — № 3—2. С. 324.

и сочетании компонентов информации (монтаж, компиляция, микширование и т.д.)»[194].

А.К. Лебедева предлагает под способами изменения голоса при помощи компьютерно-технических средств понимать, например, искажение голоса за счет его цифровой обработки при помощи специальных программных продуктов: «Если раньше для подобной цифровой обработки голоса необходимо было устанавливать сложное программное обеспечение, то сейчас достаточно просто скачать приложение на мобильное устройство. Например, в Apple Store есть приложения, которые так и называются «Запись и изменение голоса», «Изменение голоса и маскировка», «Клонируй голоса знаменитостей» и т.д. Существующие программы могут изменять как загруженную в них ранее записанную фонограмму, так и изменять речевой сигнал в реальном времени, например, при общении через Skype, WhatsApp и др.»[195].

Указанный автор отмечает, что при использовании подобных программ речевой сигнал на фонограмме можно изменить либо постфактум, либо в реальном времени, непосредственно перед его поступлением в канал записи[196]. Данное положение указывает на то, что в случае привнесения изменений в устную речь в реальном времени проследить какие-либо признаки монтажа, постобработки крайне сложно. В таком случае эксперт, естественно, может воспользоваться достижениями ИИ, однако, не забывая о допускаемых им погрешностях и ошибках.

Особо острой является вопрос определения экспертом синтезированной звучащей речи. Синтез речи — это технология, позволяющая преобразовывать

---

[194] Галяшина, Е. И. Современные проблемы экспертиз цифровых фонограмм / Е. И. Галяшина // Современные проблемы цифровизации криминалистической и судебно-экспертной деятельности: материалы научно-практической конференции с международным участием. — 2019. С.55.

[195] Лебедева, А. К. Проблемы производства судебной фоноскопической экспертизы в свете развития цифровых технологий / А. К. Лебедева // Вестник Университета имени О. Е. Кутафина. — 2020. — №6 (70). С.68.

[196] Лебедева, А. К. Особенности судебно-экспертного исследования голоса, измененного при помощи компьютерно-технических средств / А. К. Лебедева // Известия Тульского государственного университета. Экономические и юридические науки. — 2016. — № 3—2. С. 324.

текст в звучащую речь. Технологии голосового синтеза и распознавания речи используются повсеместно, позволяют наладить эффективное взаимодействие между пользователем и различными системами в сфере телекоммуникаций (например, прочтение сообщений из мессенджеров и электронной почты, голосовые напоминания и оповещения). А.К. Лебедева отмечает: «Технологии голосового синтеза уже никого не пугают. В настоящее время часто возникают вопросы, является ли речь результатам голосового синтеза или была произнесена конкретным человеком в определенной коммуникативной ситуации. Экспертам-фоноскопистам необходимо быть готовыми к тому, что перед ними может быть поставлен вопрос, связанный с установлением факта использования технологий голосового синтеза для создания спорной фонограммы»[197]. Г.Н. Зубов отмечает следующее: «в результате такого синтеза речь разных людей (например, участников одного или нескольких разговоров, записанных в одних и тех же условиях) может звучать очень похоже, а спектрально-формантные характеристики могут быть близки до неразличения при использовании типовых, традиционных методов исследования»[198].

На сегодняшний день анализ экспертной практики из открытых источников позволяет нам сделать вывод о том, что действенных методик по выявлению синтезированной речи практически нет. А проведенные в этой области опыты показывают ошибочность применения технологий ИИ. Например, одним из распространенных вариантов применения синтезированной звучащей речи в противозаконных целях является «Спуфинг». Спуфинг (от англ. spoof – имитировать, подделывать) – разновидность кибератак, в результате которых преступник выдает себя за какое-либо лицо (например, за представителя организации, родственника), чтобы получить персональные данные человека,

---

[197] Лебедева, А. К. Проблемы производства судебной фоноскопической экспертизы в свете развития цифровых технологий / А. К. Лебедева // Вестник Университета имени О. Е. Кутафина. — 2020. — №6 (70). С.69.

[198] Зубов Г.Н. «Я не я, и голос не мой»: О возможностях фальсификации фонограмм с помощью современных технологий синтеза устной речи // Сайт «Праворуб». URL: https://pravorub.ru/personal/78856.html (дата обращения: 12.01.2025).

заставить его передать или перевести денежные средства, а также с помощью персональных данных получить доступ к банковским счетам, социальным сетям и пр. Атаки спуфинга различны по своей сути, это может быть выражено в воспроизведении, клонировании голоса, повтора клонированного голоса и др.[199].

Н.Ф. Бодров и А.К. Лебедева отмечают, что технологии клонирования речи, представляют собой серьезную угрозу, поскольку могут использоваться злоумышленниками в корыстных целях: «В заявлении об этике данной компании говорится, что после обучения речевых моделей на ваших образцах голоса пользователь, как владелец «цифрового голоса», после генерации контролирует то, когда и в каких целях используются результаты синтеза. Таким образом здесь и в других упомянутых нами примерах отчетливо прослеживается запрос индустрии на создание отраслевых стандартов для борьбы с дезинформацией»[200].

О.Б. Дронова пишет о том, что в целях противодействия использованию технологий дипфейка в качестве средств совершения преступлений в деятельность экспертно-криминалистических подразделений МВД России внедряется специальное программное обеспечение, которое потенциально позволит сократить время, затрачиваемое на экспертное исследование: «В этой связи для обеспечения потребностей экспертно-криминалистических подразделений МВД России на основе выполненной НИОКР «Зеркало (Верблюд)» ведется разработка ПТК «КЛОН». Также совместно с Институтом криминалистики ФСБ России идет работа над программой «Дуализм». По утверждению разработчиков, обе они обеспечат выявление признаков внутрикадрового монтажа видеоизображений, выполненных с помощью нейронных сетей, а также автоматизацию производства поиска

---

[199] Voice spoofing detector: A unified anti-spoofing framework. / Ali Javed, Khalid Mahmood Malik, Hafiz Malik, Aun Irtaza. // Expert Systems with Applications. – 2022. – №198 (8): 116770. URL: https://www.sciencedirect.com/science/article/abs/pii/S0957417422002330 (дата обращения: 12.01.2025).

[200] Бодров, Н. Ф., Лебедева, А. К. Понятие дипфейка в российском праве, классификация дипфейков и вопросы их правового регулирования / Н. Ф. Бодров, А. К. Лебедева // Юридические исследования. — 2023. — № 11. С. 27.

отклонений и несоответствий установленных параметров при выявлении диагностических признаков внутрикадрового монтажа видеоизображений»[201].

Одним из крупных и прогрессивных разработчиков программного обеспечения для автоматизации процесса производства судебных фоноскопических экспертиз является группа компаний «Центр речевых технологий» (далее — ЦРТ). Их аппаратно-программный комплекс «ИКАР Лаб» решает широкий перечень задач, связанных с анализом цифровых фонограмм. «Входящие в состав комплекса специализированные программные средства обеспечивают высокое качество визуального представления фонограмм речи. Современные алгоритмы голосовой биометрии и мощные инструменты автоматизации всех видов исследования фонограмм речи позволяют экспертам существенно повысить надежность и эффективность экспертиз»[202].

Примечательно то, что в указанном комплексе «ИКАР Лаб» уже разработан специальный модуль диагностики «Обнаружение спуфинга», который нацелен на выявление признаков, указывающих на имитирующие действия. Однако на данный момент доля ошибок при определении признаков синтеза на фонограммах с помощью модуля диагностики «Обнаружение спуфинга» достаточно высока – программа не способна различить, где речь настоящая, а где синтезированная. Об этом также говорят исследователи в области фоноскопических экспертиз: «В результате автоматизированные методы детекции спуфинга, направленные на выявление синтезированной речи, пока не достигают высокой точности, что подчеркивает необходимость разработки алгоритмов, не привязанных к конкретной нейросети, и совершенствования инструментов для анализа подобных

---

[201] Дронова, О. Б. Криминалистические аспекты противодействия преступности в цифровом обществе: современные проблемы и перспективы развития / О. Б. Дронова // На страже закона. — 2024. — № 4. С. 15.

[202] Экспертные системы и шумоочистка Икар Лаб 3 // Группа компаний «ЦРТ». URL: https://www.speechpro.ru/product/ekspertnye-sistemy-i-shumoochistka/ (дата обращения: 12.01.2025).

фонограмм»[203]. В связи с этим требуется ручная проверка спорных объектов экспертом.

Таким образом, очевидно, что перед экспертом, с одной стороны, стоит серьезная проблема в виде распространения технологии спуфинга, который может использоваться для создания фонограммы, как объекта судебной фоноскопической экспертизы, а с другой – очевидное отсутствие действенных методик, позволяющих выявить спуфинг. Имеющиеся инструменты ИИ, в частности, модуль диагностики комплекса «ИКАР Лаб» не показывают внушительных результатов. Все сказанное позволяет нам сделать вывод о том, что эксперт, не проверяя самолично спорные фонограммы на наличие спуфинга, и доверяясь лишь выводам, сделанным вспомогательными модулями, допускает серьезную ошибку.

Развитие современных технологий привело к возникновению новых методов преступления, оставляющих за собой цифровые следы в компьютерных системах и устройствах. Это создает трудности в организации экспертиз, поскольку для работы с такими данными требуется не только привлечение специалистов с глубокими знаниями в этой области, но и базовые понятия у самих следователей. Важно привлекать экспертов, владеющих знаниями о компьютерных технологиях, в том числе способных оперативно извлекать данные, которые могут быть уничтожены подозреваемым или случайно потеряны.

Реализация профилактики экспертных ошибок, обусловленных необдуманным применением технологий ИИ в процессе исследования, представляется возможной посредством разработки соответствующего направления деятельности в рамках риск-менеджмента судебно-экспертной деятельности, как процесса распознавания возможных рисков, управления ими, а также разработки стратегии развития судебно-экспертной деятельности с учетом

---

[203] Бодров, Н. Ф., Лебедева, А. К. Анализ судебной практики установления обстоятельств в случаях противоправного распространения генеративного контента, созданного с помощью технологий ИИ / Н. Ф. Бодров, А. К. Лебедева // Юридические исследования. — 2024. — № 11. С. 17.

потенциальной опасности и негативных последствий влияния рисков, связанных с применением технологий ИИ в судебной экспертизе.

Предлагается взять за основу определение риск-менеджмента в судебно-экспертной деятельности, предложенное Е.В. Чесноковой, а затем модифицировать его для возможности повышения качества экспертных исследований при использовании технологий ИИ. Так, Е.В. Чеснокова пишет: «Деятельность любой судебно-экспертной лаборатории (далее – СЭЛ) подвержена рискам. В целом для судебно-экспертной деятельности характерен свой комплекс рисков, определяемых целями существования СЭЛ, в числе которых получение недостоверных результатов и нарушение сроков производства экспертиз и экспертных исследований»[204].

Автор также выделяет направления деятельности в рамках риск-менеджмента:

«1) идентификация риска;

2) анализ;

3) последующая оценка возможности его изменения.

Идентификация риска представляет собой выявление факторов, способных оказывать влияние на конкретный процесс»[205].

Как мы видим, благодаря данным направлениям выстраивается логичная цепочка последовательных действий, которые по своей сути очень похожи на профилактические меры. В рамках идентификации риска применительно к ИИ мы предлагаем выявлять и фиксировать все возможные и известные спорные моменты, которые могут повлечь за собой потенциальные ошибки. На этапе анализа предлагается изучать конкретные характеристики технологий ИИ, которые и приводят к совершению ошибок, а также исходные данные, заложенные в систему ИИ. Наконец, на этапе оценки возможностей изменения мы предлагаем

---

[204] Чеснокова, Е. В. Концептуальные основы стандартизации в судебно- экспертной деятельности : дис. … д-ра юрид. наук : 12.00.12 / Чеснокова Елена Владимировна. — М., 2022. С. 41.

[205] Чеснокова, Е. В. Концептуальные основы стандартизации в судебно- экспертной деятельности : дис. … д-ра юрид. наук : 12.00.12 / Чеснокова Елена Владимировна. — М., 2022. С. 117.

разработать критерии допустимости применения технологий ИИ в судебно-экспертной деятельности, а также прописать потенциальные риски, которые эксперты должны учитывать в любом случае.

О фиксации рисков пишут Г.Г. Омельянюк и А.И. Усов, перечисляя те риски, которые присущи судебно-экспертной деятельности в целом: «риск для беспристрастности, риск для конфиденциальности, риск получения недостоверных результатов, риск нарушения сроков производства экспертиз и экспертных исследований, риск стагнации или ухудшения системы менеджмента качества»[206].

На наш взгляд, предлагаемые нами риски использования ИИ подходят под риски получения недостоверных результатов, поскольку ранее мы писали, что некритическое восприятие результатов ИИ в экспертном исследовании может привести к некачественному проведению исследования и формулированию неверных выводов.

Таким образом, можно полагать, что в рамках учения о рисках в судебно-экспертной деятельности разрабатываются теоретические и практические разработки, направленные в том числе на профилактику экспертных ошибок, возникающих при исследовании цифровых объектов.

В ФБУ РФЦСЭ при Минюсте России разработан специальный Реестр рисков СМК-РР[207], в соответствии с требованием стандарта о необходимости фиксации всех процессов, происходящих в лаборатории. Фиксация результатов идентификации рисков в Реестре происходит по разработанной РФЦСЭ стандартной форме с ежегодным обновлением и включает в себя следующие позиции: «наименование процесса, к которому они относятся; наименование риска; возможные причины появления риска; возможные последствия реализации риска,

---

[206] Омельянюк, Г. Г., Усов, А. И. Управление рисками в судебно-экспертной деятельности как способ повышения качества экспертного производства / Г. Г. Омельянюк, А. И. Усов // Развитие криминалистики и судебной экспертизы в трудах профессора Е.Р. Россинской: материалы Международной научно-практической конференции, к юбилею ученого, эксперта, педагога. М.: Проспект. — 2019. С. 339.

[207] Указанный Реестр рисков обновляется каждый год, соответственно, внедрение рисков, связанных с технологиями ИИ, вполне возможно в ближайшее время.

значимость риска; вероятность риска; уровень опасности; обработка риска: мероприятия по воздействию на риск; владелец риска и статус мероприятий (им считается эксперт)»[208].

В рамках риск-менеджмента судебно-экспертных лабораторий предлагается следующее:

1) прописать риски, связанные с использованием технологий ИИ в СЭД. Речь идет:

- о недостатках машинного обучения. Например, технологии ИИ, специально обученные для распознавания и идентификации внешности человека по изображениям, способны формулировать только автоматизированный вывод. Такой вывод система ИИ строит на основании анализа большого массива изображений, которому она была обучена. Однако такая система не способна учитывать особенности строения черепа человека и т.д., таким образом, наблюдается «плоскость» и односторонность машинного сравнения, на которое с учетом указанных недостатков эксперт полагаться не должен;

- о недостатках самих баз данных ИИ. Обучение системы ИИ возможно при внедрении для этого огромного количества исходных данных – изображений лиц, отпечатков пальцев, шин и др. Для того, чтобы создать хотя бы одну полноценную базу данных, которая может использоваться для одного конкретного вида исследования, необходимо большое количество времени, ресурсов.

2) сформулировать предложения для ликвидации указанных рисков. Нами предлагается разработать критерии допустимости использования ИИ в судебной экспертизе, к которым можно отнести:

- обучение системы ИИ на достаточном количестве сравнительных образцов;

- обучение системы всем известным диагностическим характеристикам, присущим каждому отдельно взятому объекту судебной экспертизы;

- обучение системы «сопутствующим знаниям», которые должны применяться обязательно для формулирования корректного вывода;

---

[208] Указ.соч., С. 118.

- организация участия контрольного лица или группы лиц (экспертов) при отборе образцов для обучения ИИ;

- обучать конкретную систему ИИ только тем характеристикам объектов, с которыми она уже знакома либо разрабатывать для отдельных признаков собственный вектор обучения. Например, если система ИИ обучена работать с завитковыми папиллярными узорами, то для усовершенствования этой системы целесообразно и дальше направлять в качестве образцов завитковые узоры. В противном случае, если среди образцов будут направлены дугообразные узоры, то система будет подгонять свойства дугообразных узоров под папиллярные. Также должны обучаться системы, применяемые в судебных почерковедческих экспертизах: нельзя смешивать векторы обучения системы между образцами, выполненными ручкой, и образцами, выполненными карандашным грифелем, поскольку качественные признаки, важные для исследования, у них будут разные.

Разработка такого направления деятельности нам представляется крайне важной, с учетом увеличения количества объектов-результатов ИИ, а также появления систем ИИ, внедряемых в экспертное исследование, вопрос устранения рисков обретает особую актуальность и требует серьезной, своевременной проработки.

Ошибки могут возникать на любом этапе исследования. По мнению Н.П. Майлис экспертные ошибки при исследовании цифровых следов могут совершаться:

«1) на этапе обнаружения. Здесь они могут быть следствием невнимательности, недостаточной квалификации или неправильного подхода к методике расследования цифровых следов;

2) на этапе изъятия. Ошибки, возникающие на этапе изъятия, чаще всего связаны с внесением изменений в информацию, хранящуюся на цифровых носителях. Они могут быть случайными из-за недостаточной квалификации специалиста и нарушения процедур изъятия, или намеренными, когда требуется оперативное вмешательство;

3) на этапе исследования. Такие ошибки могут быть обусловлены нарушением процедуры изъятия и исследования, когда эксперт, получивший доступ к функционирующему компьютеру, ограничивается лишь поверхностным осмотром хранилища информации»[209].

По мнению Н.П. Майлис появляются специфические ошибки, возникающие при исследовании цифровых следов:

«– применение неисправного / не прошедшего метрологическую поверку оборудования;

– применение микроскопов с функцией 3D-моделирования и 3D-сканеров, не отвечающих техническим и метрологическим требованиям;

– применение нелицензионного программного обеспечения;

– отсутствие достаточной компетентности эксперта для использования информационных технологий в рамках производства судебных экспертиз и исследований;

– возможность фальсификации цифровых материалов, представленных на экспертизу;

– отсутствие навыка работы с технологиями 3D-сканирования и 3D-моделирования;

– ошибка в формулировании вывода, когда эксперт при ответе на вопрос рассматривает не графический файл, представленный на исследование, а непосредственно сам объект и др.»[210]. Как мы видим, перечень предложенных ошибок во многом пересекается с теми ошибками, которые были рассмотрены нами, что еще раз подтверждает их актуальность, а их специфичность обусловлена природой цифровых объектов.

Помимо указанных, можно также выделять экспертные ошибки, обусловленные проблемами экспертного исследования. При работе с цифровыми

---

[209] Майлис, Н. П. Экспертные ошибки, допускаемые при исследовании традиционных и цифровых следов / Н. П. Майлис // Теория и практика судебной экспертизы. — 2024. — Т. 19. № 1. С. 21.

[210] Там же.

объектами эксперт допускает гносеологическую ошибку в том случае, если игнорирует по определенным причинам сущностные новые характеристики, которыми обладают такие объекты. Например, при почерковедческом исследовании образов цифровых следов почерка на экранах мониторов, мобильных устройствах и пр. необходимо учитывать целый набор новых признаков в отличии от рукописных текстов[211].

Обобщая рассмотренные следственные и экспертные ошибки, можно сделать следующие выводы:

1. В судебно-экспертной деятельности и ранее нередко встречалась совокупность ошибок разного вида, например, следователь, при неверном использовании специального света во время осмотра места происшествия совершает одновременно как операционную, так и гносеологическую ошибку. В отношении объектов в цифровой форме такая тенденция сохраняется: нельзя совершенно четко разграничить процессуальные, гносеологические, операционные ошибки, поскольку их отнесение к конкретной классификации кроется в причине их совершения: либо следователь/эксперт знает, как проводить процедуру, но делает ее неправильно, либо не знает об особенностях действия/объекта вовсе. Таким образом, разделение ошибок носит условный характер.

2. Следственные ошибки при назначении экспертизы цифровых объектов могут совершаться на любом этапе расследования и рассмотрения дела, когда допустимо назначение судебной экспертизы, и во время следственных и оперативно-розыскных мероприятий. Традиционные следственные ошибки, неоднократно описанные учеными и исследователями, сохраняются и также имеют место при изъятии и фиксации цифровых объектов. Общая сводка следственных ошибок, допускаемых при работе с цифровыми объектами, выглядит следующим образом:

---

[211] Россинская, Е. Р., Бодров, Н. Ф. Современное состояние и перспективы исследования образов цифровых следов в судебной почерковедческой экспертизе / Е. Р. Россинская, Н. Ф. Бодров // Криминалистика: вчера, сегодня, завтра. — 2022. — Т. 21. — № 1. С. 132.

- со стороны следователя будет ошибкой не рассчитать хеш-сумму цифрового следа, который будет в дальнейшем направлен на исследование эксперту на объекте-носителе. Ошибкой это будет потому, что в случае отсутствия базового описания следа, у эксперта не будет возможности на самом деле проверить, что именно он получил в распоряжение. Данная следственная ошибка порождает экспертную, где эксперту будет не с чем сравнивать рассчитанную самостоятельно хеш-сумму, следовательно, производить такой расчет не имеет смысла. Отметим, что на данном этапе без нормативного закрепления ошибка носит гносеологический характер, в дальнейшем, если положение о необходимости указывать хеш-сумму будет узаконено, природа ошибки может быть охарактеризована как процессуальная;

- упаковке цифровых объектов должно уделяться такое же внимание, как и упаковке традиционных объектов судебных экспертиз. Вместе с тем важно учитывать, что объекты-носители цифровых следов могут быть хрупкими в силу своей физиологической природы, поэтому их ненадлежащая упаковка может привести: к утрате материального носителя, флеш-накопителя, диска; к поломке диска; к целенаправленной подмене объекта-носителя на иной, схожий по внешним характеристикам и т.д. Помимо описания самого цифрового объекта, следователь должен обязательно полноценно описывать его упаковку, это требование обусловлено простотой замены носителя цифрового следа, его подмены, перезаписи на тот же носитель другого цифрового следа;

- проведение следственных мероприятий при изъятии и фиксации цифровых следов должно осуществляться при наличии всех необходимых технических приспособлений, не допускается копирование цифрового файла на материальный носитель неизвестной природы, например, если следователь принес на место происшествия личный флеш-накопитель, а не на входящий в перечень объектов, стоящих на балансе следственных подразделений (карты память, флеш-карты, дисковые накопители и т.д.) или относящихся к расходным материалам одноразового использования (CD диски) – это будет ошибкой;

- иные следственные ошибки могут допускаться на любом этапе осмотра средств вычислительной техники, что свидетельствует о необходимости обязательно привлекать специалиста. В противном случае следователь из-за недостатка специальных знаний может непреднамеренно уничтожить цифровой след. Особенно часто это происходит в том случае, если отдельно стоящий компьютер включен и его система активна. Следователь может не знать о том, что выключение компьютера без создания копии диска может стереть находящиеся на нем сведения. Например, на некоторых персональных компьютерах диспетчер учетных данных удаляет учетные данные после выхода из системы или перезагрузки компьютера. В таком случае по ошибке следователя цифровой след, содержащий потенциально значимую криминалистическую информацию, может быть бесповоротно утерян.

Ошибкой следователя при осмотре и обыске включенного компьютера будет также следующее:

- следователь создал копию жесткого диска, скопировал находящуюся на нем информацию, но не проверил наличие активных сетевых подключений;

- следователь произвел неполноценный осмотр компьютерной информации (установленных и использующихся приложений, файловой системы, запущенных процессов). В данном случае речь идет о фиксации дерева/каталога программ, что по природе является как процессуальной, так и операционной ошибкой;

- еще одна следственная ошибка связана с неполным отражением действий специалиста в протоколе осмотра места происшествия, поскольку следователь должен зафиксировать не только сам ход действия и полученные результаты, но и указать наименование примененных специалистом технических и программных средств. Кроме того, помимо обыска и изъятия, специалист в отдельных случаях для полного сбора сведений может произвести исследование работающей компьютерной системы.

- помимо непосредственного изучения цифрового устройства и изъятия цифрового следа следователь вместе со специалистом должен учитывать важность осмотра внешней обстановки места происшествия.

В части применения компьютерной техники следователь должен соблюдать требование о фиксации предметов и окружающей обстановки на фотоаппарат. На практике данное правило часто игнорируется, большинство снимков, которые потом становятся объектами исследования либо сравнительными образцами, фиксируются на мобильные устройства, которые значительно искажают объект отображения.

Экспертные ошибки при исследовании цифровых объектов во многом связаны со следственными, но не обусловлены ими исключительно. К ним можно отнести следующие:

- эксперт получил сведения о хеш-сумме, но не провел самостоятельный расчет показателя, в силу чего нельзя говорить со стопроцентной уверенностью о том, что эксперт исследует именно тот объект, что был изъят следователем и направлен ему на экспертизу;

- эксперт не получил никаких сведений о хеш-сумме цифрового следа, находящегося на носителе, однако он не сделал об этом никакой пометки в ходе своего исследования;

- неправильное, неполное описание упаковки, в которой был получен цифровой объект, и состояния объекта также является экспертной ошибкой.

Вопросы компетенции встают в данном случае особо остро. При решении вопроса о том, выходит ли эксперт за пределы своей компетенции при необходимости изъятия цифрового следа, если это является частью экспертного исследования, необходимо исходить из того, входит ли изучение подобных следов в принципе в его компетенцию, а также где именно располагается требуемый цифровой след. Если изъятие цифрового следа находится за пределами компетенции эксперта, целесообразно привлечение специалиста в этих целях;

- также выход экспертом за пределы своей компетенции возможен и в том случае, если перед ним поставлена задача не исследовать сам цифровой след (например, базу 1С), а установить факт изменения технических свойств программы. Если эксперт не обладает компетенцией в области компьютерно-технической экспертизы, ответить на такой вопрос он не вправе;

- наиболее распространенной экспертной ошибкой является конвертирование, кадрирование, обрезка аудио- и видеодорожек в приложениях на мобильных устройствах, а также посредством использования интернет-сайтов. Аналогичная ситуация ожидает эксперта также в том случае, если он будет производить само исследование и анализ аудио- или видеодорожки через сторонние сайты либо мобильные приложения;

- еще одна экспертная ошибка обусловлена тем, что большинство программ, необходимых для исследования цифровых следов, на сегодняшний день недоступны для использования, продление или покупка официальной лицензии для конкретной программы невозможна. Вследствие этого возникает следующая проблема: в качестве альтернативы для замены недоступных программ эксперты прибегают к использованию отечественных аналогов. Такие программы находятся в открытом доступе и зачастую являются нелицензионными. Подобная практика вызывает сомнения в соответствии методическим рекомендациям, поскольку в каждом случае эксперт должен быть уверен, что функционал и специфика заменяющей программы соответствуют тем же показателям той программы, которая была указана в методике, как пригодная для работы с конкретным объектом. В данном случае эксперт допускает деятельностную ошибку;

- множество экспертных ошибок обусловлены неразумным внедрением технологий ИИ в процесс исследования. В частности, при некритичном использовании технологий ИИ, недостаточно апробированных, не поверенных, не унифицированных, а также чрезмерное полагание на те решения и ответы, которые нейросети предлагают на поставленные задачи, эксперт рискует выработать у себя привычку необдуманно доверять ИИ, не проверяя лично полученные результаты и

фактически не решая ничего самостоятельно. Здесь и кроется потенциальная опасность в действиях эксперта, поскольку подмена собственного экспертного исследования исключительно результатами работы технологий ИИ будет очевидной ошибкой.

Изучение перечисленных ошибок позволило заключить, что большая их часть обусловлена недостатком знаний и навыков в области цифровых следов. Поэтому в качестве мер профилактики предлагается следующее:

- разработать для следователей специальную инструкцию по работе с цифровыми следами, их изъятию, подсчету хеш-суммы;

- разработать для следователей рабочую программу, направленную на приобретение необходимых знаний о цифровых следах, потенциальных ошибках и т.д.;

- организовать для экспертов программы дополнительного профессионального образования, обеспечивающие подготовку эксперта, компетентного работать с цифровыми объектами, в рамках его экспертной специальности;

- разработать для экспертов примерный перечень программ, заслуживающих доверия при исследовании цифровых следов;

- выделить в рамках риск-менеджмента экспертных лабораторий направление по изучению рисков при использовании ИИ в экспертных исследованиях.

Таким образом, спрогнозированные нами ошибки и предложенные профилактические меры по их предотвращению доказывают актуальность рассмотренных вопросов и необходимость разработки частной теории экспертной профилактики ошибок при исследовании объектов в цифровой форме.

ЗАКЛЮЧЕНИЕ

В рамках диссертационного исследования проводилось изучение предпосылок и причин трансформации экспертных и следственных ошибок, возникающих при исследовании объектов в цифровой форме. Это обусловило необходимость исследования природы и характеристики цифровых следов.

Цифровым следом является криминалистически значимая компьютерная информация о событиях / действиях в процессе ее возникновения, обработки, хранения, передачи, отраженная в материальной среде. Появление таких следов обусловило формирование новых частных криминалистических и экспертных теорий о цифровизации, в рамках которых изучаются принципы выявления, изъятия и исследования подобных объектов.

Цифровые следы обладают следующими характеристиками:

- во-первых, цифровой след содержит в себе цифровую информацию или цифровые данные, в которых заключаются сведения о действии, предмете, продукте, явлениях действительности;

- во-вторых, цифровой след создается в результате совместных действий человека и компьютера (гаджета, мобильного устройства, другого устройства), не создается сам по себе;

- в-третьих, цифровой след обеспечивает представление цифровой информации в доступной для восприятия форме;

- в-четвертых, цифровой след может быть создать как в интернете, так и за его рамками – в компьютерных программах, с помощью мобильных устройств и т.д.;

- в-пятых, как правило, цифровой след является результатом преобразования информации в конкретную форму.

Цифровые следы можно подразделить на различные виды. Так, отдельную группу цифровых следов представляет цифровой мусор. По возможности получения доступа к цифровому следу, их можно подразделить на находящиеся в

свободном, ограниченном доступе либо зашифрованные (например, доступ к цифровому следу невозможен без ввода специального ключа).

Цифровые следы, так же, как и традиционные материальные, влекут за собой изменения в элементах вещной обстановки, возникающие в результате механического, химического или иного воздействия. По механизму следообразования они могут быть отнесены к электронным, электромагнитным либо механическим, исходя из чего их следует определять, как материальные, а не виртуальные.

В результате изучения цифровых следов и их видов мы пришли к выводу о том, что они не существуют сами по себе, а всегда содержатся на каких-либо носителях. И поскольку изучение только цифровых следов или только носителей представляется слишком узким, мы полагаем, что эти два компонента образуют единый цифровой объект, который и выступает в качестве объекта экспертного исследования. Так, *цифровой объект – это объект судебно-экспертного исследования, состоящий из цифровых следов разных видов, находящихся на объекте-носителе.* По структуре цифровые объекты делятся на простые и сложные (составные). Отдельным видом цифровых объектов являются цифровые документы.

Экспертное исследование объектов в цифровой форме в современных условиях порождает ошибки, обусловленные различными причинами и условиями. Анализ значения и содержания термина «ошибка» позволил определить экспертную ошибку как неправильное/несоответствующее действительности суждение/действие эксперта, которое в итоге не приводит к поставленной в рамках экспертного исследования цели, при условии, что такое суждение/действие явилось следствием добросовестного заблуждения эксперта в силу различных обстоятельств, связанных с его познавательной деятельностью.

Анализ следственной, судебной и экспертной практики, а также проведенное анкетирование позволили выявить причины и предпосылки трансформации

экспертных ошибок ввиду появления новых цифровых объектов. К ним можно относить следующее:

- замена аналоговых способов собирания и фиксации информации цифровыми (например, цифровая запись звука вытеснила аналоговые способы собирания и исследования звуковых следов). Как следствие – появление новых объектов в цифровой форме требует применения к ним новых подходов, правил и методов исследования. В силу этого эксперты в процессе работе с новыми объектами допускают качественно новые ошибки, которые нуждаются в системном, модифицированном устранении;

- отсутствие апробированной методики, которая отвечала бы задачам экспертизы при исследовании цифровых объектов, а именно:

- неполное исследование цифрового объекта экспертами;

- нехватка у эксперта компетентности для исследования цифрового объекта.

Обобщение экспертной практики свидетельствует, что многие экспертные ошибки возникают вследствие ошибок или небрежного отношения к своим обязанностям правоприменителя, поэтому в рамках диссертации исследовались и следственные ошибки.

В качестве одной из наиболее важных следственных и связанных с ними экспертных ошибок предлагается рассматривать отсутствие расчета хеш-суммы цифрового следа. Со стороны следователя будет ошибкой не рассчитать хеш-сумму цифрового следа, который будет в дальнейшем направлен на исследование эксперту на объекте-носителе. Ошибкой это будет потому, что в случае отсутствия базового описания следа, у эксперта не будет возможности на самом деле проверить достоверность полученного на исследование объекта.

Со стороны эксперта будет ошибкой следующее:

- эксперт получил сведения о хеш-сумме, но не провел самостоятельный расчет показателя, в силу чего нельзя говорить со стопроцентной уверенностью о том, что эксперт исследует ровно то, что ему прислали на экспертизу;

- эксперт не получил никаких сведений о хеш-сумме цифрового следа, находящегося на носителе, однако, он не сделал об этом никакой пометки в ходе своего исследования.

Предлагается нормативное закрепление для следователей положения о необходимости расчета хеш-суммы. По результатам анкетирования были выявлены затруднения у следователей при осуществлении подсчета хеш-суммы, в связи с чем представляется необходимым разработать Инструкцию по ее подсчету для использования следователями. На данном этапе эту ошибку можно именовать гносеологической, при должном нормативном закреплении она трансформируется в процессуальную и приобретет смешанный характер.

Следственные ошибки при назначении экспертизы цифровых объектов могут совершаться на любом этапе расследования и рассмотрения дела, когда допустимо назначение судебной экспертизы, и во время следственных и оперативно-розыскных мероприятий. Они касаются упаковки цифровых объектов, описания упаковки, проведения следственных мероприятий при изъятии и фиксации цифровых следов, осмотра средств вычислительной техники, что свидетельствует о необходимости обязательно привлекать специалиста и др.

Экспертные ошибки при исследовании цифровых объектов связаны с неправильным, неполным описанием упаковки, в которой был получен цифровой объект, недостатками компетенций, использованием в процессе исследования приложений на мобильных устройствах, нелицензионных и не сертифицированных программ. Отдельный пласт ошибок обусловлен неразумным внедрением технологий ИИ в процесс исследования. В частности, при неосторожном использовании технологий ИИ, недостаточно апробированных, не поверенных, не унифицированных, а также чрезмерное полагание на те решения и ответы, которые нейросети предлагают на поставленные задачи, эксперт рискует выработать у себя привычку необдуманно доверять ИИ, не проверяя лично полученные результаты и фактически не решая ничего самостоятельно.

Изучение перечисленных ошибок позволило заключить, что большая их часть обусловлена недостатком компетенций и знаний в области цифровых следов. Поэтому, в качестве мер профилактики предлагается следующее:

- разработать для следователей специальную инструкцию по работе с цифровыми следами, их изъятию, подсчету хеш-суммы;

- разработать для следователей рабочую программу, направленную на приобретение необходимых знаний о цифровых следах, потенциальных ошибках и т.д.;

- организовать для экспертов программы дополнительного профессионального образования;

- разработать для экспертов примерный перечень программ, заслуживающих доверия при исследовании цифровых следов.

В качестве профилактической меры, способной значительно снизить процент совершения экспертами ошибок при использовании ИИ, предлагается разработать в рамках риск-менеджмента экспертных лабораторий направление по изучению рисков при использовании ИИ в экспертных исследованиях. В рамках риск-менеджмента судебно-экспертных лабораторий предлагается следующее:

1) прописать риски, связанные с использованием технологий ИИ в СЭД. Речь идет о недостатках машинного обучения, недостатках самих баз данных ИИ. Обучение системы ИИ возможно при внедрении для этого огромного количества исходных данных – изображений лиц, отпечатков пальцев, шин и др. Для того, чтобы создать хотя бы одну полноценную базу данных, которая может использоваться для одного конкретного вида исследования, необходимо большое количество времени, ресурсов.

2) сформулировать предложения для ликвидации указанных рисков. Нами предлагается разработать критерии допустимости использования ИИ в судебной экспертизе, к которым можно отнести:

- обучение системы ИИ на достаточном количестве сравнительных образцов;

- обучение системы всем известным диагностическим характеристикам, присущим каждому отдельно взятому объекту судебной экспертизы;

- обучение системы «сопутствующим знаниям», которые должны применяться обязательно для формулирования корректного вывода;

- организация участия контрольного лица или группы лиц (экспертов) при отборе образцов для обучения ИИ;

- обучать конкретную систему ИИ только тем характеристикам объектов, с которыми она уже знакома либо разрабатывать для отдельных признаков собственный вектор обучения.

Разработанные по результатам диссертационного исследования меры профилактики экспертных ошибок включают в себя предложения по улучшению качества подготовки будущих следователей и экспертов, а также повышения квалификации уже действующих специалистов, которые могут быть внедрены в практику и позволят сформировать у указанных субъектов специальные знания, умения и навыки по работе с объектами судебных экспертиз в цифровой форме.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Нормативные правовые акты

1. Российская Федерация. Конституция Российской Федерации : принята всенародным голосованием 12 декабря 1993 г.: с изм., одобренными в ходе общероссийского голосования 01 июля 2020 г. 2001 г. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_28399/ (дата обращения: 13.02.2025).

2. Российская Федерация. Законы. Уголовно-процессуальный кодекс Российской Федерации : Федер. закон № 174-ФЗ : принят Государственной Думой 22 ноября 2001 г.: одобрен Советом Федерации 05 декабря 2001 г.: послед. ред. 21.04.2025 г. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_34481/ (дата обращения: 13.02.2025).

3. Российская Федерация. Законы. Уголовный кодекс Российской Федерации : Федер. закон № 63-ФЗ : принят Государственной Думой 24 мая 1996 г.: одобрен Советом Федерации 05 июня 1996 г.: послед. ред. 02.05.2001 г.: послед. ред. 02.05.2025 г. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 13.02.2025).

4. Российская Федерация. Законы. Кодекс Российской Федерации об административных правонарушениях : Федер. Закон № 195-ФЗ : принят Государственной Думой 20 декабря 2001 г.: одобрен Советом Федерации 26 декабря 2011 г.: послед. ред. 07.04.2025 г. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_34661/ (дата обращения: 13.02.2025).

5. Российская Федерация. Законы. Гражданский процессуальный кодекс Российской Федерации : Федер. Закон № 138-ФЗ : принят Государственной Думой 23 октября 2002 г.: одобрен Советом Федерации 30 октября 2002 г.: послед. ред.

01.04.2025 г. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_39570/ (дата обращения: 13.02.2025).

6. Российская Федерация. Законы. Арбитражный процессуальный кодекс Российской Федерации : Федер. Закон № 95-ФЗ : принят Государственной Думой 14 июня 2002 г.: одобрен Советом Федерации 10 июля 2002 г.: послед. ред. 01.04.2025 г. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_37800/ (дата обращения: 13.02.2025).

7. Российская Федерация. Законы. Кодекс административного судопроизводства Российской Федерации : Федер. Закон № 21-ФЗ : принят Государственной Думой 20 февраля 2015 г.: одобрен Советом Федерации 25 февраля 2015 г.: послед. ред. 01.04.2025 г. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_176147/ (дата обращения: 13.02.2025).

8. Российская Федерация. Законы. О государственной судебно-экспертной деятельности в Российской Федерации : Федер. закон № 73-ФЗ : принят Государственной Думой 05 апреля 2001 г.: одобрен Советом Федерации 16 мая 2001 г.: послед. ред. 31.05.2001 г. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_31871/ (дата обращения: 13.02.2025).

9. Российская Федерация. Законы. Об обеспечении единства измерений : Федер. закон № 102-ФЗ : принят Государственной Думой 11 июня 2008 г.: одобрен Советом Федерации 11 июня 2008 г. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_77904/ (дата обращения: 13.02.2025).

10. Российская Федерация. Законы. Об информации, информационных технологиях и о защите информации : Федер. закон № 149-ФЗ : принят Государственной Думой 8 июля 2006 г. : одобрен Советом Федерации 14 июля 2006

г. : послед. ред. // КонсультантПлюс : сайт. URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 13.02.2025).

11. Российская Федерация. Законы. Об электронной подписи : Федер. закон № 63-ФЗ : принят Государственной Думой 25 марта 2011 г.: одобрен Советом Федерации 30 марта 2011 г.: послед. ред. 06.04.2011 г. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_112701/ (дата обращения: 13.02.2025).

12. Российская Федерация. Законы. Об обязательном экземпляре документов : Федер. закон № 77-ФЗ : принят Государственной Думой 23 ноября 1994 г. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_112701/ (дата обращения: 13.02.2025).

13. Российская Федерация. Указы Президента Российской Федерации. О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года : Указ Президента РФ № 204 : принят Президентом РФ 07 мая 2018 г.: послед. ред. 21.07.2020 г. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_297432/ (дата обращения: 13.02.2025).

14. Российская Федерация. Указы Президента Российской Федерации. О национальных целях и стратегических задачах развития Российской Федерации на период до 2030 года и на перспективу до 2036 года : Указ Президента РФ № 309 : принят Президентом РФ 07 мая 2024 г. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_475991/ (дата обращения: 13.02.2025).

15. Российская Федерация. Постановления Пленума Верховного Суда Российской Федерации. О применении части четвертой Гражданского кодекса Российской Федерации : Постановление Пленума ВС РФ № 10 : принято Пленумом ВС РФ 23 апреля 2019 г. // КонсультантПлюс : сайт. URL:

https://www.consultant.ru/document/cons_doc_LAW_323470/ (дата обращения: 13.02.2025).

16. Российская Федерация. Постановления Пленума Верховного Суда Российской Федерации. О некоторых вопросах применения законодательства, регулирующего использование документов в электронном виде в деятельности судов общей юрисдикции и арбитражных судов : Постановление Пленума ВС РФ № 57 : принято Пленумом ВС РФ 26 декабря 2017 г. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_286321/ (дата обращения: 13.02.2025).

17. Российская Федерация. Постановления Пленума Верховного Суда Российской Федерации. О судебной экспертизе по уголовным делам : Постановление Пленума ВС РФ № 28 : принято Пленумом ВС РФ 21 декабря 2010 г.: послед. ред. 29.06.2021 г. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_108437/ (дата обращения: 13.02.2025).

18. Российская Федерация. Постановления Пленума Верховного Суда Российской Федерации. О федеральной целевой программе «Электронная Россия (2002 - 2010 годы) : Постановление Пленума ВС РФ № 65 : принято Пленумом ВС РФ 28 января 2002 г.: послед. ред. 09.06.2010 г. // КонсультантПлюс : сайт. URL: http://consultant.ru/document/cons_doc_LAW_90180/ (дата обращения: 13.02.2025).

19. Российская Федерация. Постановления Правительства Российской Федерации. Об утверждении требований к программному обеспечению, в том числе в составе программно-аппаратных комплексов, используемому органами государственной власти, заказчиками,... : Постановление Правительства РФ № 1478 : принято Правительством РФ 22 августа 2022 г.: послед. ред. 17.10.2023 г. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_425279/92d969e26a4326c5d02fa79b8f9cf4994ee5633b/ (дата обращения: 13.02.2025).

20. Российская Федерация. Постановления Правительства Российской Федерации. О проведении эксперимента по предоставлению права использования программ для электронных вычислительных машин, алгоритмов, баз данных и документации к ним, в том числе исключительное право на которые принадлежит Российской Федерации, на условиях открытой лицензии и созданию условий для использования открытого программного обеспечения : Постановление Правительства РФ № 1804 : принято Правительством РФ 10 октября 2022 г. // Официальное опубликование правовых актов : сайт. URL: http://publication.pravo.gov.ru/Document/View/0001202210120022 (дата обращения: 13.02.2025).

21. Российская Федерация. Постановления Правительства Российской Федерации. О Правительственной комиссии по координации судебно-экспертной деятельности в Российской Федерации» (вместе с «Положением о Правительственной комиссии по координации судебно-экспертной деятельности в Российской Федерации») : Постановление Правительства РФ № 1502 : Утв. постановлением Правительства РФ 8 декабря 2018 г.: послед. ред. 17.07.2019 г. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_313162/7a2c590847c9cbfad23ff1b746f51a027d8e47e9/ (дата обращения: 13.02.2025).

22. Российская Федерация. Распоряжения Правительства Российской Федерации. Об утверждении программы «Цифровая экономика Российской Федерации» : Распоряжение Правительства РФ № 1632-р : принято Правительством РФ 28 июля 2017 г. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_221756/ (дата обращения: 13.02.2025).

23. Российская Федерация. Распоряжения Правительства Российской Федерации. Об утверждении состава Правительственной комиссии по координации судебно-экспертной деятельности в Российской Федерации : Распоряжение Правительства РФ № 1618-р : принято Правительством РФ 20 июля

2019 г. // Официальное опубликование правовых актов : сайт. URL: http://publication.pravo.gov.ru/document/0001201907230021 (дата обращения: 13.02.2025).

Акты технического регулирования

24. ГОСТ Р 7.0.8-2013 «Делопроизводство и архивное дело. Термины и определения». Раздел 3». — Москва : Стандартинформ, 2014. — 16 с.

25. ГОСТ 13699-91 «Запись и воспроизведение информации. Термины и определения». — Москва : Стандартинформ, 2005. — 61 с.

26. ГОСТ Р ИСО/МЭК 19794-5-2013 «Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица». — Москва : Стандартинформ, 2015. — 117 с.

27. ГОСТ Р 34.11-2012. «Информационная технология. Криптографическая защита информации. Функция хеширования» // [Электронный ресурс] URL: http://docs.cntd.ru/document/gost-r-34-11-2012.

28. ГОСТ Р ИСО/МЭК 27037-2014 «Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме». — Москва : Стандартинформ, 2014. — 47 с.

Судебная практика

29. Решение Суда по Интеллектуальным правам от 07.12.2020 № 1027_267512 по делу № СИП-311/2020 // Картотека арбитражных дел «Мой арбитр». — URL: https://goo.su/C4Oa (дата обращения: 03.08.2024 г.).

30. Постановление Десятого Арбитражного апелляционного суда от 25.04.2016 № 10АП-17900/2014. [Электронный ресурс]. — Доступ из справ.-правовой системы «КонсультантПлюс».

31. Определение Верховного Суда Российской Федерации от 22.01.2021 № 306-ЭС20-21597 по делу № А55-23131/2018 // Картотека арбитражных дел «Мой арбитр». — URL: https://goo.su/du2HQ (дата обращения: 30.07.2024 г.).

32. Апелляционное определение Московского городского Суда от 29.11.2017 по делу № 10-15114\17. [Электронный ресурс]. — Доступ из справ.-правовой системы «КонсультантПлюс».

33. Апелляционное определение Московского городского Суда от 28.10.2019 по делу № 10-16047/2019 г. [Электронный ресурс]. — Доступ из справ.-правовой системы «КонсультантПлюс».

34. Приговор Октябрьского районного суда г. Саранска Республики Мордовия от 21.12.2023 № 1-236/2023 г. по делу № 1-236/2023 // Судебные и нормативные акты РФ (СудАкт). — URL: https://sudact.ru/regular/doc/cndyay1eS8UK/?regular-txt=%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%BE%D0%B9+%D1%81%D0%BB%D0%B5%D0%B4&regular-case_doc=&regular-lawchunkinfo=&regular-date_from=&regular-date_to=&regular-workflow_stage=&regular-area=&regular-court=&regular-judge=&snippet_pos=1310#snippet (дата обращения: 30.07.2024 г.).

Монографии, книги, учебники и учебные и научно-практические пособия

35. Аверьянова Т. В., Белкин Р. С., Корухов Ю. Г., Россинская Е. Р. Криминалистика. Учебник для вузов. Изд. 4, переработанное и доп. / Т.В. Аверьянова, Р.С. Белкин, Ю.Г. Корухов, Е.Р. Россинская — М.: Норма; ИНФРА-М, 2013. — 990 с.

36. Аубакирова, А.А. Интеллектуальные ошибки эксперта при формировании его внутреннего убеждения : монография / А.А. Аубакирова. — М. : Юрлитинформ, 2012. — 178 с.

37. Ануфриева, Е.А. Особенности методики предварительного расследования и судебного разбирательства по делам о коррупционных

преступлениях, совершаемых сотрудниками ОВД : монография / Е.А. Ануфриева — Новосибирск: Изд-во НГТУ, 2014. — 239 с.

38. Белкин, Р. С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики / Р. С. Белкин. — М. : Норма : Инфра-М, 2001. — 240 с.

39. Белкин, Р. С. Криминалистика: проблемы, тенденции, перспективы. Общая и частные теории. — М. : Юрид. лит., 1987. — 272 с.

40. Белкин, Р. С. Курс криминалистики: Криминалистические средства, приемы и рекомендации : в 3 т / Р. С. Белкин. — Т. 3. — М. : Юристъ, 1997. — 480 с.

41. Блажеев, В. В., Алтухов, А. В., Андреев, Л. В. Право и общество в эпоху социально-экономических преобразований XXI века: опыт России, ЕС, США и Китая: коллективная монография / Под общей редакцией профессора В. В. Блажеева и профессора М. А. Егоровой — М.: Проспект, 2021. — 604 с.

42. Бобылева, М.П. Управленческий документооборот: от бумажного к электронному: монография / М. А. Бобылева. — М.: ООО «ТЕРМИКА.РУ», 2023. — 426 с.

43. Вехов, В. Б. и др. Цифровая криминалистика: учебник для вузов / В. Б. Вехов; под редакцией В. Б. Вехова, С. В. Зуева. — 2-е изд., перераб. и доп. — Москва: Изда-тельство Юрайт, 2024. — 490 с.

44. Гарнцев, М.А. Проблема самосознания в западноевропейской философии (от Аристотеля до Декарта) : монография / М.А. Гарнцев. — М. : Изд-во МГУ, 1987. — 214 с.

45. Галяшина, Е. И., Голикова, В. В., Дмитриев, Е. Н. и др. Судебная экспертиза: типичные ошибки / Е.И. Галяшина, В.В. Голикова, Е.Н. Дмитриев и др.; под ред. Е.Р. Россинской. — М.: Проспект, 2012. — 301 с.

46. Кудрявцев, В. Н. Генезис преступления. Опыт криминологического моделирования : Учеб. Пособие / В. А. Кудрявцев. — М.: Издательская группа «ФОРУМ–ИНФРА–М», 1998. — 215 с.

47. Кудрявцев, В. Н. Эффективность правосудия и проблема устранения судебных ошибок / под ред. В.Н. Кудрявцева. — М., 1975. — 298 с.

48. Меланич, Е.В. Печати: семь тысяч лет. Профилактика правонарушений : Издание 1-е / Е.В. Меланич. — Москва, 2021. — 201 с.

49. Мещеряков, В.А. Теоретические основы механизма следообразования в цифровой криминалистике: монография / В.А. Мещеряков. — М.: Проспект, 2022. — 176 с.

50. Поль, К.Д. Естественно-научная криминалистика / пер. с нем.; под общ. ред. и со вступ. ст. В.Я. Колдина. / К.Л. Поль. — М.: Юридическая литература, 1985. — 300 с.

51. Россинская Е.Р., Галяшина Е.И. Настольная книга судьи / Е.Р. Россинская, Е.И. Галяшина. — М. : Судебная экспертиза, 2010. — 458 с.

52. Россинская Е.Р., Семикаленова А.И., Рядовский И.А., Сааков Т.А. Теории информационно-компьютерного обеспечения криминалистической деятельности : монография / под. ред. заслуженного деятеля науки РФ, доктора юридических наук, профессора Е.Р. Россинской. — М.: Проспект, 2022. — 256 с.

53. Россинская, Е. Р. Судебная экспертиза: типичные ошибки: 2-е издание, монография / под. ред. Россинской Е.Р. — М.: Проспект, 2024. — 735 с.

54. Россинская, Е. Р., Усов, А. И. Судебная компьютерно-техническая экспертиза : монография / Е. Р. Россинская, А. И. Усов. — М.: Право и закон, 2001. — 416 с.

55. Севастьянов, П. В. Использование цифровых технологий в технико-криминалистическом обеспечении осмотров мест происшествий: Практические рекомендации / П.В. Севастьянов, В.И. Полов, С.В. Томчик и др. — М.: ЭКЦ МВД России, 2022. — 177 с.

56. Штофф, В. А. Моделирование и философия / В. А. Штофф. — М. — Л.: Издательство «Наука», 1966. — 303 с.

Статьи и тезисы докладов

57. Акишин, Д. Г. Особенности подготовки и назначения судебной портретной экспертизы. [Электронный ресурс] URL: http://www.proexpertizu.ru/theory_and_practice/portret/713/?ysclid=lydeludx6k781410013 (дата обращения: 05.07.2024 г.).

58. Аминев, Ф. Г. О проблемах судебно-экспертной деятельности в Российской Федерации и путях их решения / Ф. Г. Аминев // Пробелы в российском законодательстве. Юридический журнал. — 2017. — № 3. — С. 390-393.

59. Балдов, Д. В., Петрова, С. Ю., Лебедев, А. А. Использование технологии блокчейн для защиты данных / Д. В. Балдов, С. Ю. Петрова, А. А. Лебедев // International Journal of Open Information Technologies. — 2021. — № 9. — С. 27-34.

60. Бессонов, А. А. О некоторых возможностях современной криминалистики в работе с электронными следами / А. А. Бессонов // Вестник Университета имени О.Е. Кутафина (МГЮА). — 2019. — №3. — С. 46-52.

61. Боброва, Л.А., Хуэй, Ю. Что такое цифровой объект? / Л. А. Боброва, Ю. Хуэй // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 3, Философия: Реферативный журнал. — 2014. — №3. — С. 380-395.

62. Бодров, Н. Ф., Лебедева, А. К. Понятие дипфейка в российском праве, классификация дипфейков и вопросы их правового регулирования / Н. Ф. Бодров, А. К. Лебедева // Юридические исследования. — 2023. — № 11. — С. 26-41.

63. Бодров, Н. Ф., Лебедева, А. К. Анализ судебной практики установления обстоятельств в случаях противоправного распространения генеративного контента, созданного с помощью технологий ИИ / Н. Ф. Бодров, А. К. Лебедева // Юридические исследования. — 2024. — № 11. — С. 1-25.

64. Буйнов, Д. О. Назначение комплексных судебных экспертиз при исследовании цифровых следов в расследовании экономических преступлений / Д. О. Буйнов // Полицейская деятельность. — 2022. — №4. — С. 20-28.

65. Бушуев, В. В. Экспертные ошибки: причины и профилактика / В. В. Бушуев //Вестник Московского университета МВД России. — 2015. — №3. — С. 23-26.

66. Вехов, В. Б. Электронная криминалистика: понятие и система / В. Б. Вехов // Криминалистика: актуальные вопросы теории и прак-тики: сб. тр. участников Междунар. науч.-практ. конф. Ро-стов н/Д. — 2017. — С. 40-46.

67. Гаврилин, Ю. В. Особенности следообразования при совершении мошенничеств в сфере компьютерной информации / Ю. В. Гаврилин // Российский следователь. — 2013. — № 23. — С. 2-5.

68. Гаврилин, Ю. В. О понятии и содержании государственной научно-технической политики в области криминалистического обеспечения правоохранительной деятельности / Ю. В. Гаврилин // Труды Академии управления МВД России. — 2022. — №2 (62). — С. 96-102.

69. Газизов, В. А., Заварихина, Е. О., Бондаренко, Д. М. 3D-сканирование и совершенствование методов габитоскопических исследований в условиях цифровой трансформации криминалистики / В. А. Газизов, Е. О. Заварихина, Д. М. Бондаренко // Технико-криминалистическое обеспечение раскрытия и расследования преступлений: Сб. науч. трудов. — 2022. — С. 67-77.

70. Гайдаш, О. В. Феномен цифрового следа в современном обществе / О. В. Гайдаш // Вестник магистратуры. — 2020. — №6 (105). — С. 10-12.

71. Галяшина, Е. И. Проблемы использования в доказывании по уголовным делам фонограмм, получаемых по результатам оперативно-розыскных мероприятий / Е. И. Галяшина // Судебная власть и уголовный процесс. — 2018. — №2. — С. 38-47.

72. Галяшина, Е. И. Современные проблемы экспертиз цифровых фонограмм / Е. И. Галяшина // Современные проблемы цифровизации криминалистической и судебно-экспертной деятельности: материалы научно-практической конференции с международным участием. — 2019. — С. 54-61.

73. Галяшина, Е. И. Современные проблемы экспертного исследования звуковых следов / Е. И. Галяшина // Известия Тульского государственного университета. Экономические и юридические науки. — 2013. — № 4-2. — С. 36-42.

74. Галяшина, Е. И. Цифровые фонограммы как доказательства / Е. И. Галяшина // Эксперт-криминалист. — 2008. — № 4. — С. 46-48.

75. Галяшина, Е. И. Об истории судебной фоноскопической экспертизы / Е. И. Галяшина // Вестник Университета имени О. Е. Кутафина. — 2014. — №3. — С. 181-195.

76. Галяшина, Е. И. Судебная фоноскопическая экспертиза: проблемы диагностики аутентичности фонограмм / Е. И. Галяшина // Вестник Университета имени О. Е. Кутафина. — 2014. — №3. — С. 15-26.

77. Грановский, Г. Л. Природа, причины экспертных ошибок и пути их устранения / Г. Л. Грановский // Новые разработки и дискуссионные проблемы теории и практики судебной экспертизы. Экспресс-информация. —1983. — Вып. №2. — С. 2-9.

78. Дронова, О. Б., Кочкин А. В. Доэкспертная оценка вещественных доказательств как средство оптимизации назначения и производства компьютерных экспертиз / О. Б. Дронова, А. В. Кочкин // Судебная экспертиза. — 2025. — № 1. — С.21-31.

79. Дронова, О. Б. Криминалистические аспекты противодействия преступности в цифровом обществе: современные проблемы и перспективы развития / О. Б. Дронова // На страже закона. — 2024. — № 4. — С. 11–16.

80. Дронова, О. Б. Экспертные «ошибки» как способ совершения преступлений / О. Б. Дронова // Экспертные ошибки: современные проблемы возникновения, выявления и профилактики : материалы Международной научно-практической конференции. — Москва : РГ-Пресс, 2024. — С. 52-55.

81. Друки А. А. Системы поиска, выделения и распознавания лиц на изображениях / А. А. Друки // Известия Томского политехнического университета. — 2011. —№ 5. — С. 64-70.

82. Дьяконова, О. Г. Организация профессионального сообщества судебных экспертов на основе судебной экспертологии / О. Г. Дьяконова // Судебная экспертиза. — 2023. — № 1 (73). — С. 8-21.

83. Дьяконова, О. Г. Рецензия специалиста на заключение судебной экспертизы и консультация специалиста: понятие, сущность, нормативное регулирование / О. Г. Дьяконова // Журнал российского права. — 2023. — Том 27. №4. — С. 84-97.

84. Дьяконова, О. Г., Иванова, Е. В. О некоторых функциях руководителя судебно-экспертной организации, связанных с назначением и проведением судебной экспертизы / О. Г. Дьяконова, Е. В. Иванова // Известия Тульского ГУ. Экономические и юридические науки. — 2022. — Вып.2. — С. 27-36.

85. Зинин, А. М. Нейросети и судебно-портретная экспертиз / А. М. Зинин // Вестник криминалистики. — 2020. — № 2 (74). — С. 66-69.

86. Зинин, А. М., Дьяконова, О. Г. Мышление человека и ИИ в аспекте сравнительного исследования внешнего облика человека по его изображениям / А. М. Зинин, О. Г. Дьяконова // Эксперт-криминалист. — 2023. — №3. — С. 2-5.

87. Качук, А. В. Особенности трасологического исследования следов, зафиксированных на цифровых фотоизображениях / А. В. Качук // Право, общество, государство: проблемы истории, теории и практики. Сборник материалов Всероссийской научно-теоретической конференции. Составитель С.Г. Куликова. — 2023. — С. 502-507.

88. Клевно, В. А., Максимов, А. В. К вопросу о классификации и терминологии экспертных ошибок / А. В. Клевно, А. В, Максимов // Судебная медицина. — 2017. — №2. — С. 8-11.

89. Клименко, Н. И. Экспертные ошибки и их причины / Н. И. Клименко /Криминалистика и судебная экспертиза. — 1988. — Вып. 37. — С. 36-39.

90. Курбанаева, Э., Степанова, И., Чепрасов, М. Г. Значение 3D-технологий в науке «Криминалистика» / Э. Курбанаева, И. Степанова, М. Г. Чепрасов // Вестник казахско-русского международного университета. — 2015. — № 4 (13). — С. 92–96.

91. Лапин, Е. С. Вопросы, возникающие при работе с цифровыми следами в ходе расследования преступлений / Е. С. Лапин // Правовая политика и правовая жизнь. — 2021. — №2. — С. 175-180.

92. Лебедев, М. Д., Саввоев, С. А. К вопросу об оптимизации судебно-экспертной деятельности в эпоху цифровизации / М. Л. Лебедев, С. А. Саввоев // Скиф. — 2021. — №3 (55). — С. 41-45.

93. Лебедева, А. К. Особенности судебно-экспертного исследования голоса, измененного при помощи компьютерно-технических средств / А. К. Лебедева // Известия Тульского государственного университета. Экономические и юридические науки. — 2016. — № 3—2. — С. 323-328.

94. Лебедева, А. К. Проблемы производства судебной фоноскопической экспертизы в свете развития цифровых технологий / А. К. Лебедева // Вестник Университета имени О. Е. Кутафина. — 2020. — №6 (70). — С.62-71.

95. Майлис, Н. П. Цифровая трасология: современное состояние и пути решения проблем / Н. П. Майлис // Роль права в обеспечении благополучия человека: сб. докладов XXII Междунар. на- уч.-практ. конф.: в 5 ч. М. — 2022. — Ч. 4. — С. 490-494.

96. Майлис, Н. П. Экспертные ошибки, допускаемые при исследовании традиционных и цифровых следов / Н. П. Майлис // Теория и практика судебной экспертизы. — 2024. — Т. 19. № 1. — С. 20–24.

97. Неретина, Н. С. Взаимосвязь следственных, судебных и экспертных ошибок / Н. С. Неретина // Вестник Университета имени О.Е. Кутафина (МГЮА). —2024. — №3 (115). — С. 99-108.

98. Низаева, С. В. Цифровые следы, виды, перспективы использования в целях раскрытия и расследования преступлений / С. В. Низаева // Государственная служба и кадры. — 2020. — №4. — С. 189-190.

99. Омельянюк, Г. Г., Усов, А. И. Управление рисками в судебно-экспертной деятельности как способ повышения качества экспертного производства / Г. Г. Омельянюк, А. И. Усов // Развитие криминалистики и судебной экспертизы в трудах профессора Е.Р. Россинской: материалы Международной научно-практической конференции, к юбилею ученого, эксперта, педагога. М.: Проспект. — 2019. — С. 337-343.

100. Осипенко, А. Л. Проблемы вовлечения электронно-цифровых следов в уголовный процесс / А. Л. Осипенко // Научный вестник Омской академии МВД России. — 2009. — №4. — С. 31-34.

101. Перепечина, И. О. Экспертные ошибки в контексте профессиональной деятельности экспертов / И. О. Перепечина // Вестник Московского университета МВД России. — 2015. — №3. — С. 34-36.

102. Подволоцкий, И. Н. Использование цифровых технологий в деятельности экспертов / И. Н. Подволоцкий // Вестник криминалистики. — 2023. — № 4. — С. 46-58.

103. Попов, В. А., Рудавин, А. А. Современные особенности технико-криминалистического обеспечения практики работы с цифровыми следами преступлений / В. А. Попов, А. А. Рудавин // в сб.: Технико-криминалистическое обеспечение раскрытия и расследования преступлений. Сб. науч.тр. всеросс. научн.-практ. конф., проводимая в рамках деловой программы Международной выставки средств обеспечения безопасности государства «Интерполитех-2022». — 2022. — С. 181-185.

104. Россинская, Е. Р. К вопросу о частной теории информационно-компьютерного обеспечения криминалистической деятельности / Е. Р. Россинская // Известия ТулГУ. Экономические и юридические науки. — 2016. — Вып. 3, ч. II. — С. 109—117.

105. Россинская, Е. Р. Система теории цифровизации судебно-экспертной деятельности / Е. Р. Россинская // Теория и практика судебной экспертизы. — 2024. — Т. 19. № 3. — С. 20-32.

106. Россинская Е. Р. Теория информационно-компьютерного обеспечения криминалистической деятельности: концепция, система, основные закономерности // Вестник Восточно-Сибирского института МВД России. — 2019. — № 2 (89). — С. 193-202.

107. Россинская, Е. Р., Бодров, Н. Ф. Современное состояние и перспективы исследования образов цифровых следов в судебной почерковедческой экспертизе / Е. Р. Россинская, Н. Ф. Бодров // Криминалистика: вчера, сегодня, завтра. — 2022. — Т. 21. — № 1. — С. 123-135.

108. Россинская, Е. Р. Современное состояние и перспективы цифровизации судебно-экспертной деятельности: материалы Межд. науч.-практ. конф. «Теория и практика судебной экспертизы в современных условиях» (г. Москва, 17-18 января 2019 г.). М.: РГ-Прогресс, 2019.

109. Россинская, Е. Р., Семикаленова, А. И. 2020. Основы учения о криминалистическом исследовании компьютерных средств и систем как часть теории информационно-компьютерного обеспечения криминалистической деятельности / Е. Р. Россинская, А. И. Семикаленова // Вестник Санкт-Петербургского университета. Право 3. — 2020. — Том. 11. №3. — С. 745-759.

110. Ростовцев, А. В. Особенности судебно-экспертного исследования «Цифровых следов» / А. В. Ростовцев // Академическая мысль. — 2019. — №3 (8). — С. 71-73.

111. Сааков, Т. А. Письменные речевые следы, оставленные в цифровой среде, как источник значимой информации о личности неизвестного / Т. А. Сааков // Законы России: опыт, анализ, практика. — 2021. — № 3. — С. 55-59.

112. Савенков, А. Н., Россинская, Е. Р. Вектор развития криминалистической науки в условиях глобальной цифровизации / А. Н. Савенков, Е. Р. Россинская // Государство и право. — 2023. — № 5. — С. 100-110.

113. Савенков, А. Н., Россинская, Е. Р. Актуальные направления развития общей теории криминалистики сквозь призму современных технологий / А. Н. Савенков, Е. Р. Россинская // Государство и право. — 2024. — № 10. — С. 156—168.

114. Саркисян, А. А. Цифровые базы данных в судебно экспертной деятельности / А. А. Саркисян // Вестник Университета имени О. Е. Кутафина. — 2020. — №6 (70). — С. 133-140.

115. Семикаленова, А. И. Проблемы определения потребительской стоимости программного продукта / А. И. Семикаленова // Теория и практика судебной экспертизы. — 2018. — Том 13. № 4. — С. 130-134.

116. Семикаленова, А. И. Судебная компьютерно-техническая экспертиза: проблемы компетенций экспертов / А. И. Семикаленова // Вестник криминалистики. — 2020. — № 2 (74). — С. 70-74.

117. Семикаленова, А. И. Цифровые следы: назначение и производство экспертиз / А. И. Семикаленова // Вестник Университета имени О. Е. Кутафина. — 2019. — №5 (57). — С. 115-120.

118. Ушаков, О. М. Процедура доказывания и «цепь законного владения» / О. М. Ушаков // Право и государство: теория и практика. — 2021. — №12 (204). — С. 271-274.

119. Федотова, В. В., Емельянов, Б. Г., Типнер, Л. М. Понятие блокчейн и возможности его использования / В. В. Федотова, Б. Г. Емельянов, Л. М. Типнер // European science. — 2018. — №1 (33). — С. 40-48.

120. Флеров, О. В. Цифровой след человека в интернете: основные гуманитарные подходы / О. В. Флеров // Образовательные ресурсы и технологии. — 2018. — №4 (25). — С. 79-82.

121. Худяков, В. В., Ананьев, А. А. Цифровые следы / В. В. Худяков, А. А. Ананьев // Криминологический журнал. — 2023. — №4. — С. 243-246.

122. Цветкова, А. Д. Криминалистическое исследование компьютерного (клавиатурного) почерка / А. Д. Цветкова // Электронное приложение к Российскому юридическому журналу. — 2022. — №2. — С. 55-65.

123. Шихалиева С.З. Модификация объективных ошибок судебного эксперта в контексте цифровизации / С. З. Шихалиева // Судебная экспертиза. — 2025. — № 3 (79). — С. 144–152.

124. Шихалиева С.З. Отсутствие хэш-суммы как процессуальная ошибка, возникающая в судебной экспертизе при исследовании объектов в цифровой форме / С. З. Шихалиева // Правовое государство: теория и практика. — 2025. — №1 (79). — С. 256–264.

125. Шихалиева С.З. Проблема определения понятия электронных доказательств: законодательные и судебно-практические аспекты/ С. З. Шихалиева // Российский судья. — 2024. — № 9. — С. 35-39.

126. Шихалиева С.З. Трансформация экспертных ошибок в контексте появления новых цифровых объектов / С. З. Шихалиева // Вестник университета имени О.Е. Кутафина (МГЮА). — 2024. — № 3. — С. 170-175.

127. Яскина, В. Э., Лакеев, П. И., Круглов, Л. М. О некоторых вопросах исследования почерковых объектов, представленных на экспертизу в электронном виде / В. Э. Яскина, П. И. Лакеев, Л. М. Круглов // Теория и практика судебной экспертизы. — 2023. — Т. 18. № 2. — С. 54-61.

Диссертации и авторефераты диссертаций

128. Аубакирова, А. А. Следственные и экспертные ошибки при формировании внутреннего убеждения : дис.... д-ра юрид. наук : 12.00.12 / Аубакирова Анна Александровна. — Челябинск, 2010. — 512 с.

129. Бушуев, В. В. Внутреннее убеждение судебного эксперта в уголовном судопроизводстве : дис. … канд. юрид. наук : 12.00.09 / Виталий Валентинович Бушуев М. . — Москва, 2008. — 201 с.

130. Дьяконова, О. Г. Специальные знания в судебной и иной юрисдикционной деятельности государств-членов ЕАЭС: теория и практика : дис.... д-ра юрид. наук : 12.00.12 / Дьяконова Оксана Геннадьевна. — М., 2021. — 647 с.

131. Краснобаева, А. Ю. Экспертные ошибки: причины, последствия, профилактика : дис. … канд. юрид. наук : 12.00.09 / Анна Юрьевна Краснобаева. — Волгоград, 1997. — 153 с.

132. Мельник, С. Л. Актуальные вопросы экспертной инициативы : дис. … канд. юрид. наук : 12.00.09 / Светлана Львовна Мельник. — Челябинск, 2005. — 287 с.

133. Оконенко, Р.И. «Электронные доказательства» и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ законодательства Соединенных Штатов Америки и Российской Федерации: дис. … канд. юрид. наук : 12.00.09 / Оконенко Роман Иванович. — Москва, 2016. — 158 с.

134. Педенчук, А. К. Заключение судебного эксперта: логика, истинность, достоверность : автореферат дис. ... д-ра юрид.наук. Москва, 1995. 48 с.

135. Полякова, А. В. Формирование и развитие 3D-технологий в судебно-экспертной деятельности: методологические и организационные аспекты : дис. …канд. юрид. наук : 5.1.4 / Полякова Анастасия Васильевна. — Уфа, 2023. — 244 с.

136. Саркисян, А. А. Цифровизация судебно-экспертной деятельности: теоретические, правовые и организационные аспекты : дис ...канд. юрид. наук : 5.1.4 / Саркисян Анна Ашотовна. — М., 2023. — 168 с.

137. Усов, А. И. Концептуальные основы судебной компьютерно-технической экспертизы : дис. ... докт. юрид. наук : 12.00.09 / Александр Иванович. — М., 2002. — 402 с.

138. Чеснокова, Е. В. Концептуальные основы стандартизации в судебно-экспертной деятельности : дис. … д-ра юрид. наук : 12.00.12 / Чеснокова Елена Владимировна. — М., 2022. — 573 с.

139. Рыбин, А. В. Электронный документ как вещественное доказательство по делам о преступлениях в сфере компьютерной информации (процессуальные и криминалистические аспекты: дис. ... докт. юрид. наук : 12.00.09 / Александр Владимирович Рыбин. — Краснодар, 2005. — 192 с.

Справочная и методическая литература

140. Ефремова Т. Ф. Новый словарь русского языка. Толково-словообразовательный. – М.: Русский язык, 2000.

141. Словарь русского языка: В 4-х т. / РАН, Ин-т лингвистич. исследований; Под ред. А. П. Евгеньевой. — 4-е изд., стер. — М.: Рус. яз.; Полиграфресурсы, 1999; (электронная версия): Фундаментальная электронная библиотека.

142. Толковый словарь русского языка [Текст] : 72500 слов и 7500 фразеологических выражений / С. И. Ожегов, Н. Ю. Шведова ; Российская АН, Ин-т рус. яз., Российский фонд культуры. - 2-е изд., испр. и доп. - Москва : Азъ, 1994. — 907.

Интернет-ресурсы

143. 46 инструментов судебной экспертизы информационной безопасности. URL: https://waksoft.susu.ru/2018/01/18/podborka-besplatnyih-utilit-kompyuternoy-kriminalistiki-forenziki/ (дата обращения: 12.01.2025).

144. Все мобильное устройства с функцией ретуши лиц на фото (face retouch). URL: https://sravnismart.ru/camera_extra_functions/face-retouch/ (дата обращения: 05.07.2024).

145. Двоичный код // SkillFactory Media. Словарь IT. URL: https://blog.skillfactory.ru/glossary/dvoichnyy-kod/ (дата обращения: 20.07.2024).

146. Зубов Г.Н. «Я не я, и голос не мой»: О возможностях фальсификации фонограмм с помощью современных технологий синтеза устной речи // Сайт «Праворуб». URL: https://pravorub.ru/personal/78856.html (дата обращения: 12.01.2025).

147. Кафедра судебных экспертиз // Официальный сайт Университета имени О.Е. Кутафина (МГЮА). URL: https://msal.ru/structure/kafedry-obshcheakademicheskie/kafedra-sudebnykh-ekspertiz/?ysclid=mahc6cisv0554799660 (дата обращения: 23.02.2025).

148. Конверт С4 (229х324мм) Security с защитными просечками, стрип. URL: https://www.kanctanta.ru/catalog/9249/41311/ (дата обращения: 25.01.2025).

149. Концепция комплексного регулирования (правового регулирования) отношений, возникающих в связи с развитием цифровой экономики // Некоммерческая организация «Фонд развития центра разработки и коммерциализации новых технологий». URL: https://webcache.googleusercontent.com/search?q=cache:ZUfngxYZ6X0J:https://sk.ru/documents/358/ (дата обращения: 29.07.2024).

150. Мы взяли портреты известных мужчин и сфотографировали их еще раз мобильное устройствоом Huawei Honor 6 Plus с включенной функцией «Украшение // Официальный сайт форума «Пикабу». URL: https://pikabu.ru/story/vstroennoy_funktsiey_retushi_v_smartfonakh_obyichno_polzuyutsya_devushki_interesno_kak_ona_rabotaet_na_sereznyikh_muzhchinakh_3423505#comments (дата обращения: 05.07.2024).

151. Научно-технический энциклопедический словарь. URL: https://rus-scientific-technical.slovaronline.com/?ysclid=mah6lznq5b462907443 (дата обращения: 06.10.2024).

152. Некоммерческое партнерство «Русское общество содействия развитию биометрических технологий, систем и коммуникаций». URL: http://www.rusbiometrics.com/ (дата обращения 06.05.2024).

153. Особенности криминалистической фиксации цифровых доказательств и следов // Официальный сайт «Закон.ру». URL: https://zakon.ru/blog/2022/08/09/osobennosti_kriminalisticheskoj_fiksacii_cifrovyh_dokazatelstv_i_sledov / (дата обращения: 12.01.2025).

154. Почему камера телефона искажает лицо и как это исправить. URL: https://androidinsider.ru/polezno-znat/pochemu-kamera-telefona-iskazhaet-liczo-i-kak-eto-ispravit.html?ysclid=lydgdclnrl936468974 (дата обращения: 05.07.2024 г.).

155. Право.ru: законодательство, судебная система, новости и аналитика // Официальный сайт Право.ru. URL: https://pravo.ru (дата обращения: 01.03.2025).

156. Программа «ВОКОРД» Видеоэксперт. Регистрационный номер в едином реестре российского ПО – 3294. Производитель: ООО «Вокорд Софтлаб» // Сайт «Целевые технологии». URL: http://aimtech.ru/catalog/152 (дата обращения: 21.02.2025).

157. Сейф-пакет – что это такое и где применяется. URL: https://em-pack.ru/sejf-paket-chto-eto-takoe-i-gde-primenyaetsya/ (дата обращения: 17.02.2025).

158. Словарь эксперта // НОЧУ ДПО «Институт СЭиК» [Электронный ресурс]. — URL: https://ceur.ru/library/words/page-132/ (дата обращения: 22.12.2023).

159. Справочник технического переводчика // Интент. 2009-2013. Инженерная переводческая компания. URL: https://intent.gigatran.com/ (дата обращения: 13.11.2024).

160. Судебные и нормативные акты Российской Федерации // Официальный сайт «СудАкт». URL: https://sudact.ru (дата обращения 01.03.2025).

161. Центр по проведению судебных экспертиз и исследований автономная некоммерческая организация «Судебный Эксперт» // Автономная некоммерческая организация «Судебный эксперт» [Электронный ресурс] URL: https://sudexpa.ru/. Дата обращения: 05.01.2024 г. АНО ЭКЦ «Судебная экспертиза». URL: https://ekc-se.ru/fobo_ekspertiza?ysclid=m6nmkxayv3104781557 (дата обращения: 05.01.2024).

162. Цифровой мусор // Словарь «Makves». URL: https://makves.ru/blog/slovar-cifrovoy-musor/ (дата обращения: 26.07.2024).

163. Экспертные системы и шумоочистка Икар Лаб 3 // Группа компаний «ЦРТ». URL: https://www.speechpro.ru/product/ekspertnye-sistemy-i-shumoochistka/ (дата обращения: 12.01.2025).

164. Энциклопедия «Касперского». URL: https://encyclopedia.kaspersky.ru/glossary/hash/?ysclid=m5crbl0myp242650144 / (дата обращения: 12.01.2025).

165. Digital object // Archives Terminology. URL: https://dictionary.archivists.org/entry/digital-object.html (дата обращения: 26.07.2024 г.).

166. Why Hash Values Are Crucial in Digital Evidence Authentication // Pagefreezer Blog. URL: https://blog.pagefreezer.com/importance-hash-values-evidence-collection-digital-forensics#fre902 (дата обращения: 11.12.2024).

167. Forensic Science Regulator code of practice // Gov.UK. URL: https://www.gov.uk/government/publications/forensic-science-regulator-code-of-practice (дата обращения: 26.12.2024).

168. Federal Rules of Evidence. URL: https://www.rulesofevidence.org/fre/article-ix/rule-902/ (дата обращения: 12.01.2025).

169. Nakamoto S. Bitcoin: a peer-to-peer electronic cash system // Bitcoin.org. URL: https://bitcoin.org/bitcoin.pdf (дата обращения: 01.01.2025).

170. Voice spoofing detector: A unified anti-spoofing framework. / Ali Javed, Khalid Mahmood Malik, Hafiz Malik, Aun Irtaza. // Expert Systems with Applications. – 2022. – №198 (8): 116770. URL: https://www.sciencedirect.com/science/article/abs/pii/S0957417422002330 (дата обращения: 12.01.2025).

Приложение 1. Общий вид анкеты для сотрудников следственных и судебных органов по вопросам, связанным с назначением экспертизы цифровых следов

АНКЕТА

Анкета создана в целях выяснения мнений следователей и судей по вопросам назначения судебных экспертиз цифровых следов.

Цифровой след - это криминалистически значимая компьютерная информация о событиях или действиях, отраженная в материальной среде в процессе её возникновения, обработки, хранения и передачи. Цифровым следом выступают, например, фото-, видео-, аудиофайлы, скриншоты и т.д.

Опрос проводится анонимно в научных целях.

Благодарим за сотрудничество!

1. Укажите Вашу должность*

- Следователь
- Судья

2. Приходилось ли Вам назначать судебные экспертизы цифровых следов? Если да, как часто?

_____

3. Считаете ли Вы необходимым предпринимать меры по защите содержания цифрового следа от изменений?

- Да
- Нет

4. Каким образом Вы обеспечиваете защиту от изменения содержания цифрового следа при назначении экспертизы? (если соответствующие меры не осуществляются, поставьте прочерк)

_____

5. Знаете ли Вы, что такое "хеш-сумма"?

- Да
- Нет

6. Считаете ли Вы подсчёт хеш-суммы файла надёжным способом защиты содержания цифрового следа? ***Хеш-сумма (хеш) — это уникальный цифровой***

отпечаток, который можно присвоить любому файлу. Ключевой смысл хеш-функции — убедиться, что данные нельзя изменить или подделать.

- Да
- Нет

7. Осуществляете ли Вы подсчёт хеш-суммы файла при назначении экспертизы цифрового следа?

- Да
- Нет

8. Что является причиной отрицательного ответа на предыдущий вопрос?

- Не считаю это необходимым
- Подсчёт хеш-суммы файла занимает много времени
- Не умею считать хеш-сумму файла
- Не знаю, правильно ли я осуществил подсчёт
- Ответ положительный
- Другое _____

9. Будет ли для Вас актуальным и полезным получить инструкцию по подсчёту хеш-суммы файла?

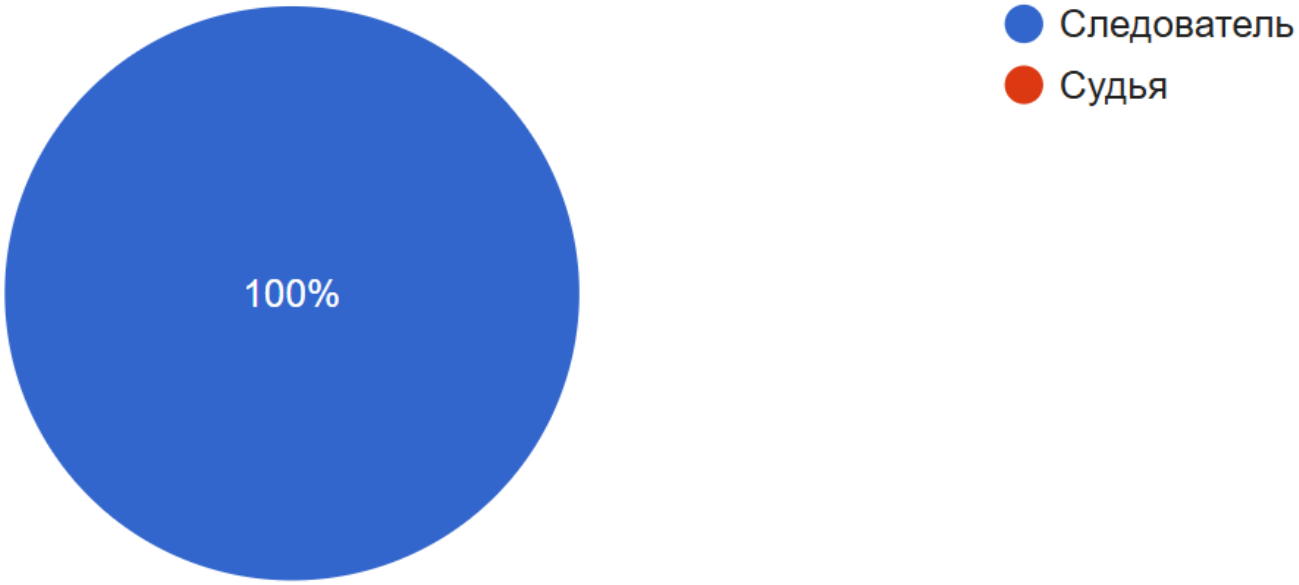
- Да
- Нет

10. Как Вы считаете, необходима ли эксперту дополнительная квалификация (помимо основной) в области судебной компьютерно-технической экспертизы для работы с цифровыми следами? Укажите, в каких случаях.

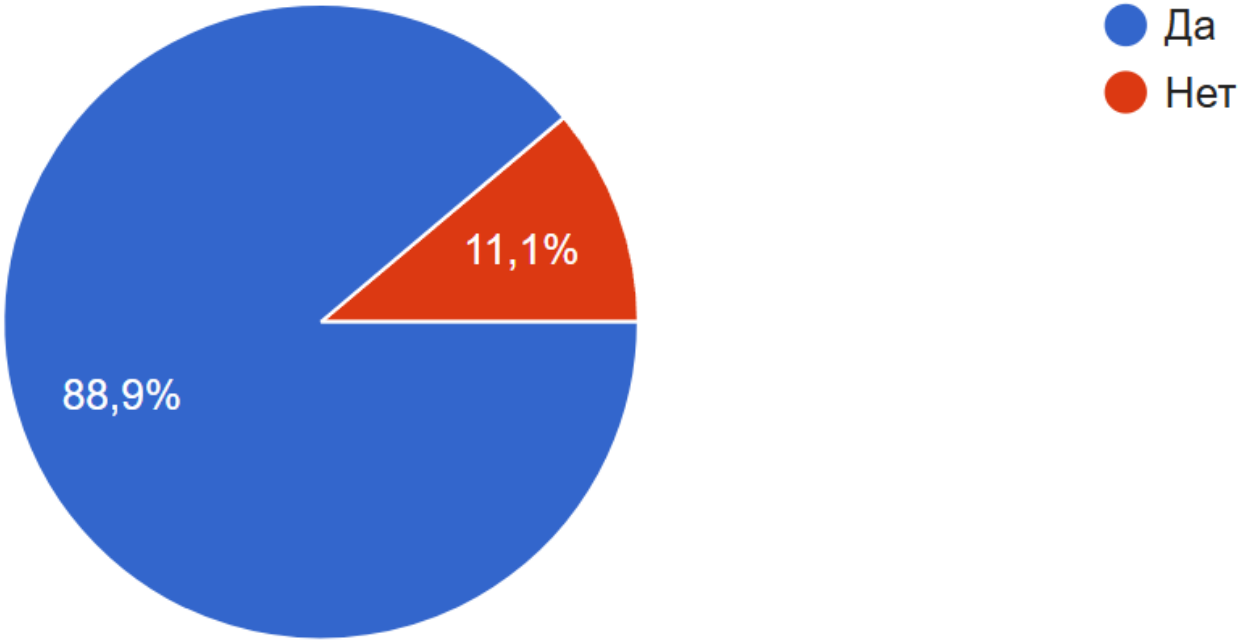
_____

Приложение 2. Результаты опроса сотрудников следственных и судебных органов по вопросам, связанным с назначением экспертизы цифровых следов

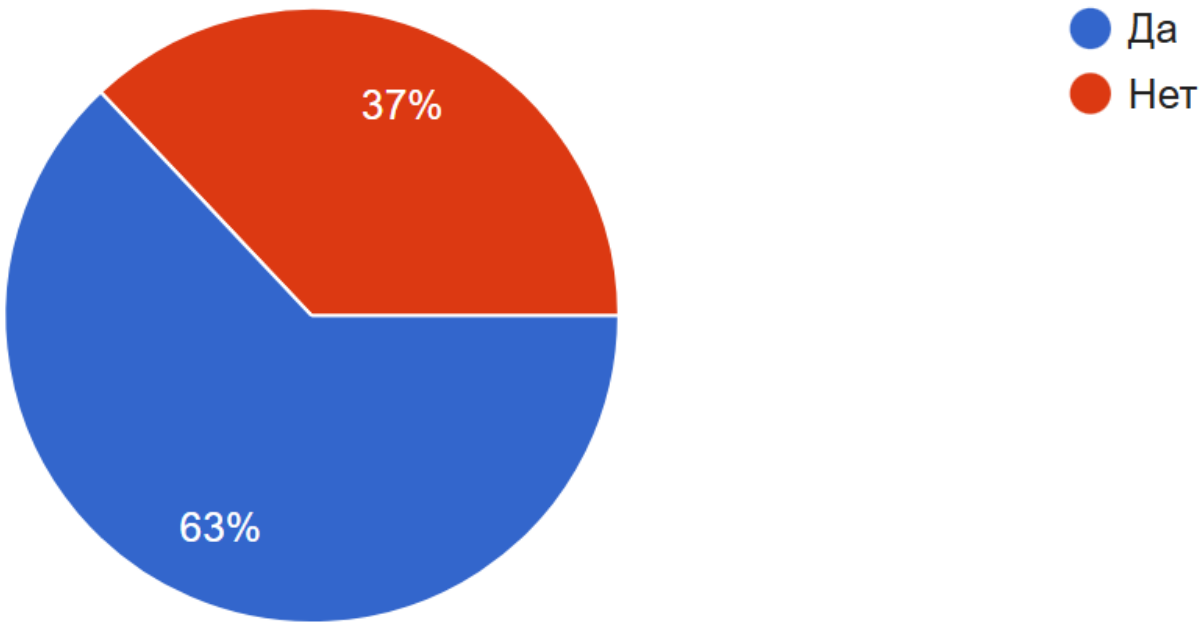
Укажите Вашу должность



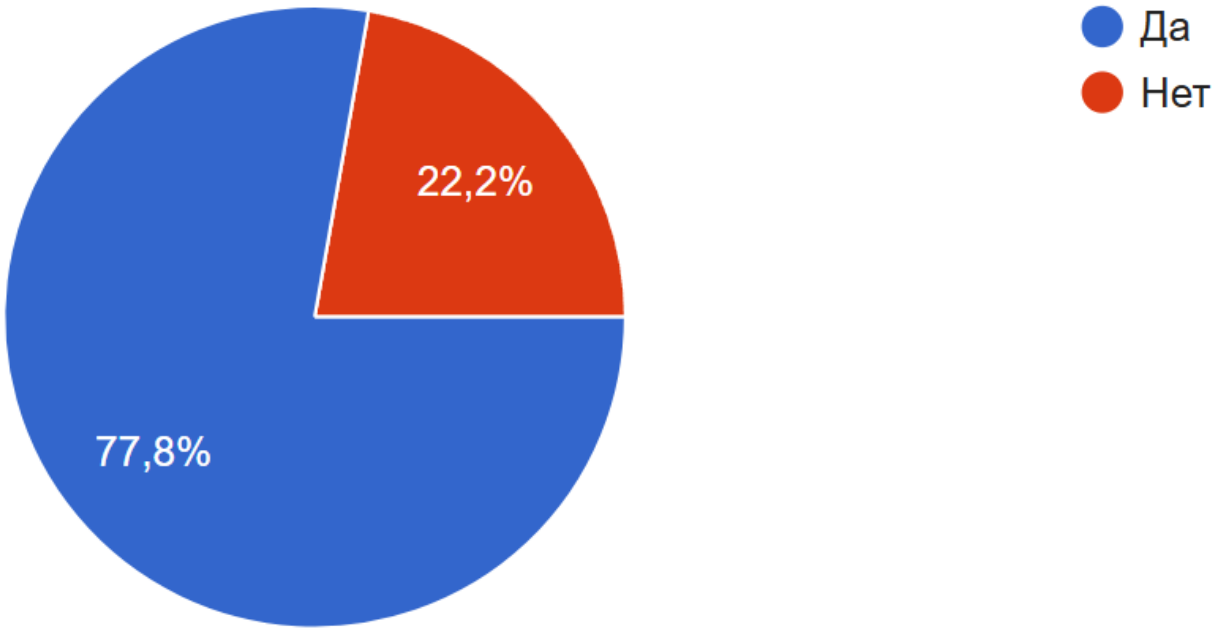
Считаете ли Вы необходимым предпринимать меры по защите содержания цифрового следа от изменений?



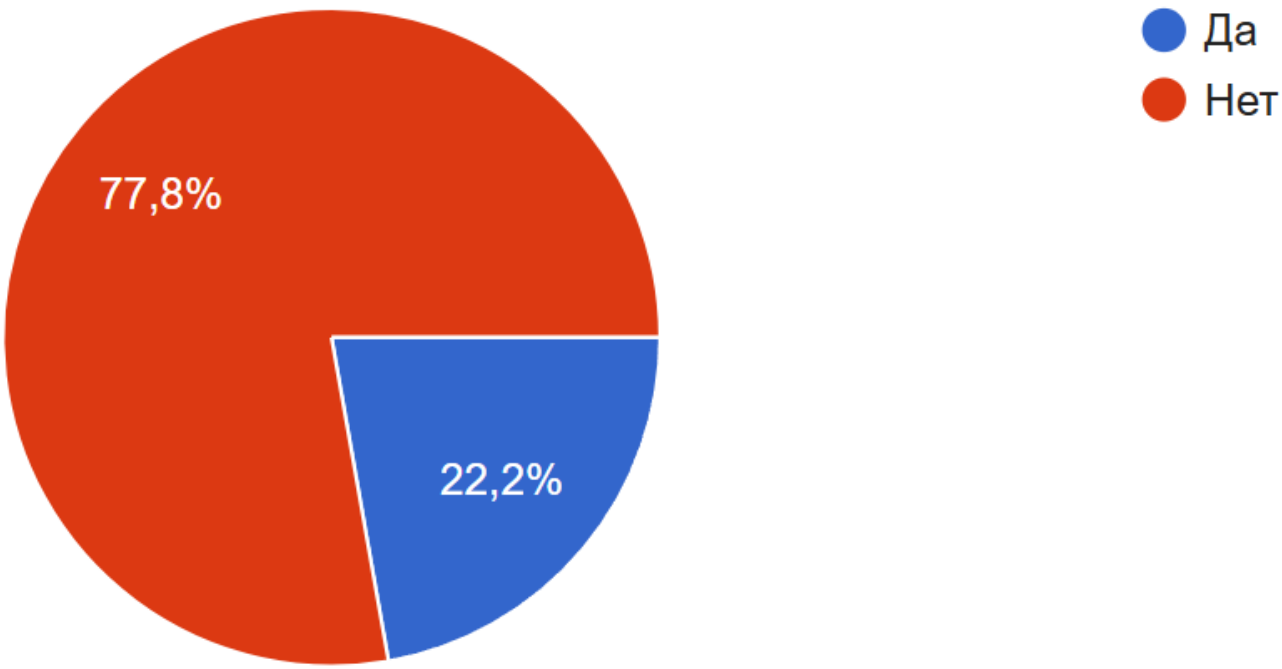
Знаете ли Вы, что такое "хеш-сумма"?



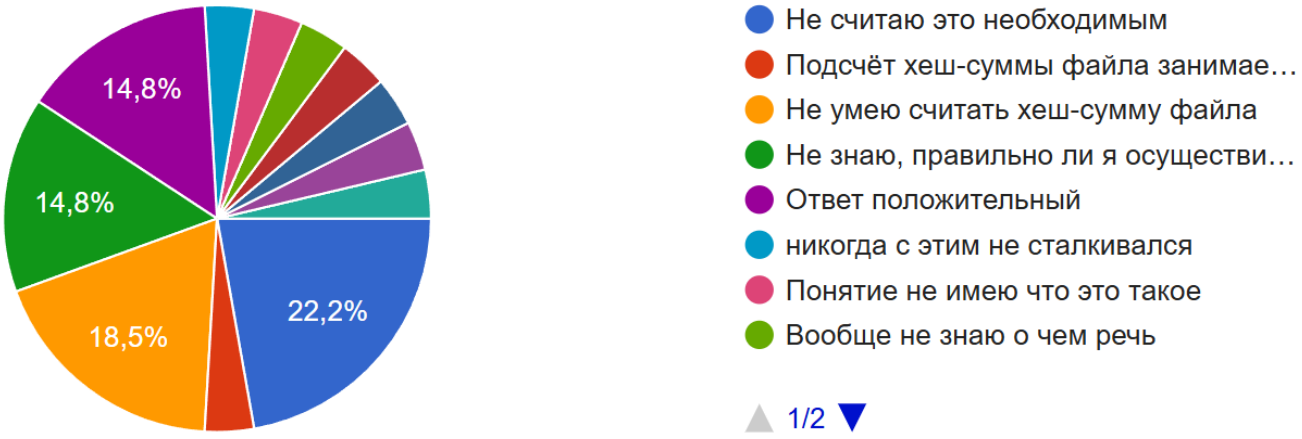
Считаете ли Вы подсчёт хеш-суммы файла надёжным способом защиты содержания цифрового следа?



Осуществляете ли Вы подсчёт хеш-суммы файла при назначении экспертизы цифрового следа?



Что является причиной отрицательного ответа на предыдущий вопрос?



Приложение 3. Общий вид анкеты для государственных, негосударственных и частных судебных экспертов по вопросам, связанным с производством судебных экспертиз цифровых следов

АНКЕТА

Анкета создана в целях выяснения мнений судебных экспертов по вопросам исследования цифровых следов, а также программного обеспечения.
Цифровой след - это криминалистически значимая компьютерная информация о событиях или действиях, отраженная в материальной среде в процессе её возникновения, обработки, хранения и передачи. Цифровым следом выступают, например, фото-, видео-, аудиофайлы, скриншоты и т.д.
Опрос проводится анонимно в научных целях.
Благодарим за сотрудничество!

1. Укажите Вашу экспертную специальность

_____

2. Вы…

- Эксперт - сотрудник государственного СЭУ
- Эксперт - сотрудник частной судебно-экспертной организации
- Эксперт - сотрудник неэкспертной организации
- Частный эксперт (не являющийся сотрудником организации)
- Ученый-исследователь, преподаватель (судебная экспертология, криминалистика)

3. Приходилось ли Вам принимать к производству судебную экспертизу цифровых следов? Если да, как часто?

_____

4. Считаете ли Вы необходимым предпринимать меры по защите содержания цифрового следа от изменений?

- Да
- Нет

5. На Ваш взгляд, каким образом должна обеспечиваться защита от изменения первоначального содержания цифрового файла при назначении экспертизы? Какие способы защиты Вам известны?

_____

6. Знаете ли Вы, что такое "хеш-сумма"?

- Да
- Нет

7. Считаете ли Вы подсчёт хеш-суммы файла надёжным способом защиты содержания цифрового следа? ***Хеш-сумма (хеш) — это уникальный цифровой отпечаток, который можно присвоить любому файлу. Ключевой смысл хеш-функции — убедиться, что данные нельзя изменить или подделать.***

- Да
- Нет

8. Осуществляете ли Вы подсчёт хеш-суммы файла при производстве экспертизы цифрового следа?

- Да
- Нет

9. Что является причиной отрицательного ответа на предыдущий вопрос?

- Не считаю это необходимым
- Подсчёт хеш-суммы файла занимает много времени
- Не умею считать хеш-сумму файла
- Не знаю, правильно ли я осуществил подсчёт
- Ответ положительный
- Другое _____

10. Будет ли для Вас актуальным и полезным получить инструкцию по подсчёту хеш-суммы файла?

- Да
- Нет

11. Как Вы считаете, необходима ли эксперту дополнительная квалификация (помимо основной) в области судебной компьютерно-технической экспертизы для работы с цифровыми следами? Укажите, в каких случаях.

_____

12. Знаете ли Вы, что такое блокчейн? Считаете ли Вы создание блокчейна хорошим способом защиты содержания цифрового следа от изменений?

_____

13. На Ваш взгляд, каким критериям должно соответствовать программное обеспечение судебного эксперта?

_____

14. По Вашему мнению, возможно ли создание единого, установленного ГОСТ перечня программ, необходимых судебному эксперту для работы с цифровым объектом? Свой ответ обоснуйте.

_____

15. Какие потенциальные ошибки может допустить эксперт при исследовании цифровых объектов?

_____

16. Допускались ли Вами экспертные ошибки при исследовании объектов такого рода? Если да, расскажите о них подробнее.

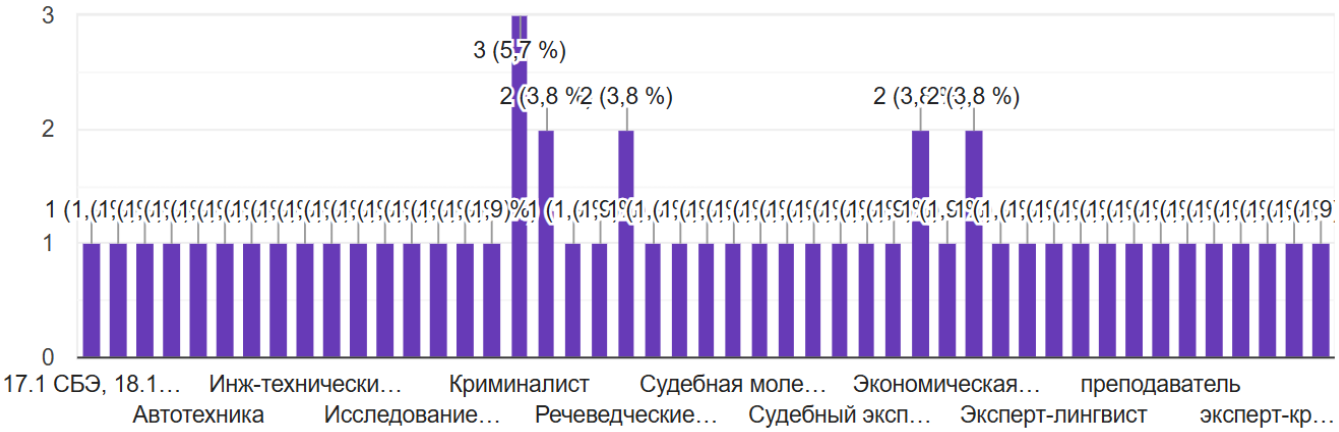
_____

17. Считаете ли Вы необходимым получение знаний по работе с цифровыми следами:

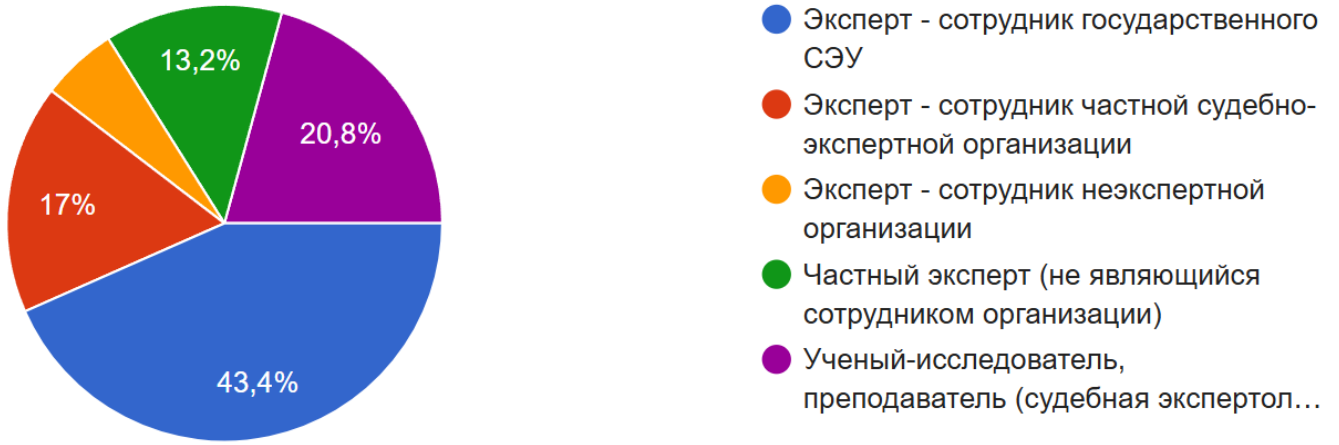
- Посредством прохождения программы дополнительного образования по работе с цифровыми объектами
- В рамках повышения квалификации по своей экспертной специальности
- Другое _____

Приложение 4. Примеры ответов на вопросы из анкеты для государственных, негосударственных и частных судебных экспертов по вопросам, связанным с производством судебных экспертиз цифровых следов

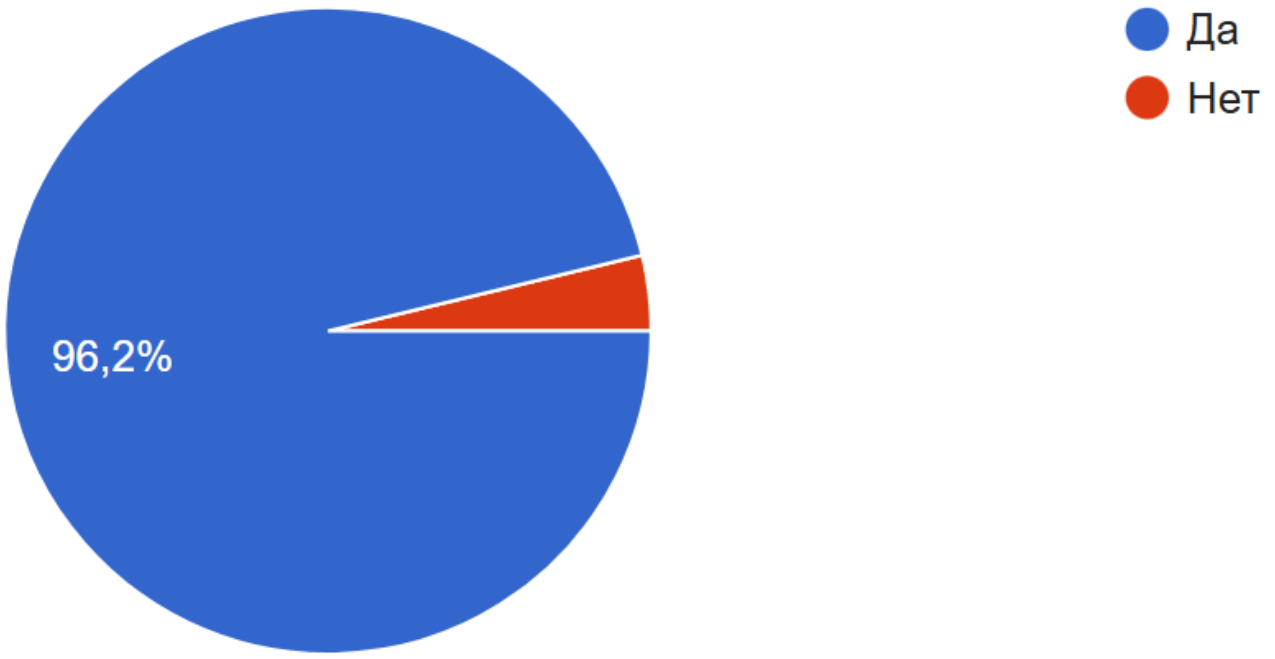
Укажите Вашу экспертную специальность



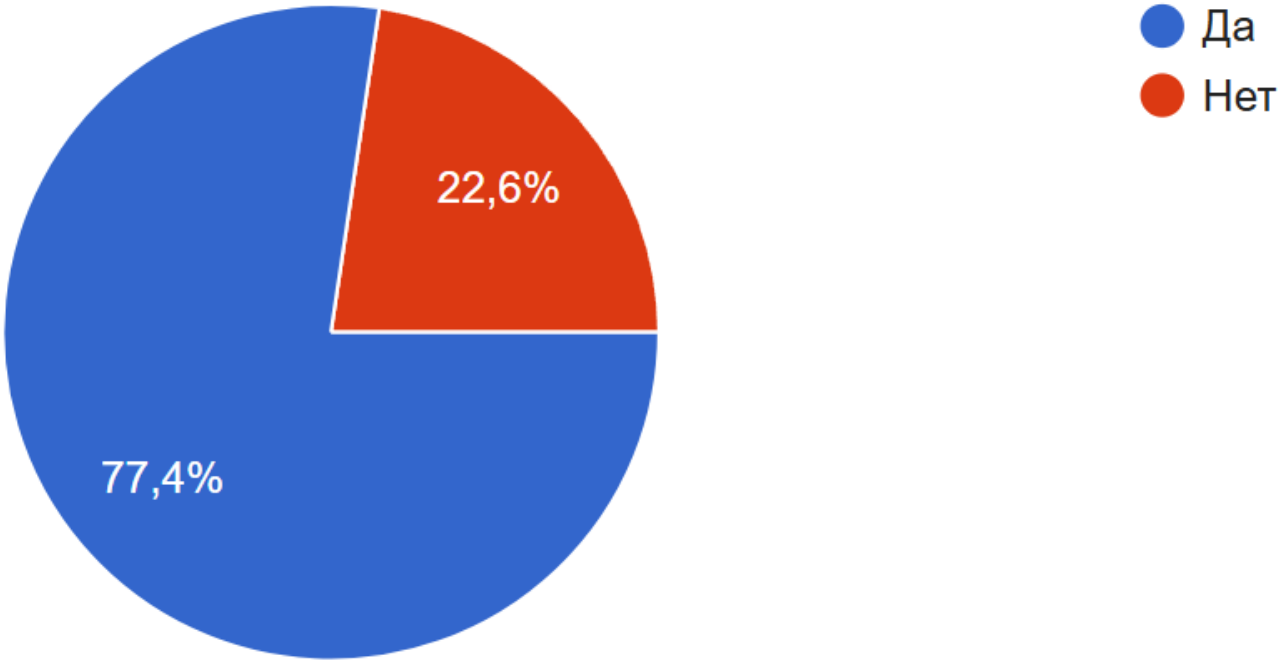
Вы…



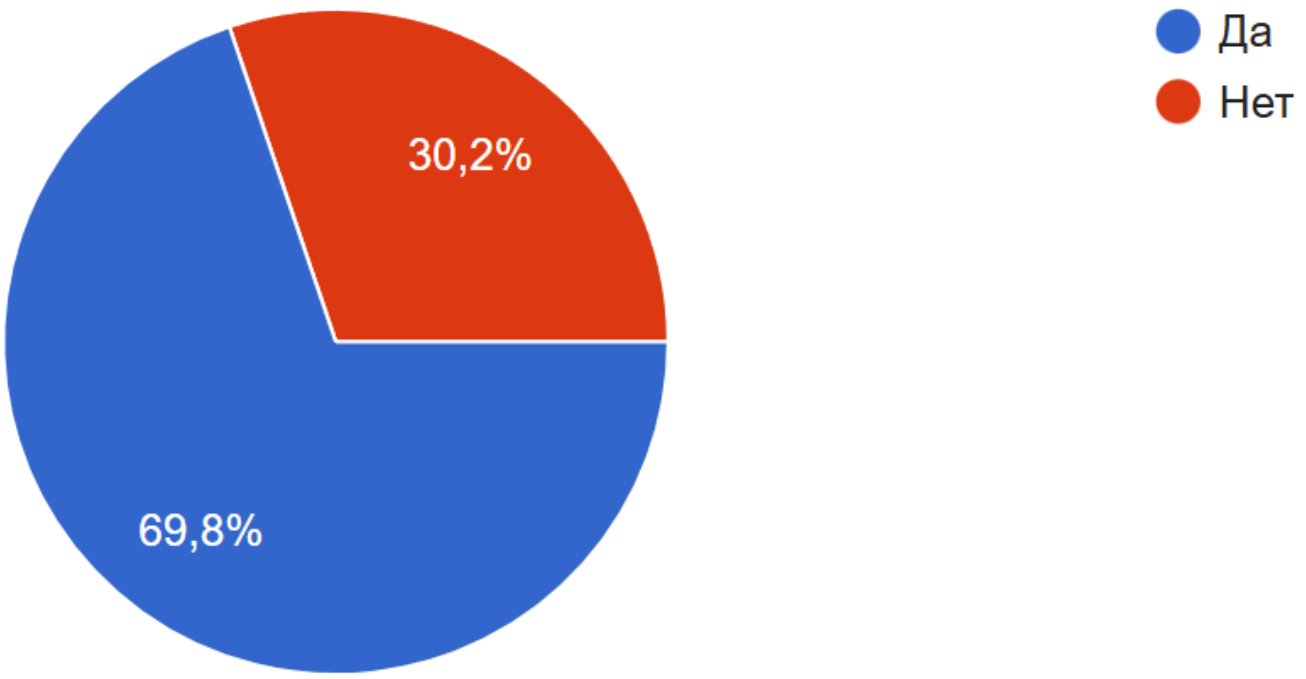
Считаете ли Вы необходимым предпринимать меры по защите содержания цифрового следа от изменений?



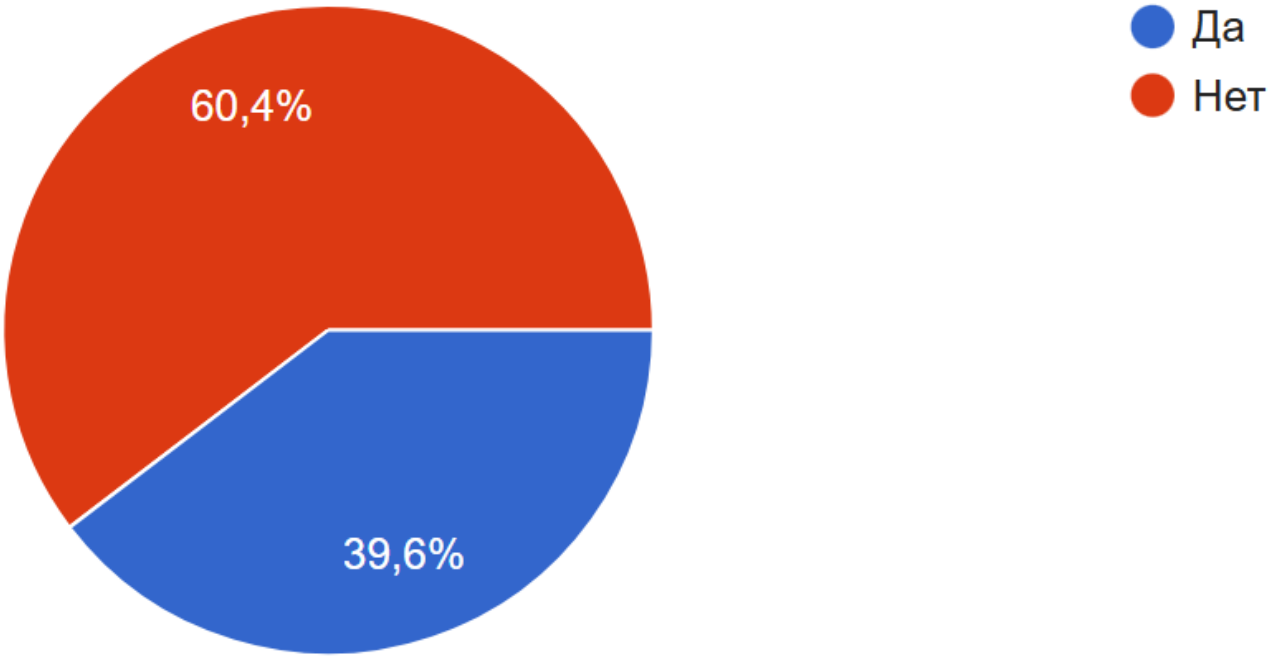
Знаете ли Вы, что такое «хеш-сумма»?



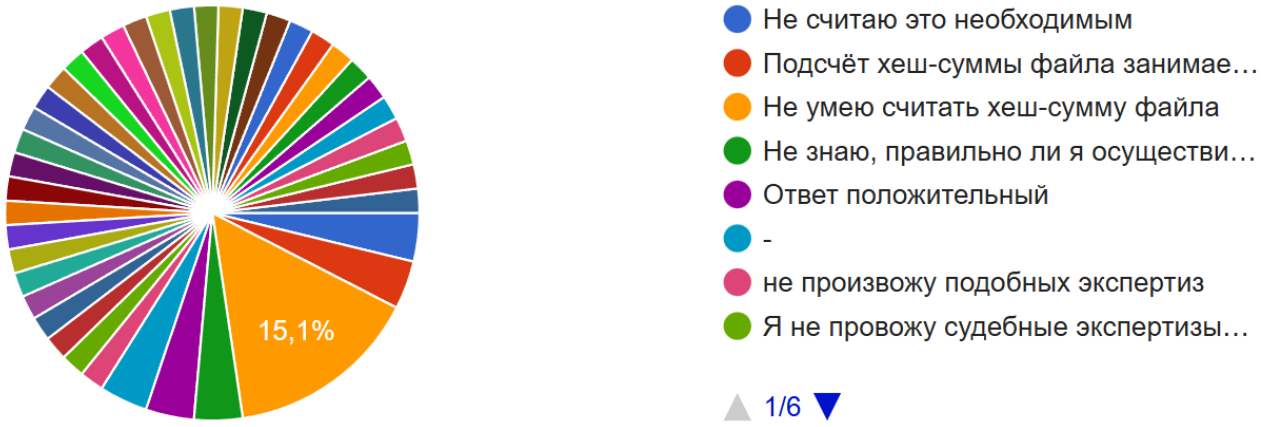
Считаете ли Вы подсчёт хеш-суммы файла надёжным способом защиты содержания цифрового следа?



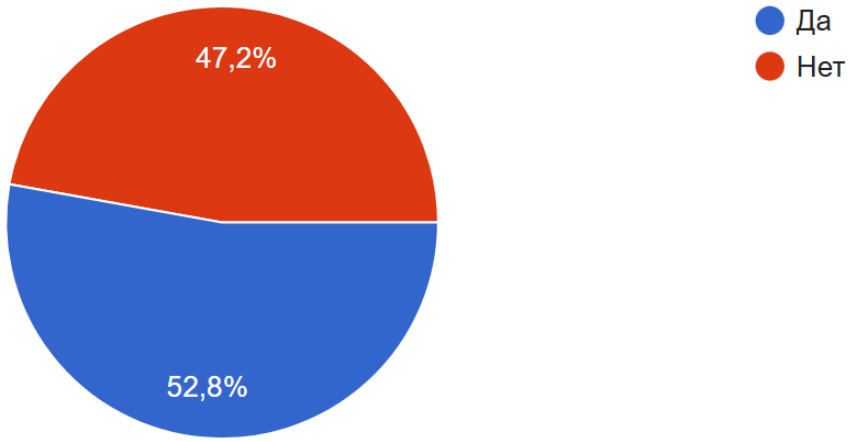
Осуществляете ли Вы подсчёт хеш-суммы файла при производстве экспертизы цифрового следа?



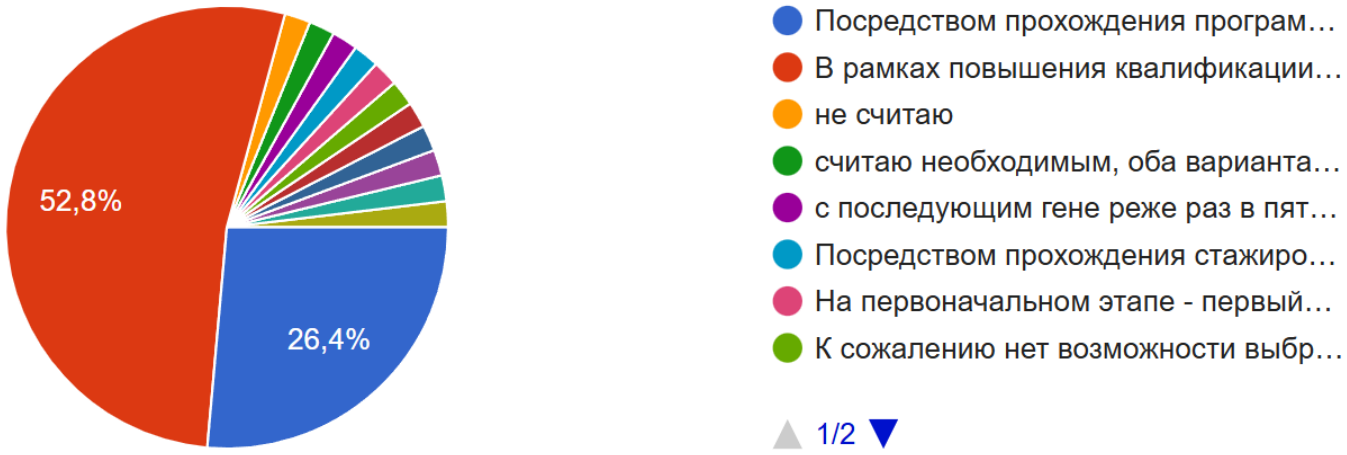
Что является причиной отрицательного ответа на предыдущий вопрос?



Будет ли для Вас актуальным и полезным получить инструкцию по подсчёту хеш-суммы файла?



Считаете ли Вы необходимым получение знаний по работе с цифровыми следами:



Приложение 5. Макет рабочей программы для следователей, направленной на приобретение знаний и навыков, необходимых для расследования преступлений в цифровой среде

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ЮРИДИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ О.Е. КУТАФИНА (МГЮА)»

Кафедра судебных экспертиз

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ИСПОЛЬЗОВАНИЕ СПЕЦИАЛЬНЫХ ЗНАНИЙ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В ЦИФРОВОЙ СРЕДЕ

Б1.В.ДВ.02

год набора – 20XX

Код и наименование направления подготовки/специальности:	40.04.01 Юриспруденция
Уровень высшего образования:	специалитет
Направленность (профиль) ОПОП ВО	юриспруденция
специализация ОПОП ВО:	следственная деятельность
Форма (формы) обучения:	очная
Квалификация:	юрист

Москва – 2025

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Цели и задачи освоения дисциплины (модуля)

Целью изучения учебной дисциплины *«Использование специальных знаний при расследовании преступлений в цифровой среде»* является получение обучающимися теоретических знаний и практических навыков об использовании специальных знаний при расследовании преступлений в цифровой среде, формирование компетенций в области борьбы с киберпреступностью и других направлений обеспечения законности в киберпространстве, компетенций в области использования современных IT-технологий, понимание основных категорий и положений цифровизации следственной и судебно-экспертной деятельности, основных представлений о цифровых следах, их материальной сущности, технологической природе, механизме формирования, правил проведения следственных действий при работе с цифровыми следами, а также возможных ошибок, которые могут возникнуть при неправильном выявлении, фиксации и изъятии таких объектов.

Задачей **изучения учебной дисциплины *«Использование специальных знаний при расследовании преступлений в цифровой среде»*** является формирование умения обучающегося на основе приобретенных во время изучения дисциплины знаний – использовать специальные знания для эффективного расследования преступлений в цифровой среде, а также взаимодействия с судебным экспертом и специалистом.

1.2. Место дисциплины (модуля) в структуре ОПОП ВО

Дисциплина (модуль) *«Использование специальных знаний при расследовании преступлений в цифровой среде»* относится *к части, формируемой участниками образовательных отношений основной профессиональной образовательной программы высшего образования.*

Освоение дисциплины дает возможность расширения и углубления знаний, полученных на предшествующем этапе обучения, приобретения умений и навыков, определяемых содержанием программы. Компетенции, которые формируются в процессе освоения дисциплины, необходимы для успешной профессиональной деятельности. Обучающиеся приобретают способность самостоятельно находить и использовать необходимые содержательно-логические связи с другими дисциплинами программы, такими как, *«Уголовно-процессуальное право (Уголовный процесс)», «Гражданское процессуальное право (Гражданский процесс)», «Криминалистика», «Криминология»*, «*Экспертиза в судопроизводстве*» и другими.

1.3. Формируемые компетенции и индикаторы их достижения (планируемые результаты освоения дисциплины (модуля))

По итогам освоения дисциплины (модуля) обучающийся должен обладать следующими компетенциями (*из матрицы компетенций*) в соответствии с ФГОС ВО:

Общепрофессиональные компетенции:

ОПК-10 – Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности

Разделы (темы) дисциплины (модуля)	Код и наименование формируемых компетенций	Индикатор достижения компетенций (планируемый результат освоения дисциплины (модуля))
Концепция цифровых следов в криминалистике и судебной экспертологии	ОПК-10 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ИОПК 10.1 Понимает принципы работы современных информационных технологий ИОПК 10.2 Умеет выбрать современные информационные технологии, необходимые для решения конкретных задач профессиональной деятельности ИОПК 10.3 Владеет навыками использования современных информационных технологий, необходимыми для решения конкретных задач профессиональной деятельности
Классификации цифровых следов	ОПК-10 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ИОПК 10.1 Понимает принципы работы современных информационных технологий ИОПК 10.2 Умеет выбрать современные информационные технологии, необходимые для решения конкретных задач профессиональной деятельности ИОПК 10.3 Владеет навыками использования современных информационных технологий, необходимыми для решения конкретных задач профессиональной деятельности
Участие специалиста при производстве следственных и судебных действий при расследовании преступлений и судебном	ОПК-4 Способен участвовать в экспертной	ИОПК 4.1 Понимает сущность и значение экспертной юридической деятельности ИОПК 4.2 Умеет формулировать экспертные задачи, понимает особенности

рассмотрении дел в цифровой среде	юридической деятельности	использования экспертного заключения в судебной и прокурорской деятельности ИОПК 4.3 Принимает участие в проведении правовой экспертизы нормативных правовых актов и актов применения норм права, а также их проектов
Цифровые следы в судебных экспертизах	ОПК-10 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ИОПК 10.1 Понимает принципы работы современных информационных технологий ИОПК 10.2 Умеет выбрать современные информационные технологии, необходимые для решения конкретных задач профессиональной деятельности ИОПК 10.3 Владеет навыками использования современных информационных технологий, необходимыми для решения конкретных задач профессиональной деятельности
Оценка и использование экспертиз с цифровыми следами, консультации специалиста	ОПК-4 Способен участвовать в экспертной юридической деятельности	ИОПК 4.1 Понимает сущность и значение экспертной юридической деятельности ИОПК 4.2 Умеет формулировать экспертные задачи, понимает особенности использования экспертного заключения в судебной и прокурорской деятельности ИОПК 4.3 Принимает участие в проведении правовой экспертизы нормативных правовых актов и актов применения норм права, а также их проектов

В результате освоения дисциплины (модуля) обучающийся должен:

В результате обучения по программе слушатели должны

знать:

– понятие и сущность специальных знаний;

– современные IT-технологии в профессиональной сфере;

– понятие и сущность цифровых следов, механизма их формирования;

– классификации цифровых следов в криминалистике и судебной экспертологии;

– особенности собирания цифровых следов при производстве следственных действий;

– наиболее распространенные виды следственных ошибок при выявлении, изъятии и фиксации цифровых следов при производстве следственных действий;

уметь:

– применять полученные знания и навыки при решении задач, которые возникают перед следователями при проведении следственных действий, связанных с цифровыми следами;

– пользоваться помощью специалиста и эксперта при проведении следственных действий при расследовании преступлений в цифровой среде;

– осуществлять выбор методов и средств, специфичных для работы с цифровыми следами и объектами при их выявлении, изъятии и фиксации;

владеть:

– навыками постановки вопросов перед экспертами и специалистами;

– навыками использования специальных знаний для проведения следственных действий и расследования преступлений в цифровой среде;

– навыками подготовки материалов, направляемых для производства судебных экспертиз при расследовании преступлений в цифровой среде.

2.1.1. Тематический план для очной формы обучения

№ п/п	Разделы (темы) дисциплины (модуля)	семестр/триместр	Технология образовательного процесса			Форма текущего контроля/ Форма промежуточной аттестации	
			лекции	ПЗ	СР		
1	Цифровые следы в криминалистике и судебной экспертологии: понятие и виды		2	2	4	*Управляемая дискуссия, метод публичных выступлений, презентации*	*Контрольные задания*
2	Участие специалиста в процессуальных действиях в целях обеспечения процесса доказывания в условиях цифровизации		2	4	10	*Управляемая дискуссия, метод публичных выступлений, презентации*	*Контрольные задания*
3	Частная теория цифровизации судебно-		2	2	6	*Управляемая дискуссия, метод публичных*	*контрольные задания*

	экспертной деятельности					*выступлений, презентации*	
4	Объекты судебных экспертиз в цифровой форме		2	6	10	*Управляемая дискуссия, метод публичных выступлений, презентации*	*контрольные задания*
5	Следственные ошибки, возникающие при неправильной работе с объектами в цифровой форме и пути их предотвращения		4	6	10	*Управляемая дискуссия, публичных выступлений, презентации, кейс-метод*	*контрольные задания*
	Всего по ОФО		**10**	**20**	**40**	**Зачет**	

Содержание дисциплины (модуля)

2.2.1. Занятия лекционного типа для очной формы обучения

Лекция 1. Тема 1. Концепция цифровых следов в криминалистике и судебной экспертологии. Классификации цифровых следов. 2 часа.

Содержание:

1. Понятие цифровых следов в криминалистике и судебной экспертологии, цифровые следы.
2. Материальная сущность цифровых следов, технологическая природа и механизмы формирования цифровых следов.
3. Свойства цифровых следов.
4. Виды и формы цифровых следов.
5. Цифровые следы как результат противоправного использования вредоносных программ.
6. Контрафактные информационно-компьютерные продукты как цифровые следы.
7. Классификация носителей цифровых следов.

Задание для подготовки:

Изучить нормативные правовые источники, а также рекомендованную основную и дополнительную литературу.

Лекция 2. Тема 2. Участие специалиста в процессуальных действиях в целях обеспечения процесса доказывания в условиях цифровизации. 2 часа.

Содержание:

1. Процессуальный статус специалиста в уголовном судопроизводстве. Требования, предъявляемые к специалисту, как участнику судопроизводства.
2. Принципы взаимодействия специалиста со следователем. Обязательность привлечения специалиста при работе с цифровыми следами.
3. Выбор специалиста и оценка его компетентности при расследовании преступлений в цифровой среде.
4. Участие специалиста в производстве процессуальных действий: осмотр места происшествия, обыск, выемка и т.д. при расследовании преступлений в цифровой среде.
5. Основные правила выявления, изъятия и фиксации цифровых следов.

Задание для подготовки:

Изучить нормативные правовые источники, а также рекомендованную основную и дополнительную литературу.

Лекция 3. Тема 3. Частная теория цифровизации судебно-экспертной деятельности. 2 часа.

Содержание:

1. Генезис информационно-компьютерного обеспечения судебной экспертизы в последней четверти XX века и первой четверти XXI века.
2. Предмет, объекты, система частной теории цифровизации судебно-экспертной деятельности.
3. Место теории цифровизации судебно-экспертной деятельности в общей теории судебной экспертологии.
4. Взаимосвязи и разграничения теории информационно-компьютерного обеспечения криминалистической деятельности и частной теории цифровизации судебно-экспертной деятельности.

Задание для подготовки:

Ознакомиться с тематикой лекции, изучить правовую регламентацию рассматриваемых вопросов, ознакомиться с литературой по теме.

Лекция 4. Тема 4. Объекты судебных экспертиз в цифровой форме. 2 часа.

Содержание:

1. Объекты судебных экспертиз, фиксируемые в цифровой форме.
2. Особенности судебно-экспертного исследования цифровых объектов.
3. Особенности комплексных экспертиз и исследований цифровых объектов.
4. Компетенции судебных экспертов в условиях цифровизации судебной экспертизы.
5. Проблемы подготовки судебных экспертов в условиях цифровизации судебно-экспертной деятельности.

Задание для подготовки:

Ознакомиться с тематикой лекции, изучить правовую регламентацию рассматриваемых вопросов, ознакомиться с литературой по теме.

Лекция 5. Тема 5. Следственные ошибки, возникающие при неправильной работе с объектами в цифровой форме и пути их предотвращения. 4 часа.

Содержание:

1. Методические рекомендации по сбору и подготовке объектов исследования, полученных из цифровой среды, при назначении судебных экспертиз.
2. Типичные следственные ошибки, возникающие при неправильном сборе и подготовке цифровых объектов для экспертного исследования.
3. Компетенции следователей в условиях цифровизации судебной экспертизы.
4. Проблемы подготовки следователей в условиях цифровизации судебно-экспертной деятельности.
5. Оценка заключения судебной экспертизы цифровых объектов и его использование следователем.

Задание для подготовки:

Ознакомиться с тематикой лекции, изучить правовую регламентацию рассматриваемых вопросов, ознакомиться с литературой по теме.

2.3.1. Занятия семинарского типа для очной формы обучения

Практическое занятие 1.

Тема 1. Концепция цифровых следов в криминалистике и судебной экспертологии. 2 часа

Вопросы для обсуждения:

1. Понятие цифровых следов в криминалистике и судебной экспертологии, цифровые следы.
2. Материальная сущность цифровых следов, технологическая природа и механизмы формирования цифровых следов.
3. Свойства цифровых следов. Носители цифровых следов, их виды.

Задание для подготовки:

Повторите материалы лекции. Изучите нормативные правовые источники, а также основную и дополнительную литературу по теме.

Практическое занятие 2.

Тема 2. Участие специалиста при производстве следственных и судебных действий при расследовании преступлений в цифровой среде. 4 часа.

Содержание:

1. Процессуальный статус специалиста в уголовном судопроизводстве. Требования, предъявляемые к специалисту, как участнику судопроизводства.

2. Принципы взаимодействия специалиста со следователем. Обязательность привлечения специалиста при работе с цифровыми следами.

3. Выбор специалиста и оценка его компетентности при расследовании преступлений и судебном рассмотрении дел в цифровой среде.

4. Участие специалиста в производстве процессуальных действий: осмотр места происшествия, обыск, выемка и т.д. при расследовании преступлений в цифровой среде.

5. Основные правила выявления, изъятия и фиксации цифровых следов.

Задание для подготовки:

Повторите материалы лекции. Изучите нормативные правовые источники, а также основную и дополнительную литературу по теме.

Практическое занятие 3.

Тема 3. Частная теория цифровизации судебно-экспертной деятельности. 2 часа

Вопросы для обсуждения:

1. Генезис информационно-компьютерного обеспечения судебной экспертизы в последней четверти XX века и первой четверти XXI века.

2. Предмет, объекты, система частной теории цифровизации судебно-экспертной деятельности.

3. Место теории цифровизации судебно-экспертной деятельности в общей теории судебной экспертологии.

4. Взаимосвязи и разграничения теории информационно-компьютерного обеспечения криминалистической деятельности и частной теории цифровизации судебно-экспертной деятельности.

Задание для подготовки:

Повторите материалы лекции. Изучите нормативные правовые источники, а также основную и дополнительную литературу по теме.

Практическое занятие 4-6.

Тема 5. Цифровые следы в судебных экспертизах. 6 часов.

1. Объекты судебных экспертиз, фиксируемые в цифровой форме.

2. Особенности судебно-экспертного исследования цифровых объектов.

3. Особенности комплексных экспертиз и исследований цифровых объектов.

4. Компетенции судебных экспертов в условиях цифровизации судебной экспертизы.

5. Проблемы подготовки судебных экспертов в условиях цифровизации судебно-экспертной деятельности.

Задание для подготовки:

Повторите материалы лекции. Изучите нормативные правовые источники, а также основную и дополнительную литературу по теме.

Практическое занятие 7-9.

Тема 5. Следственные ошибки, возникающие при неправильной работе с объектами в цифровой форме и пути их предотвращения. 6 часов.

Вопросы для обсуждения:

1. Методические рекомендации по сбору и подготовке объектов исследования, полученных из цифровой среды, при назначении судебных экспертиз.
2. Типичные следственные ошибки, возникающие при неправильном сборе и подготовке цифровых объектов для экспертного исследования.
3. Компетенции следователей в условиях цифровизации судебной экспертизы.
4. Проблемы подготовки следователей в условиях цифровизации судебно-экспертной деятельности.
5. Оценка заключения судебной экспертизы цифровых объектов и его использование следователем.
6. Консультация специалиста при расследовании преступлений и судебном рассмотрении дел в цифровой среде.

Задание для подготовки:

Повторите материалы лекции. Изучите нормативные правовые источники, а также основную и дополнительную литературу по теме.

Приложение 6. Перечень программ для исследования цифровых объектов

Название программы[212]	Наличие лицензии/режим доступа	Функционал	К каким объектам применима
FileList Creator	Freeware[213]	Составляет перечни файлов и рассчитывает хеш-код	Для любых файлов
JPEGSnoop	Freeware	Анализ матриц преобразования для цифровых фотографий (поиск признаков монтажа)	Для цифровых фото
ExifTool	Freeware	Исследование метаданных цифровых изображений	Для цифровых фото
USB Deview	Freeware	Описание USB носителей	Для USB носителей
Nero InfoTool	Freeware	Описание компакт-дисков	Для CD, DVD
GIMP	Freeware	Графический редактор	Для обработки изображений
Kinovea	Freeware	Программа для просмотра видео в разных режимах	Для исследования видеофайлов
ImageJ	Freeware	Измерение размеров на изображениях	Для цифровых фото
Nanocad	Freeware (версия 5.1)	Построение схем и планов, чертежей	Создание схем
Adobe Acrobat Reader	Freeware	Чтение PDF	Для PDF-документов
FastStone Image Viewer	Freeware	Просмотр изображений	Для цифровых фото
Мобильный криминалист Эксперт+	Доступны различные варианты лицензирования, включая версию с USB-ключом для работы без интернета, программа платная	Извлечение, анализ данных, исследование ПК	Исследование мобильных устройств

[212] В данном перечне представлены некоторые программы, находящиеся в свободном доступе и пригодные для использования в процессе экспертного исследования. Перечень программ является ознакомительным.

[213] (СПО – свободное программное обеспечение).

Приложение 7. Правила изъятия и фиксации цифровых следов в ходе следственных и оперативно-розыскных действий[214]

Сфера применения	Настоящие правила рассчитаны для использования сотрудниками, выполняющими следственные и оперативно-розыскные мероприятия
Цель применения	Настоящие правила содержат основные моменты, на которые необходимо обращать внимание при обнаружении, изъятии и фиксации цифровых следов
Источники	Рекомендации и положения инструкции составлялись на основе следующих нормативных и литературных источников: 1. УПК РФ; 2. Россинская Е.Р. Проблемы использования специальных знаний в судебном исследовании компьютерных преступлений в условиях цифровизации // Вестник Ун-та им. О.Е. Кутафина (МГЮА). 2019. № 5. С. 31-44. 3. Федотов Н.Н. Форензика – компьютерная криминалистика – М.: Юридический Мир, 2007. – 432 с.

Основные моменты

1. Правила сбора и фиксации цифровых доказательств не имеют законодательного закрепления (за исключением некоторых отдельных норм), не отражены в ведомственных нормативных актах, что заставляет сомневаться в доброкачественности проведенного мероприятия. Поскольку следователи и сотрудники ОРМ должны взаимодействовать с цифровыми доказательствами, им необходимо обладать определенными специальными знаниями, которых в большинстве случаев нет. В целях обеспечения надежности и достоверности сбора и изъятия цифровых следов, необходимо **привлечение специалиста.**

2. Автор предлагает соблюдать при проведении следственных действий положения настоящих правил и в дальнейшем ссылаться на них для подтверждения «соблюдения общепринятых и признанных ведущими специалистами правил и стандартов».

[214] Данные правила носят ознакомительный характер, содержат лишь некоторые правила осмотра и изъятия, которые были описаны в диссертационном исследовании, а именно – правила осмотра компьютерной техники, правила расчета хеш-суммы изымаемого цифрового следа. В дальнейшем при разработке таких правил предполагается описание для всех следственных действий.

Термины и определения

Понятие	Дефиниция	Значимость для фиксации и изъятия цифровых следов
Хеш, хеш-сумма	Последовательность символов фиксированной длины, полученная путем преобразования произвольных исходных данных (числа, текста, файла и др.) при помощи специального математического алгоритма. Обладает свойством уникальности	Следует рассматривать хеш-сумму файла как значимую характеристику при работе с объектами в цифровой форме. В рамках судебного-экспертного исследования хеш-сумма лишь подтверждает, что экспертом на исследование был получен именно тот файл, который ему направил правоприменитель. Таким образом, соответствие хеш-суммы файла свидетельствует о том, что в первоначальное содержание цифрового файла не вносилось никаких изменений. Сравнивая контрольные суммы файла, можно сразу узнать, был он модифицирован или нет. Если есть ошибка контрольной суммы, контрольная сумма не соответствует требуемой или имеющейся, то значит, что файл был изменен.
Цифровой след	Криминалистически значимая компьютерная информация о событиях / действиях в процессе ее возникновения, обработки, хранения, передачи, отраженная в материальной среде	Необходимо для наличия базовых представлений о том, что именно следователь должен выявить и изъять в ходе следственного действия, где такие следы искать
Цифровой объект	Объект судебно-экспертного исследования, состоящий из цифровых следов различных видов, находящихся на объекте-носителе	Необходимо знать для того, чтобы следователь понимал, что именно в последующем нужно направить на экспертное исследование

Осмотр вещной обстановки

При производстве обыска или осмотра в ходе расследования преступлений могут быть обнаружены не только цифровые следы, но и следы рук, микрообъекты, следы ДНК и пр. Исходя из этого, стоит придерживаться следующего алгоритма действий в ходе осмотра места происшествия при расследовании компьютерных преступлений:

1) статическая стадия осмотра:

- определить местоположение компьютерной техники и подробно описать его в протоколе следственного действия;
- осмотреть все внешние устройства, которые подключены к ПК (клавиатура, мышь, веб-камера и др.);
- обратить пристальное внимание на индивидуальные особенности всей компьютерной техники (системного блока, клавиатуры, монитора и пр.);

2) динамическая стадия осмотра:

- обнаружить на поверхности внешних устройств материальные следы преступления (микрообъекты, следы пальцев рук);

- изучить аппаратное обеспечение (координатные устройства, устройства для ввода текста, устройства ввода изображений и видео и т. п.);

- определить операционную систему;

- установить IP-адрес;

- посмотреть данные о пользователе с помощью браузера. Работая с браузером, нельзя закрывать открытые вкладки, а переходить по гиперссылкам необходимо в режиме новой вкладки;

- изучить историю просмотра веб-страниц;

- изучить электронную почту;

- определить, имеются ли у пользователя средства анонимизации;

- исследовать средства синхронизации данных;

- использовать программы для поиска и восстановления недавно удаленных файлов (Recuva, Hetman Partition Recovery, EaseUS Data Recovery и др.).

3) осмотр вещной обстановки:

- при проведении следственных действий по изъятию компьютерной техники и цифровых следов нельзя игнорировать вещную обстановку места происшествия, под которой в данном случае понимается осмотр рабочего места, проверка на наличие стикеров/документов/записок, потенциально содержащих в себе данные, которые могли использоваться как «логин» и «пароль» для входа в устройство.

На заключительной стадии осмотра, если следователь принимает решение изъять компьютерную технику, необходимо перевести компьютер в «спящий» режим, поскольку это позволит сохранить информацию с жесткого диска и с запущенных приложений. Далее, соблюдая все требования уголовно-процессуального законодательства, необходимо изъять электронные носители информации и упаковать их должным образом. После чего с соблюдением уголовно-процессуальных требований необходимо упаковать осмотренный объект.

Правила осуществления расчета хеш-суммы цифрового следа

1. Хеш-сумма цифрового следа должна быть рассчитана следователем/сотрудником ОРМ **строго ДО** момента изъятия/копирования/переноса на носитель, поскольку только в таком случае можно гарантировать неизменность самого следа. Полученная хеш-сумма должна быть **обязательно зафиксирована** в протоколе соответствующего следственного действия, а в дальнейшем **указана в постановлении/определении о назначении судебной экспертизы**. Это нужно для того, чтобы у эксперта была возможность сравнить полученную им хеш-сумму с той, что указана в документации.

2. Следует использовать надежные и апробированные алгоритмы подсчета, например, SHA-1, CRC32, SHA-2 и SHA-256. В некоторые операционные системы ПК уже включена функция автоматического подсчета данного показателя, если таковой нет, необходимо установить специальную программу.

3. Хеш-сумма может быть рассчитана **<u>следующими способами</u>**:

Способ №1

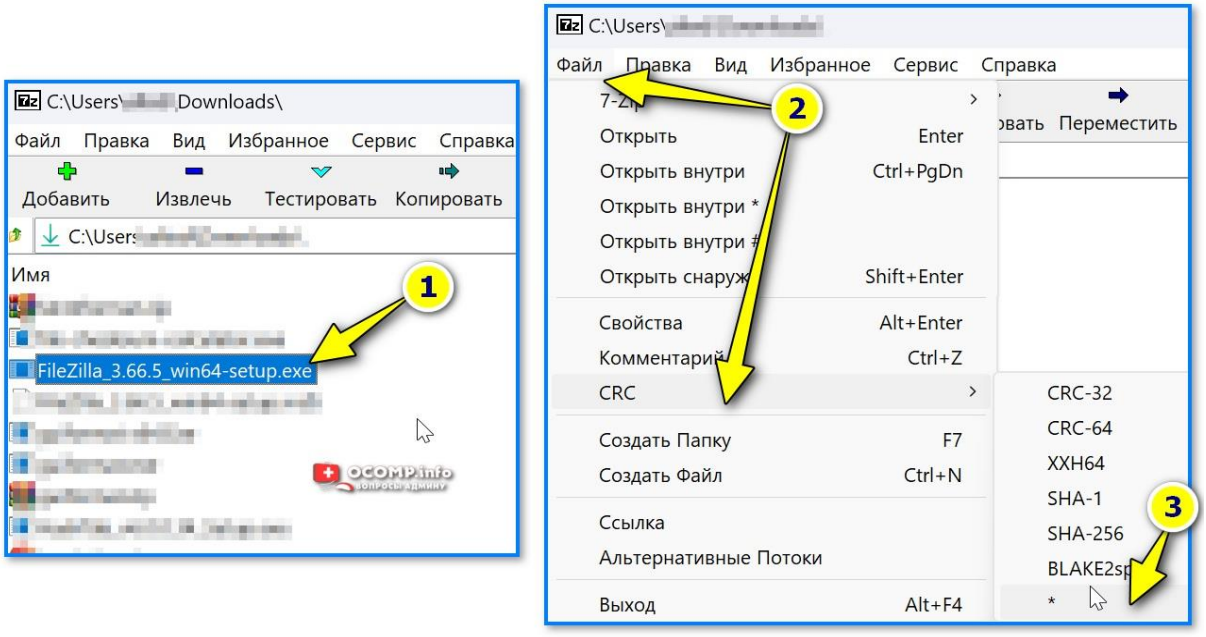
Архиватор 7ZIP (ссылка на офиц. сайт: https://www.7-zip.org/).
Для того, чтобы рассчитать хеш-сумму файла через 7ZIP, нужно:

Шаг 1: Запуск 7ZIP
- Найдите и запустите программу 7ZIP на вашем компьютере.
- Запустите программу.

Шаг 2: Выбор файла
- Используйте интерфейс 7ZIP для навигации к папке, в которой находится файл, для которого вы хотите рассчитать хеш-сумму.
- Щелкните правой кнопкой мыши на нужном файле.
- Выберите файл (отм.1).

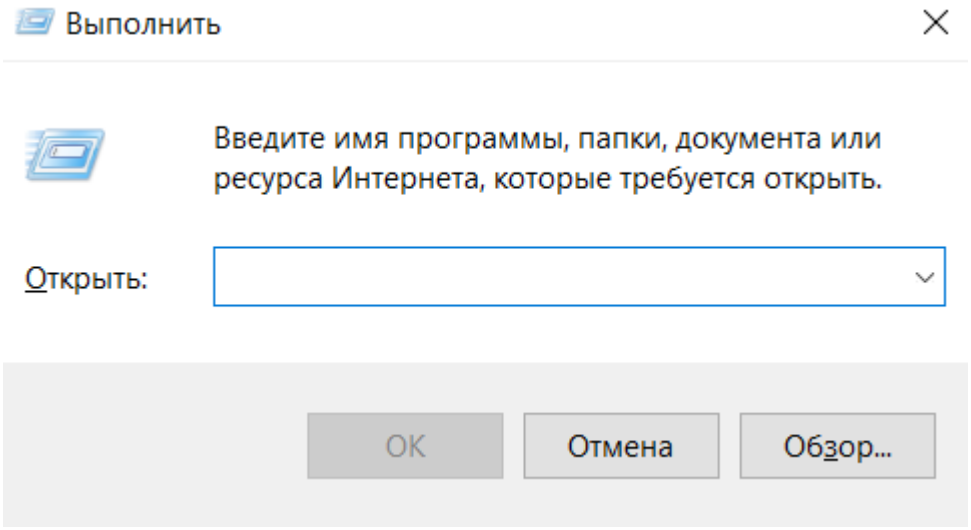
Шаг 3: Копирование в буфер обмена
- В появившемся контекстном меню выберите пункт "Файл / CRC /» (отм.2).

Шаг 4: Получение хеш-суммы
- В открывшемся окне вы увидите различные варианты хеш-сумм (MD5, SHA-1, SHA-256 и др.) (отм.3).
- Вы можете скопировать нужную хеш-сумму в буфер обмена, выделив её и нажав Ctrl + C.
- Хеш-сумма сгенерирована.



Способ №2

Встроенная в Windows утилита **CertUtil**.
Для этого понадобится:
- запустить командную строку: Нажать сочетание клавши «WIN+R»;



- ввести в нее нижеприведенную команду и нажать Enter).

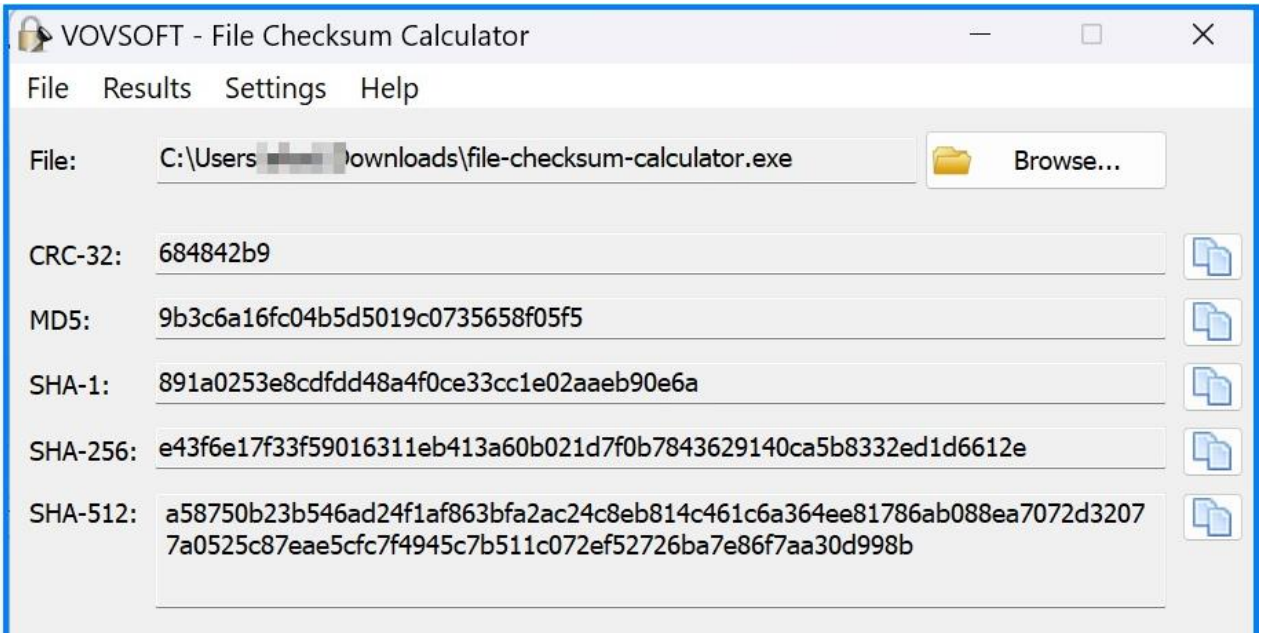
certutil -hashfile C:\Users\alex\Downloads\FileZilla_3.66.5_win64-setup.exe MD5

Важно иметь в виду, что:
- вместо указанного пути к программе (C:\Users\alex\Downloads\FileZilla_3.66.5_win64-setup.exe) нужно указать **свой путь** к файлу;
- **ПУТЬ ФАЙЛА** можно узнать, нажав правой кнопкой мыши на нужный файл, затем выбрать клавишу «Свойства», перейти во вкладку «Общие»;
- вместо MD5 — можно указать другой тип контр. суммы (SHA1 или SHA256, например).

Способ №3

Total Commander (ссылка: https://www.ghisler.com/download.htm); HashTab V 6.0 (ссылка: https://implbits.com/hashtab); File Checksum Calculator (ссылка: https://vovsoft.com/software/file-checksum-calculator/) и другие специализированные программы. Алгоритм действий и функционал у всех программ по расчету хеш-суммы примерно одинаковый.

Например, при использовании утилиты File Checksum Calculator нужно указать расположение файла: и через 1-2 сек. программа выдаст несколько видов рассчитанной величины по разным алгоритмам (строки CRC32, MD5, SHA1, SHA256, SHA512).


VOVSOFT - File Checksum Calculator
File
Results
Settings
Help
File:
C:\Users [redacted] ownloads\file-checksum-calculator.exe
Browse...
CRC-32:
684842b9
MD5:
9b3c6a16fc04b5d5019c0735658f05f5
SHA-1:
891a0253e8cdfdd48a4f0ce33cc1e02aaeb90e6a
SHA-256:
e43f6e17f33f59016311eb413a60b021d7f0b7843629140ca5b8332ed1d6612e
SHA-512:
a58750b23b546ad24f1af863bfa2ac24c8eb814c461c6a364ee81786ab088ea7072d3207
7a0525c87eae5cfc7f4945c7b511c072ef52726ba7e86f7aa30d998b