

СПЕЦИФИЧЕСКИЕ ОСОБЕННОСТИ ПРОВЕДЕНИЯ ЦИФРОВЫХ
ЭКСПЕРТИЗ

Наджмиддинов Муhibулло Гайратджонович
КУРСАНТ АКАДЕМИЯ МВД РЕСПУБЛИКИ УЗБЕКИСТАН

Kalit soʻzlar: raqamli ekspertiza, sud ekspertizasi, raqamli dalillar, elektron maʼlumotlar, kompyuter kriminalistikasi, elektron axborot tashuvchilar, axborot texnologiyalari, maʼlumotlar yaxlitligi, ekspert xulosasi, kiberjinoyatchilik.

Annotatsiya: Maqolada axborot texnologiyalarining jadal rivojlanishi va jinoyatlarni tergov qilish jarayonida elektron maʼlumotlardan foydalanish koʻlaminig kengayishi sharoitida raqamli ekspertizalarni oʻtkazishning oʻziga xos xususiyatlari koʻrib chiqiladi. Raqamli dalillarni aniqlash, olib qoʻyish, saqlash va tekshirishning asosiy bosqichlari, elektron axborot tashuvchilar, mobil qurilmalar, kompyuter tizimlari hamda tarmoq resurslari bilan ishlashning oʻziga xos jihatlari tahlil qilinadi. Raqamli maʼlumotlarning yaxlitligini taʼminlash, maxsus dasturiy-texnik vositalardan foydalanish, protsessual talablarga rioya etish va asoslantirilgan ekspert xulosasini shakllantirish masalalariga alohida eʼtibor qaratiladi. Shuningdek, raqamli ekspertizalarni oʻtkazishdagi dolzarb muammolar hamda jamiyatni raqamlashtirish sharoitida ekspertlik faoliyatini takomillashtirish istiqbollari yoritiladi.

Ключевые слова: цифровая экспертиза, судебная экспертиза, цифровые доказательства, электронные данные, компьютерная криминалистика, электронные носители информации, информационные технологии, целостность данных, экспертное заключение, киберпреступность.

Аннотация: В статье рассматриваются специфические особенности проведения цифровых экспертиз в условиях стремительного развития информационных технологий и расширения сферы использования электронных данных в процессе расследования правонарушений и преступлений. Анализируются основные этапы обнаружения, изъятия, сохранения и исследования цифровых доказательств, особенности работы с электронными носителями информации, мобильными устройствами, компьютерными системами и сетевыми ресурсами. Особое внимание уделяется обеспечению целостности цифровых данных, применению специализированных программно-технических средств, соблюдению процессуальных требований и формированию обоснованного экспертного заключения. Также рассматриваются актуальные проблемы проведения цифровых экспертиз и перспективы совершенствования экспертной деятельности в условиях цифровизации общества.

Keywords: digital forensics, forensic examination, digital evidence, electronic data, computer forensics, electronic storage media, information technologies, data integrity, expert report, cybercrime.

Annotation: The article examines the specific features of conducting digital forensic examinations in the context of the rapid development of information technologies and the

growing use of electronic data in the investigation of offenses and crimes. It analyzes the main stages of identifying, seizing, preserving, and examining digital evidence, as well as the specific aspects of working with electronic storage media, mobile devices, computer systems, and network resources. Particular attention is paid to ensuring the integrity of digital data, the application of specialized software and technical tools, compliance with procedural requirements, and the preparation of well-founded expert reports. The article also addresses current challenges in conducting digital forensic examinations and explores prospects for improving forensic practice in the context of the digital transformation of society.

ВВЕДЕНИЕ

В условиях стремительной цифровизации общественных отношений, развития информационно-коммуникационных технологий и расширения сферы применения электронных устройств особую актуальность приобретает совершенствование методов выявления, фиксации, исследования и использования цифровой информации в процессе раскрытия и расследования правонарушений и преступлений. Современные информационные технологии активно используются в различных сферах общественной жизни, включая экономику, государственное управление, образование, банковскую деятельность и межличностное общение. Вместе с тем расширение цифрового пространства сопровождается появлением новых способов совершения противоправных деяний, использованием электронных устройств и сетевых ресурсов для подготовки, совершения и сокрытия преступлений. В подобных условиях цифровая информация приобретает важное значение для установления обстоятельств расследуемого события, определения круга причастных лиц, выявления взаимосвязей между участниками противоправной деятельности и проверки выдвинутых следственных версий. Цифровые следы могут сохраняться в памяти компьютеров и мобильных устройств, на электронных носителях, в облачных хранилищах, системах видеонаблюдения, журналах событий, переписке, электронных документах и сетевом трафике. Однако специфика таких данных заключается в их нематериальной форме представления, высокой изменчивости, возможности удалённого удаления или модификации, а также зависимости результатов исследования от применяемых технических средств и программного обеспечения. Даже незначительное изменение исходной информации способно повлиять на результаты экспертного исследования, поэтому обеспечение целостности и достоверности цифровых данных является одним из важнейших условий проведения качественной цифровой экспертизы. Цифровая экспертиза представляет собой специальное исследование цифровых данных, электронных устройств и информационных систем, направленное на установление фактических обстоятельств, имеющих значение для расследования и судебного рассмотрения дел. В зависимости от объекта исследования она может включать компьютерно-техническую экспертизу, исследование мобильных устройств, анализ цифровых изображений и видеозаписей, изучение электронных документов, сетевых соединений и иных источников цифровой информации. Каждое из указанных направлений характеризуется собственными методами исследования, техническими

требованиями и особенностями интерпретации полученных результатов. При этом проведение цифровой экспертизы требует не только специальных знаний в области информационных технологий, но и понимания положений криминалистики, судебной экспертизы и соответствующего процессуального законодательства. Особую значимость приобретает соблюдение установленного порядка обнаружения, изъятия, упаковки, транспортировки и хранения электронных носителей информации. Нарушение последовательности указанных действий может привести к утрате данных, изменению их содержания либо возникновению сомнений в достоверности результатов исследования. Поэтому при проведении цифровой экспертизы необходимо применять научно обоснованные методики, использовать специализированные программно-технические средства, документировать каждый существенный этап работы и обеспечивать возможность проверки полученных результатов другими специалистами. Не менее важным аспектом является разграничение исходных данных и информации, полученной в результате экспертной обработки, а также точное описание использованных методов и инструментов в экспертном заключении. Актуальность рассматриваемой темы обусловлена также постоянным усложнением цифровой инфраструктуры, распространением облачных технологий, шифрования, распределённых систем хранения данных и программных средств, позволяющих удалённо изменять или уничтожать информацию. Указанные обстоятельства предъявляют повышенные требования к профессиональной подготовке экспертов, техническому оснащению экспертных подразделений и совершенствованию методического обеспечения экспертной деятельности. Важное значение имеет и международное сотрудничество, поскольку цифровые данные, имеющие отношение к одному расследуемому событию, могут одновременно храниться на устройствах, расположенных в разных государствах, и на серверах зарубежных информационных платформ. Это требует учёта особенностей трансграничного получения электронных данных, соблюдения законодательства и обеспечения допустимости полученных материалов в соответствующем процессуальном порядке. Цель исследования заключается в комплексном анализе специфических особенностей проведения цифровых экспертиз, определении основных требований к работе с цифровыми доказательствами и выявлении перспектив совершенствования методов экспертного исследования электронных данных. Для достижения поставленной цели предусматривается решение следующих задач: раскрыть понятие и значение цифровой экспертизы в современной экспертной практике; определить основные виды объектов цифрового исследования и их криминалистические характеристики; изучить порядок обнаружения, фиксации, изъятия и сохранения цифровых доказательств; проанализировать методы обеспечения целостности и достоверности электронных данных; выявить основные организационные, технические и процессуальные проблемы проведения цифровых экспертиз; определить перспективные направления развития методического и технического обеспечения экспертной деятельности. Объектом исследования выступают общественные отношения, возникающие в процессе назначения, организации и проведения цифровых экспертиз при

расследовании и судебном рассмотрении дел. Предмет исследования составляют закономерности обнаружения, фиксации, сохранения, извлечения и исследования цифровой информации, методы и технические средства цифровой криминалистики, а также организационные и процессуальные требования, обеспечивающие достоверность результатов экспертного исследования. Методологическую основу исследования составляют общенаучные и специальные методы познания, включая анализ, синтез, системный подход, сравнительно-правовой метод, формально-юридический метод и метод обобщения экспертной практики. Их применение позволяет рассмотреть цифровую экспертизу как комплексную деятельность, объединяющую технические, криминалистические и правовые аспекты. Практическая значимость исследования заключается в возможности использования сформулированных положений для совершенствования деятельности экспертных подразделений, повышения качества исследования электронных носителей информации, улучшения подготовки специалистов и разработки рекомендаций по обеспечению сохранности цифровых доказательств. Таким образом, исследование специфических особенностей проведения цифровых экспертиз имеет важное научное и практическое значение, поскольку эффективность экспертной деятельности в цифровой среде непосредственно связана с полнотой, объективностью и достоверностью установления обстоятельств расследуемых событий.

ОСНОВНАЯ ЧАСТЬ

Цифровая экспертиза в современных условиях представляет собой одно из наиболее динамично развивающихся направлений судебно-экспертной деятельности, обусловленное широким распространением электронных устройств, информационных систем и цифровых коммуникаций. Её значение определяется необходимостью установления фактических обстоятельств, связанных с использованием информационных технологий, а также выявления, исследования и интерпретации цифровых следов, имеющих доказательственное значение. В отличие от традиционных объектов судебной экспертизы, цифровая информация характеризуется высокой изменчивостью, зависимостью от технической среды, возможностью многократного копирования без существенного изменения содержания и риском незаметной модификации. Эти особенности требуют разработки специальных методик исследования, применения проверенных программно-технических средств и строгого соблюдения процедур обращения с электронными данными. При этом цифровая экспертиза не ограничивается исследованием компьютерной техники. Она охватывает широкий спектр объектов, включая мобильные телефоны, планшеты, серверы, электронные носители информации, сетевое оборудование, системы видеонаблюдения, облачные хранилища, электронные документы и данные различных информационных платформ. В зависимости от поставленных задач эксперт может устанавливать наличие и содержание определённых файлов, восстанавливать последовательность действий пользователя, исследовать сведения о подключении устройств, анализировать метаданные, определять признаки изменения информации и выявлять взаимосвязи между отдельными цифровыми объектами. Результаты такого

исследования могут использоваться для проверки следственных версий, установления механизма совершения противоправного деяния и определения обстоятельств, имеющих значение для правильного разрешения дела. Понятие, сущность и основные направления цифровой экспертизы. Сущность цифровой экспертизы заключается в применении специальных знаний и научно обоснованных методов для исследования информации, представленной в цифровой форме, с целью получения объективных и проверяемых результатов. В научной и практической литературе понятие цифровой экспертизы тесно связано с компьютерной криминалистикой, под которой понимается совокупность методов выявления, сохранения, извлечения, анализа и представления цифровых данных. Вместе с тем указанные понятия не всегда полностью совпадают: компьютерная криминалистика может рассматриваться как более широкое научно-практическое направление, тогда как цифровая экспертиза в процессуальном контексте представляет собой исследование, проводимое в установленном законом порядке уполномоченным экспертом с подготовкой соответствующего заключения. Конкретное соотношение этих понятий зависит от национального законодательства, принятой терминологии и характера экспертной деятельности. Одним из основных направлений является компьютерно-техническая экспертиза, в рамках которой исследуются аппаратные компоненты компьютерных систем, операционные системы, файловые структуры, установленные программы, пользовательские данные и системные журналы. Данный вид исследования позволяет установить особенности функционирования устройства, определить наличие определённых файлов и программ, выявить следы удаления или изменения информации, а также изучить последовательность операций, выполненных в компьютерной среде. Другим значимым направлением выступает экспертиза мобильных устройств, ориентированная на исследование смартфонов, планшетов, SIM-карт и иных компонентов мобильной инфраструктуры. В процессе такого исследования могут анализироваться контакты, сообщения, журналы вызовов, фотографии, видеозаписи, сведения о геолокации, история использования приложений и другие доступные данные. При этом возможность извлечения информации зависит от модели устройства, версии операционной системы, состояния памяти, применяемых механизмов шифрования и наличия законных оснований для доступа к соответствующим сведениям. Существенное место занимает исследование цифровых изображений и видеозаписей. Его задачами могут быть установление технических характеристик файла, изучение метаданных, обнаружение признаков редактирования, сопоставление отдельных изображений и анализ последовательности визуальных событий. При этом наличие технических несоответствий или признаков обработки само по себе не всегда свидетельствует о фальсификации: необходимо учитывать особенности работы камеры, алгоритмы сжатия, автоматическую обработку изображений и программные преобразования. Отдельное направление связано с исследованием сетевых данных, включая журналы сетевых соединений, сведения о передаче информации, сетевые протоколы и записи событий информационной безопасности. Такие исследования могут способствовать установлению времени соединений, выявлению подозрительной

сетевой активности и анализу взаимодействия между устройствами. Однако сетевые идентификаторы, IP-адреса и технические журналы не всегда позволяют однозначно установить конкретного пользователя, поскольку могут применяться общие сети, прокси-серверы, виртуальные частные сети и другие технологии, затрудняющие непосредственную атрибуцию действий. Поэтому эксперт обязан разграничивать технически подтверждённые факты и предположения, которые требуют дополнительной проверки. Обнаружение и фиксация цифровых следов. Одним из важнейших этапов проведения цифровой экспертизы является обнаружение и первоначальная фиксация цифровых следов. Цифровые следы представляют собой сведения, возникающие в результате функционирования электронных устройств, программного обеспечения и сетевых систем и потенциально содержащие информацию о действиях пользователей, времени событий, технических процессах и взаимодействии между объектами. Они могут находиться как в постоянной памяти устройств, так и в оперативной памяти, системных журналах, временных файлах, резервных копиях и удалённых информационных ресурсах. Обнаружение таких следов требует предварительного определения возможных источников информации с учётом характера расследуемого события. Например, при исследовании обстоятельств несанкционированного доступа к информационной системе особое значение могут иметь журналы аутентификации, сведения о сетевых соединениях, данные средств защиты информации и записи систем мониторинга. Если исследуются обстоятельства распространения определённого файла, необходимо учитывать метаданные, историю передачи, сведения о создании и изменении файла, а также доступные записи приложений и коммуникационных сервисов. При этом обнаружение цифрового следа ещё не означает автоматического признания его доказательством. Необходимо установить источник информации, обстоятельства её получения, связь с исследуемым событием и возможность проверки достоверности. Первоначальная фиксация включает документирование состояния устройства, его внешних характеристик, подключённых компонентов, обнаруженных носителей и иных существенных обстоятельств. В зависимости от ситуации могут фиксироваться дата и время, состояние питания, активные сетевые подключения, отображаемые на экране сведения, используемые интерфейсы и другие характеристики, имеющие значение для дальнейшего исследования. Особая осторожность требуется при работе с включёнными устройствами, поскольку их выключение или изменение состояния может привести к утрате данных, содержащихся в оперативной памяти, временных хранилищах или активных процессах. В то же время сохранение устройства включённым может создавать риски удалённого доступа, автоматического удаления информации или дальнейшего изменения данных. Следовательно, решение о порядке обращения с устройством должно приниматься с учётом конкретных обстоятельств, технических особенностей и применимых процессуальных требований. Фиксация цифровых следов должна обеспечивать возможность последующей проверки исходных сведений и понимания того, каким образом они были обнаружены и получены. Изъятие, сохранение и обеспечение целостности цифровых доказательств.

Специфика цифровой экспертизы наиболее отчётливо проявляется при изъятии и сохранении электронных носителей информации. В отличие от многих материальных объектов, цифровые данные могут изменяться вследствие обычной работы операционной системы, автоматической синхронизации, обновления программ, изменения системного времени или действий пользователя. Кроме того, некоторые данные доступны только при наличии определённых учётных записей, криптографических ключей либо активного сетевого соединения. Поэтому сохранение цифровой информации требует применения процедур, направленных на минимизацию непреднамеренных изменений и обеспечение проверяемости всех выполненных действий. Важным инструментом является создание криминалистической копии данных, позволяющей проводить исследование без непосредственного воздействия на оригинальный носитель. В соответствующих случаях применяются аппаратные или программные средства блокирования записи, препятствующие изменению содержимого исследуемого носителя. Однако эффективность таких средств зависит от типа устройства, используемого интерфейса и особенностей исследуемой системы. При работе с современными твердотельными накопителями, мобильными устройствами и зашифрованными хранилищами необходимо учитывать технические ограничения, которые могут влиять на полноту извлечения информации. Одним из распространённых методов контроля целостности является вычисление криптографических хеш-значений, например с использованием алгоритмов SHA-256. Хеш-значение представляет собой результат обработки цифровых данных по определённому алгоритму и позволяет сопоставлять содержимое файлов или образов носителей на разных этапах работы. Если исходные данные и полученная копия имеют одинаковые хеш-значения, это служит весомым техническим подтверждением совпадения их содержимого в пределах проверяемых данных и применённого алгоритма. Вместе с тем совпадение хеш-значений само по себе не доказывает законность получения информации, правильность идентификации её источника или достоверность содержащихся в ней сведений. Эти обстоятельства требуют самостоятельной оценки. Для обеспечения надлежащей сохранности цифровых доказательств необходимо вести документированный учёт всех операций, включая получение объекта, его упаковку, передачу между ответственными лицами, создание копий, вычисление контрольных значений и выполнение исследовательских действий. Такая последовательность действий позволяет обеспечить прослеживаемость происхождения цифровых данных и уменьшить риск возникновения сомнений относительно их неизменности. При этом оригинальный носитель, когда это технически возможно и необходимо, должен сохраняться в условиях, исключающих несанкционированное вмешательство. Исследовательские операции предпочтительно проводить на проверенных копиях, что позволяет снизить вероятность случайного изменения исходных сведений. Если изменение оригинала было неизбежным по техническим причинам, эксперт должен документировать характер и причины такого изменения, а также оценивать его влияние на результаты исследования. Методика исследования цифровых объектов. Методика цифровой экспертизы представляет собой

систему взаимосвязанных научных и технических приёмов, применяемых для решения конкретных экспертных задач. Выбор методов определяется видом объекта, состоянием носителя, характером предполагаемых цифровых следов, вопросами, поставленными перед экспертом, и установленными правовыми ограничениями. Исследование обычно включает подготовительный, аналитический и заключительный этапы, хотя их последовательность может изменяться в зависимости от обстоятельств дела. На подготовительном этапе эксперт изучает постановление или определение о назначении экспертизы, уточняет поставленные вопросы, проверяет достаточность представленных материалов и определяет технические условия проведения исследования. При необходимости устанавливаются модель устройства, особенности файловой системы, версия программного обеспечения и возможные ограничения доступа к информации. На аналитическом этапе проводится извлечение данных, изучение файловой структуры, анализ метаданных, исследование системных журналов, сопоставление временных отметок и поиск сведений, относящихся к поставленным вопросам. Для повышения полноты исследования могут использоваться фильтрация по типам файлов, поиск по ключевым словам, анализ временных интервалов, восстановление доступных удалённых данных и сопоставление сведений из нескольких независимых источников. При этом автоматизированные инструменты не заменяют экспертную оценку: результаты их работы необходимо проверять с учётом технических особенностей объекта и ограничений применяемых алгоритмов. Особое значение имеет анализ временных характеристик цифровых событий. Дата и время, указанные в свойствах файла, системном журнале или сообщении, могут зависеть от часового пояса, настроек устройства, синхронизации системного времени и способа хранения временных меток. Кроме того, некоторые значения могут отражать время последнего изменения, а не момент первоначального создания или фактического использования объекта. Поэтому сопоставление временных данных требует установления источника каждой отметки и оценки возможных отклонений. Например, при восстановлении последовательности событий необходимо учитывать расхождения системного времени между устройствами, особенности хранения времени в универсальном координированном формате и локальном времени, а также возможные изменения часов устройства. Игнорирование этих факторов способно привести к неправильной реконструкции хронологии событий. Не менее важным направлением является восстановление удалённых данных. Удаление файла в пользовательском интерфейсе не всегда означает физическое уничтожение содержащейся в нём информации. В некоторых случаях сведения могут сохраняться в нераспределённом пространстве носителя, резервных копиях, временных каталогах или других информационных структурах. Вместе с тем успешное восстановление не гарантируется: результат зависит от типа накопителя, механизма удаления, последующих операций записи, применения шифрования и функционирования технологий оптимизации памяти. Например, механизм TRIM, применяемый в ряде твердотельных накопителей, может существенно ограничивать возможность восстановления удалённых данных. Поэтому эксперт должен указывать не только

обнаруженные сведения, но и ограничения использованной методики, не делая категоричных выводов там, где имеющихся данных недостаточно. Важным компонентом методики выступает анализ метаданных. Метаданные могут содержать сведения о названии файла, его размере, формате, датах изменения, параметрах создания, используемом программном обеспечении и других характеристиках. В зависимости от типа объекта они могут включать сведения об авторе документа, параметрах фотосъёмки, истории редактирования или технических свойствах аудио- и видеозаписи. Однако метаданные могут изменяться, удаляться или автоматически формироваться программами. Следовательно, их доказательственное значение определяется не только содержанием, но и происхождением, способом получения и согласованностью с другими источниками информации. Особенности исследования мобильных устройств и облачных данных. Современные мобильные устройства представляют собой сложные информационные системы, объединяющие функции связи, хранения данных, геолокации, фото- и видеозаписи, электронных платежей и взаимодействия с сетевыми сервисами. В результате смартфон может содержать значительный объём информации, позволяющей установить характер коммуникаций, последовательность использования приложений и отдельные обстоятельства деятельности пользователя. Вместе с тем исследование мобильных устройств сопряжено с рядом технических трудностей. Среди них следует выделить шифрование пользовательских данных, блокировку экрана, использование биометрической аутентификации, ограничения доступа к отдельным разделам памяти и зависимость возможностей извлечения информации от версии операционной системы. В некоторых случаях получение данных возможно только через штатные механизмы экспорта, резервные копии или доступные интерфейсы приложений. Эксперт должен учитывать, что различные способы извлечения могут обеспечивать неодинаковую полноту сведений и создавать различные ограничения для последующего анализа. При исследовании мобильных устройств особое внимание уделяется разграничению данных, непосредственно хранящихся на устройстве, и информации, синхронизируемой с внешними сервисами. Например, отдельные сообщения, фотографии и сведения о местоположении могут одновременно находиться в локальной памяти и облачном хранилище. При этом данные в разных источниках могут отличаться вследствие настроек синхронизации, удаления отдельных элементов, изменения учётной записи или особенностей работы приложения. Сопоставление нескольких источников позволяет повысить полноту анализа, однако требует установления самостоятельного происхождения каждого набора данных. Облачные технологии создают дополнительные сложности, поскольку физическое расположение серверов, юридическая принадлежность инфраструктуры и местонахождение пользователя могут не совпадать. Получение информации из облачного хранилища может зависеть от правил соответствующего сервиса, доступных механизмов экспорта, требований законодательства и международных процедур правовой помощи. Кроме того, эксперт не всегда имеет непосредственный доступ к серверной инфраструктуре и может исследовать только предоставленную выгрузку данных или резервную копию.

В подобных случаях необходимо документировать способ получения материалов, их объём, формат, контрольные значения и сведения, позволяющие проверить полноту предоставленной информации. Особую осторожность следует проявлять при интерпретации данных геолокации. Координаты могут определяться посредством спутниковых систем, сетей мобильной связи, беспроводных сетей и программных сервисов. Точность таких данных зависит от способа определения местоположения, условий приёма сигнала, настроек устройства и характеристик используемого приложения. Наличие координат в файле или истории приложения не всегда подтверждает, что конкретное лицо физически находилось в указанном месте в определённый момент. Для обоснованного вывода необходимо исследовать источник координат, время их регистрации, возможные технические погрешности и взаимосвязь с другими материалами. Таким образом, исследование мобильных устройств и облачных данных требует комплексного подхода, учитывающего технические особенности хранения информации, механизмы синхронизации, ограничения доступа и правовые условия получения цифровых материалов. Исследование сетевых следов и установление обстоятельств цифровых инцидентов. Значительное место в современной цифровой экспертизе занимает исследование сетевых следов, формирующихся в процессе взаимодействия устройств и информационных систем. К таким объектам относятся журналы сетевых подключений, записи межсетевых экранов, данные систем обнаружения вторжений, сведения об аутентификации, журналы веб-серверов и другие технические записи. Их анализ позволяет выявлять последовательность соединений, устанавливать временные параметры активности, определять использованные протоколы и выявлять признаки подозрительных операций. При расследовании инцидентов информационной безопасности исследуются возможные способы первоначального доступа, характер перемещения между компонентами сети, признаки использования вредоносного программного обеспечения и обстоятельства передачи данных. Важным условием такого исследования является сопоставление журналов из разных источников, поскольку отдельная запись обычно отражает только ограниченную часть произошедшего события. Например, сведения о подключении к серверу могут подтверждать факт сетевого взаимодействия, однако сами по себе не раскрывают полный объём выполненных действий или личность человека, осуществившего подключение. Для более обоснованного вывода необходимо учитывать данные аутентификации, настройки инфраструктуры, сведения о времени, конфигурацию сетевых устройств и иные доступные материалы. Дополнительные трудности возникают при исследовании зашифрованного сетевого трафика, использовании виртуальных частных сетей, прокси-сервисов и распределённых систем. В подобных ситуациях содержание передаваемой информации может быть недоступно для непосредственного анализа, а отдельные сетевые адреса могут принадлежать посреднической инфраструктуре. Поэтому эксперт должен разграничивать установленные технические факты, вероятностные выводы и обстоятельства, которые невозможно подтвердить представленными материалами. Отдельное значение имеет исследование

вредоносного программного обеспечения и подозрительных файлов. Оно может включать анализ структуры исполняемого файла, его метаданных, импортируемых библиотек, строковых данных, цифровых подписей и поведения в контролируемой среде. При необходимости используются изолированные лабораторные системы, позволяющие снизить риск воздействия вредоносного кода на рабочую инфраструктуру. Результаты такого анализа могут способствовать выявлению функционального назначения программы, признаков взаимодействия с внешними серверами и способов изменения данных на исследуемом устройстве. Однако обнаружение вредоносного файла не всегда подтверждает факт его фактического запуска или успешного выполнения всех предусмотренных функций. Для установления соответствующих обстоятельств требуется исследование дополнительных следов, включая журналы событий, артефакты выполнения программ и сетевую активность. Следовательно, анализ сетевых следов и вредоносного программного обеспечения должен осуществляться в рамках комплексной методики, обеспечивающей проверяемость результатов и обоснованность экспертных выводов. Процессуальные требования и доказательственное значение результатов цифровой экспертизы. Техническая достоверность цифрового исследования является необходимым, но не единственным условием использования его результатов в судопроизводстве. Не менее важным выступает соблюдение процессуального порядка назначения и проведения экспертизы, законность получения исходных материалов и надлежащее оформление результатов. Конкретные требования определяются законодательством соответствующего государства, характером производства и полномочиями участников процесса. Поэтому при проведении цифровой экспертизы необходимо учитывать нормы, регулирующие собирание, проверку и оценку доказательств, порядок назначения экспертизы, права участников процесса и требования к экспертному заключению. Эксперт должен действовать в пределах своей компетенции и разрешать вопросы, требующие специальных знаний. При этом установление правовой квалификации деяния, определение виновности конкретного лица и решение иных вопросов, относящихся исключительно к полномочиям следователя, прокурора или суда, не должны подменяться техническими выводами эксперта. Например, эксперт может установить наличие определённого файла на носителе, выявить признаки его изменения и описать обнаруженные технические связи. Однако вопрос о том, образуют ли установленные обстоятельства состав преступления и какое юридическое значение им следует придать, разрешается уполномоченными субъектами в рамках соответствующего процессуального решения. Важнейшим документом, отражающим результаты исследования, является заключение эксперта. Оно должно содержать описание представленных объектов и материалов, поставленных вопросов, использованных методов, последовательности существенных исследовательских действий, полученных результатов и обоснования выводов. Изложение должно быть логичным, понятным и проверяемым. При необходимости указываются применённые программные инструменты, их версии, параметры обработки, контрольные значения цифровых копий и ограничения, повлиявшие на

полноту исследования. Если отдельные вопросы не могут быть разрешены из-за недостаточности материалов, технических ограничений или отсутствия необходимых исходных данных, это должно быть отражено в заключении с соответствующим обоснованием. Категоричность выводов должна соответствовать реальному объёму полученной информации. Использование вероятностных формулировок допустимо в тех случаях, когда характер данных не позволяет сделать однозначный вывод. Кроме того, экспертное заключение не должно содержать утверждений, которые выходят за пределы проведённого исследования или не подтверждаются установленными фактами. Важное значение имеет воспроизводимость исследования. Она предполагает наличие достаточной документации для понимания того, каким образом получены результаты, какие инструменты использовались и какие ограничения могли повлиять на анализ. Полная повторяемость всех операций не всегда возможна из-за особенностей оборудования, изменения программных сред или ограниченного доступа к внешним сервисам. Тем не менее эксперт должен обеспечить максимально возможную проверяемость применённых методов и обоснованность полученных результатов. Такой подход способствует повышению доверия к заключению и позволяет другим специалистам оценить его научную состоятельность. Основные проблемы и ограничения проведения цифровых экспертиз. Несмотря на развитие технических средств и методик цифровой криминалистики, проведение цифровых экспертиз сопровождается рядом проблем, требующих комплексного решения. Одной из них является быстрый темп обновления информационных технологий. Новые модели устройств, версии операционных систем, файловые форматы и способы хранения данных могут появляться быстрее, чем разрабатываются и проходят практическую проверку соответствующие экспертные методики. Вследствие этого экспертные подразделения нуждаются в постоянном обновлении программно-технических комплексов и регулярном повышении квалификации специалистов. Другой проблемой выступает использование современных механизмов шифрования. Шифрование обеспечивает защиту конфиденциальности информации, однако при отсутствии необходимых ключей или законного способа доступа оно может существенно ограничивать возможности извлечения данных. При этом наличие технических средств для исследования устройства не означает, что эксперт имеет возможность обойти все предусмотренные механизмы защиты. Поэтому необходимо учитывать технические ограничения, соблюдать правовые требования и использовать доступные законные методы получения информации. Серьёзным затруднением остаётся неоднородность цифровых данных. Информация может храниться в различных форматах, распределяться между несколькими устройствами и сервисами, дублироваться в резервных копиях и изменяться вследствие автоматической синхронизации. Объём цифровых материалов в крупных расследованиях может достигать значительных масштабов, что затрудняет их ручную обработку. В таких случаях используются автоматизированные средства поиска, индексирования, классификации и анализа данных. Однако автоматизация также создаёт риски, связанные с ошибками программных алгоритмов, неполнотой обработки,

неправильной интерпретацией результатов и чрезмерным доверием к автоматически сформированным выводам. Поэтому результаты автоматизированного анализа должны подвергаться профессиональной проверке, особенно если они используются для обоснования существенных выводов. Отдельную проблему представляет дефицит квалифицированных специалистов. Цифровая экспертиза требует сочетания знаний в области операционных систем, компьютерных сетей, информационной безопасности, программирования, криминалистики и процессуального законодательства. Подготовка таких специалистов предполагает не только теоретическое обучение, но и регулярную практическую работу с современными инструментами, изучение новых способов совершения киберпреступлений и освоение методик исследования различных типов цифровых объектов. Дополнительные сложности могут быть связаны с недостаточным техническим оснащением экспертных подразделений, ограниченным доступом к лицензированным программным продуктам и отсутствием единых внутренних процедур документирования исследований. Существенное значение имеет также обеспечение конфиденциальности и защита персональных данных. Электронные устройства могут содержать значительный объём сведений о частной жизни, финансовых операциях, состоянии здоровья и личных коммуникациях. В связи с этим исследование должно ограничиваться задачами, имеющими отношение к назначенной экспертизе, и осуществляться с соблюдением применимых правовых требований. Получение доступа к информации не должно автоматически рассматриваться как основание для неограниченного изучения всех содержащихся в устройстве сведений. Соблюдение принципов законности, необходимости и соразмерности позволяет сочетать эффективность экспертной деятельности с защитой прав и законных интересов граждан. Ещё одним ограничением является сложность подтверждения происхождения цифровых данных. Отдельные файлы и сообщения могут копироваться между устройствами, изменяться с помощью программных средств или размещаться под различными учётными записями. В некоторых случаях невозможно достоверно установить конкретного автора информации только на основании технических свойств файла. Поэтому эксперт должен учитывать альтернативные объяснения происхождения данных и избегать необоснованного отождествления технического источника с определённым человеком. Для решения подобных задач требуется сопоставление цифровых следов с другими доказательствами, включая документы, показания, результаты иных экспертиз и сведения, полученные в установленном законом порядке. Перспективы совершенствования цифровой экспертной деятельности. Совершенствование цифровых экспертиз предполагает развитие нескольких взаимосвязанных направлений, включающих техническое оснащение, методическое обеспечение, подготовку кадров, организацию экспертного процесса и международное взаимодействие. Прежде всего необходимо систематически обновлять лабораторное оборудование и программно-технические комплексы с учётом современных типов электронных устройств, новых файловых систем и распространённых способов хранения информации. При выборе специализированных инструментов следует учитывать их функциональные возможности,

документированность алгоритмов, надёжность результатов и возможность независимой проверки. Использование программных средств, прошедших соответствующее тестирование, позволяет уменьшить риск технических ошибок и повысить качество экспертных исследований. Вместе с тем приобретение современного оборудования должно сопровождаться разработкой методических рекомендаций и подготовкой специалистов, способных правильно применять доступные инструменты. Важным направлением является стандартизация процедур обнаружения, изъятия, копирования, хранения и исследования цифровых данных. Разработка единых требований к документированию действий, контролю целостности, ведению учёта объектов и оформлению экспертных заключений способствует повышению сопоставимости результатов, полученных разными экспертами и учреждениями. При этом стандартизация не должна ограничивать возможность адаптации методики к особенностям конкретного объекта. Напротив, общие требования должны сочетаться с научно обоснованными специализированными процедурами для исследования мобильных устройств, облачных данных, сетевых следов, мультимедийных материалов и других цифровых объектов. Перспективным направлением выступает развитие систем автоматизированного анализа больших объёмов информации. Технологии машинного обучения и искусственного интеллекта могут применяться для предварительной классификации файлов, выявления сходных объектов, обнаружения аномалий в сетевых журналах и формирования поисковых наборов. Их использование позволяет ускорить обработку значительных массивов данных и сосредоточить внимание эксперта на наиболее существенных материалах. Однако автоматизированные системы могут допускать ошибки, зависеть от качества обучающих данных и затруднять объяснение отдельных результатов. Поэтому искусственный интеллект целесообразно рассматривать как вспомогательный инструмент, а не как замену экспертной оценки. Решения, имеющие существенное значение для выводов экспертизы, должны проверяться специалистом с учётом исходных данных, ограничений алгоритма и возможности альтернативной интерпретации. Не менее важна организация непрерывного профессионального обучения экспертов. Образовательные программы должны охватывать основы цифровой криминалистики, методы анализа операционных систем и сетевых данных, особенности исследования мобильных устройств, механизмы шифрования, правила обеспечения целостности информации и требования процессуального законодательства. Практическая подготовка должна включать работу с учебными образцами цифровых носителей, моделирование различных ситуаций и проверку правильности оформления экспертных заключений. В целях повышения качества исследований целесообразно развивать межведомственное сотрудничество между экспертными учреждениями, правоохранительными органами, научными организациями и образовательными учреждениями. Обмен обезличенными практическими материалами, проведение научно-практических конференций и разработка совместных методических рекомендаций могут способствовать распространению эффективных подходов и повышению профессионального уровня

специалистов. Отдельное значение имеет международное сотрудничество в сфере получения и исследования трансграничных цифровых данных. Учитывая распределённый характер современной информационной инфраструктуры, расследование отдельных преступлений может требовать взаимодействия с иностранными компетентными органами и поставщиками цифровых услуг. Эффективное сотрудничество предполагает соблюдение национального законодательства, применимых международных соглашений и процедур, обеспечивающих законность получения информации и сохранение её доказательственной ценности. Важным условием развития цифровой экспертной деятельности является совершенствование научно-методической базы. Необходимо проводить исследования, направленные на оценку точности программных инструментов, изучение особенностей новых технологий хранения данных и разработку способов проверки достоверности результатов. Результаты таких исследований должны внедряться в практику после соответствующей научной и технической оценки. Кроме того, целесообразно расширять применение процедур внутреннего контроля качества и независимой проверки экспертных исследований, особенно в сложных случаях, связанных с большими массивами данных, зашифрованными устройствами и противоречивыми цифровыми следами. В совокупности указанные меры способны повысить научную обоснованность, объективность и эффективность цифровой экспертизы. Таким образом, специфические особенности проведения цифровых экспертиз определяются сложной природой цифровых данных, их изменчивостью, многообразием источников и необходимостью сочетания технических методов исследования с процессуальными гарантиями. Эффективность экспертной деятельности зависит от правильного обнаружения и сохранения цифровых следов, применения проверенных методов извлечения и анализа информации, документирования исследовательских операций и обоснованного представления результатов. При этом цифровая экспертиза должна осуществляться с учётом технических ограничений, требований законодательства, принципов защиты персональных данных и необходимости обеспечения возможности независимой проверки полученных выводов. Дальнейшее развитие данного направления связано с внедрением научно обоснованных методик, модернизацией технической базы, подготовкой квалифицированных кадров и расширением межведомственного и международного сотрудничества.

ЗАКЛЮЧЕНИЕ

Проведённое исследование специфических особенностей проведения цифровых экспертиз позволяет сделать вывод о том, что в условиях стремительной цифровизации общественных отношений и широкого распространения информационных технологий данное направление судебно-экспертной деятельности приобретает особое научное и практическое значение. Цифровая информация всё чаще выступает важным источником сведений об обстоятельствах совершения правонарушений и преступлений, способствуя установлению последовательности событий, выявлению взаимосвязей между участниками противоправной деятельности и проверке

следственных версий. Вместе с тем особенности цифровых данных, включая их изменчивость, возможность незаметного копирования и модификации, зависимость от технической среды и сложности восстановления удалённой информации, предъявляют повышенные требования к организации и проведению экспертных исследований. Установлено, что важнейшими условиями обеспечения достоверности результатов цифровой экспертизы являются правильное обнаружение и процессуальная фиксация цифровых следов, соблюдение установленного порядка изъятия и хранения электронных носителей, применение научно обоснованных методов исследования и обеспечение целостности исходных данных. Использование криминалистических копий, криптографических хеш-функций и специализированных программно-технических средств позволяет повысить надёжность исследования и создать условия для проверки полученных результатов. Однако применение отдельных технических инструментов само по себе не гарантирует достоверности выводов, поскольку необходимо также учитывать происхождение информации, законность её получения, особенности функционирования исследуемых устройств и ограничения используемых методов. В ходе исследования установлено, что цифровая экспертиза охватывает различные направления, включая компьютерно-технические исследования, экспертизу мобильных устройств, анализ цифровых изображений и видеозаписей, исследование сетевых следов и изучение данных, размещённых в облачных хранилищах. Каждое из указанных направлений характеризуется специфическими объектами, методами и техническими ограничениями, что обуславливает необходимость дифференцированного подхода к организации экспертной деятельности. Особое значение имеет комплексный анализ цифровых данных из нескольких независимых источников, позволяющий сопоставлять результаты исследования и устанавливать возможные противоречия. При этом экспертные выводы должны соответствовать фактическому содержанию исследованных материалов и не выходить за пределы специальных знаний. Отдельного внимания заслуживает соблюдение процессуальных требований при назначении и проведении цифровых экспертиз. Даже технически обоснованные результаты могут утратить доказательственное значение при нарушении установленного порядка получения, фиксации и представления соответствующих материалов. Поэтому экспертное заключение должно содержать последовательное описание исследовательских действий, применённых методов и технических средств, полученных результатов и оснований сформулированных выводов. Необходимо также указывать ограничения исследования, если они влияют на полноту или достоверность полученных сведений. Такой подход способствует повышению прозрачности экспертной деятельности, обеспечивает возможность проверки результатов и укрепляет доверие к выводам специалиста. Вместе с тем проведённый анализ позволяет выделить ряд проблем, затрудняющих развитие цифровой экспертизы. К ним относятся быстрое обновление информационных технологий, распространение сложных механизмов шифрования, увеличение объёма исследуемых данных, недостаточная унификация отдельных экспертных методик, необходимость постоянного обновления технического оснащения и дефицит специалистов,

обладающих комплексными знаниями в области цифровой криминалистики и процессуального права. Дополнительные трудности возникают при исследовании облачных сервисов и трансграничных цифровых данных, когда получение необходимой информации зависит от технических возможностей, правовых процедур и взаимодействия компетентных органов разных государств. В целях совершенствования цифровой экспертной деятельности представляется необходимым развивать научно-методическую базу, внедрять проверенные программно-технические комплексы, совершенствовать процедуры документирования и контроля целостности цифровых данных, а также обеспечивать систематическое повышение квалификации экспертов. Перспективным направлением является применение автоматизированных инструментов обработки больших массивов информации и технологий искусственного интеллекта для предварительного поиска, классификации и выявления закономерностей в цифровых материалах. Вместе с тем результаты автоматизированного анализа должны проверяться квалифицированным специалистом, а выводы экспертизы — основываться на проверяемых данных и научно обоснованных методах. Не менее важными являются развитие межведомственного взаимодействия, обмен профессиональным опытом, проведение совместных научных исследований и совершенствование международного сотрудничества в сфере получения и исследования цифровых доказательств. Таким образом, цифровая экспертиза представляет собой сложное междисциплинарное направление, эффективность которого определяется сочетанием технической компетентности эксперта, научной обоснованности применяемых методов, соблюдения процессуальных требований и обеспечения прав участников судопроизводства. Её дальнейшее совершенствование должно быть направлено на повышение объективности и полноты исследования, обеспечение сохранности цифровой информации, развитие единых методических подходов и укрепление гарантий достоверности экспертных заключений. Реализация указанных мер позволит повысить эффективность использования цифровых доказательств при раскрытии и расследовании преступлений, укрепить доказательственную базу и обеспечить более качественное применение специальных знаний в современных условиях развития информационного общества.

ИСПОЛЬЗОВАННЫЕ ЛИТЕРАТУРНЫЕ ИСТОЧНИКИ:

- ✧ The Rise of the Network Society
Castells, M. (1996). *The Rise of the Network Society*. Oxford: Blackwell Publishers.
- ✧ Security Engineering
Anderson, R. (2008). *Security Engineering: A Guide to Building Dependable Distributed Systems* (2nd ed.). Indianapolis: Wiley.
- ✧ Secrets and Lies
Schneier, B. (2000). *Secrets and Lies: Digital Security in a Networked World*. New York: Wiley.

✧ Regulating

Blockchain

Hacker, P., Lianos, I., Dimitropoulos, G., & Eich, S. (eds.). (2020). *Regulating Blockchain: Techno-Social and Legal Challenges*. Oxford: Oxford University Press.

✧ Soft Law and the Global Financial System

Brummer, C. (2012). *Soft Law and the Global Financial System*. Cambridge: Cambridge University Press.