

Приходько Юрий Сергеевич

студент магистратуры
Московский университет им. С.Ю. Витте
Москва, Россия

Уварова Ирина Александровна

заведующий кафедрой уголовного права и процесса
Московский университет им. С.Ю. Витте
Москва, Россия

**ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ СПЕЦИАЛЬНЫХ ЗНАНИЙ
ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В ЦИФРОВОЙ СРЕДЕ****Аннотация**

С учётом стремительного развития цифровых технологий, а также усложнения способов фиксации и анализа цифровых следов преступлений, актуализируется задача нормативного закрепления процессуальных особенностей использования специальных знаний при производстве экспертных исследований, связанных с информацией в электронной форме. Современное состояние уголовно-процессуального законодательства не содержит специальных положений, отражающих специфику назначения и проведения экспертиз, предметом которых выступают цифровые данные. Между тем, именно такие объекты всё чаще становятся решающими с точки зрения доказывания обстоятельств совершённого преступления, особенно в делах, связанных с компьютерными преступлениями, мошенничеством с использованием информационно-телекоммуникационных сетей, незаконным оборотом данных, распространением вредоносного программного оборудования и иных противоправных деяний, совершаемых в цифровой среде. Предлагаются изменения в уголовно-процессуальный кодекс Российской Федерации, направленные на устранение правовых пробелов и повышение эффективности расследования цифровых преступлений с использованием специальных знаний.

Ключевые слова: специальные знания, цифровая среда, уголовный процесс, судебная экспертиза

Современный этап цифровизации оказывает принципиальное влияние на трансформацию способов совершения преступлений и, как следствие, на характер и методы их расследования. Расширение круга противоправных деяний, совершаемых с использованием компьютерных технологий и глобальных сетей, выдвигает новые требования к качеству собираемой доказательственной базы, в том числе к степени научной обоснованности специальных знаний, используемых следователем. При этом содержание самого понятия «специальные знания» в условиях цифровой среды требует дополнительного теоретического осмысления и нормативной конкретизации.

Расследование преступлений, совершаемых с использованием цифровых технологий, требует от органов предварительного расследования привлечения специальных знаний, без которых невозможно обеспечить полноту, объективность и достоверность доказывания. Расширение сферы цифровых взаимодействий предопределяет необходимость интеграции в уголовно-процессуальную деятельность соответствующих экспертных и технических подходов, в том числе с привлечением

специалистов в области информационной безопасности, программирования, цифровой криминалистики.

Согласно статье 73 Уголовно-процессуального кодекса Российской Федерации (далее – УПК РФ [3]), предметом доказывания являются, в том числе, сведения о способе совершения преступления, а также о средствах и инструментах, применявшихся при его совершении. Раскрытие данных обстоятельств применительно к расследованию преступлений, совершаемых в цифровой среде, предполагает качественно иную доказательственную работу, поскольку в большинстве случаев следовая информация представлена в электронно-цифровом формате и не воспринимается без применения технических средств.

Так, в отличие от традиционных способов фиксации следов преступной деятельности (отпечатки, предметы, документы), цифровые следы, оставляемые при совершении преступлений с использованием информационно-коммуникационных технологий, имеют нефизическую природу и хранятся в распределённых и часто удалённых средах. К ним относятся, прежде всего, лог-файлы, временные файлы, журналы активности, метаданные сетевых соединений, следы удалённого доступа, данные о маршрутизации пакетов, а также остаточные файлы, зафиксированные в кэше устройств или серверных хранилищах. Без привлечения специальных знаний в области сетевых протоколов, криптографии, архитектуры операционных систем сложно выявить, интерпретировать и закрепить такие сведения. Кроме того, специфика цифровых доказательств проявляется в их высокой изменчивости, нестабильности и уязвимости к воздействию. Любое неосторожное действие следователя или оперативного сотрудника может привести к утрате значимых сведений, что делает участие специалиста в расследовании цифровых преступлений не просто желательным, а фактически обязательным. Следует подчеркнуть, что даже установление субъекта преступления в киберпространстве возможно лишь при технически корректной атрибуции IP-адресов, устройств и конкретных программных сред, с чем сопряжено применение как отечественных, так и международных стандартов киберэкспертизы.

Под специальными знаниями в теории уголовного процесса традиционно понимаются знания, выходящие за пределы общеобразовательной и правовой подготовки участников процесса, и применяемые для получения, проверки, оценки и использования доказательственной информации [2, с. 183]. Использование

специальных знаний возможно в двух формах – не процессуальной (участие специалиста) и процессуальной (проведение экспертизы). Специалист может быть привлечён на стадии осмотра места происшествия, при выемке и анализе цифровой информации, а эксперт на стадии проведения экспертизы с целью установления технических характеристик цифровых следов, восстановления удалённой информации, выявления признаков несанкционированного вмешательства [1, с. 229].

Применительно к цифровой среде специальные знания охватывают в том числе сферу программирования, информационной безопасности, цифровой криминалистики, телекоммуникационных технологий. Законодательное регулирование их использования основывается на положениях главы 8 УПК РФ, в частности, статей 57, 58 и 168, которые предусматривают возможность участия эксперта и специалиста в следственных действиях. Однако особенности применения этих знаний применительно к расследованию преступлений, совершаемых в цифровой среде, в действующем законодательстве не конкретизированы.

Развитие киберугроз привело к возникновению и активному использованию таких направлений, как компьютерно-техническая экспертиза, лингвистическая экспертиза интернет-коммуникаций, трасологический анализ цифровых следов, анализ лог-файлов и метаданных. Каждое из этих направлений опирается на определённую совокупность специальных знаний, требующих не только высокой квалификации, но и понимания особенностей цифровой инфраструктуры, включая распределённые вычисления, шифрование, анонимизацию трафика.

Федеральный закон от 31.05.2001 № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации» закрепляет возможность проведения экспертных исследований с применением технических и цифровых средств [4]. Однако в действующем законодательстве не представлены ни перечни методов, ни классификация видов экспертиз, адаптированных к преступлениям в цифровой среде.

Следующей значимой проблемой является отсутствие системного подхода к процессу нормативного закрепления квалификационных требований к экспертам в области цифровых технологий. Специалисты в сфере IT, привлекаемые в уголовный процесс, часто не обладают правовой подготовкой, что снижает эффективность их участия в следственных действиях. В то же время профессиональные судебные эксперты зачастую не располагают необходимыми знаниями в области современных

цифровых архитектур, протоколов и форматов данных. Кроме того, отсутствует единый нормативный акт, регулирующий взаимодействие следователей с поставщиками цифровых сервисов и хостинг-провайдерами, а также порядок извлечения и сохранения цифровой информации, обладающей доказательственным значением. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», формулирует лишь общие положения о работе с информацией, не устанавливая процедурной регламентации для уголовно-процессуальных целей [5].

Исходя из анализа представленных проблем, целесообразным представляется нормативное закрепление следующего авторского определения: «специальные знания в цифровой среде – это систематизированные сведения технического, математического, программного, телекоммуникационного и иного прикладного характера, позволяющие выявлять, анализировать, интерпретировать и использовать информацию, зафиксированную в цифровом формате, в целях установления обстоятельств, подлежащих доказыванию по уголовному делу».

С учетом возможностей формирования единообразия практики применения специальных знаний при расследовании преступлений, совершаемых в цифровой среде, представляется обоснованным предложение о дополнении УПК РФ специальной нормой, в которой установить, что при назначении экспертизы, объектом которой является информация, зафиксированная в цифровом формате, следователь обязан конкретизировать технические средства, методы и программное обеспечение, предполагаемые к использованию в ходе исследования. Полагаем, такой подход направлен на обеспечение воспроизводимости результатов и возможности последующего контроля со стороны суда и участников процесса за соблюдением условий достоверности и допустимости заключения эксперта.

Рекомендуется также законодательно закрепить, что к производству указанной категории экспертиз могут быть допущены исключительно лица, обладающие профильной квалификацией в области информационных технологий, подтвержденной соответствующими документами, и позволяющей им осуществлять квалифицированную интерпретацию цифровых артефактов, метаданных, логов, остаточной информации, а также обеспечивать верификацию данных в условиях нестандартных форматов, распределённых хранилищ и зашифрованных систем.

Кроме того, полагаем обоснованным нормативное закрепление требования, согласно которому экспертное заключение, подготовленное по результатам анализа цифровых объектов, должно составляться в форме электронного документа и подписываться усиленной квалифицированной электронной подписью эксперта. Такой подход отвечает как требованиям юридической достоверности, так и условиям надёжного удостоверения подлинности экспертных выводов. Приобщение заключения к материалам уголовного дела в электронной форме обеспечит его дальнейшее использование в рамках цифрового документооборота, что особенно актуально в условиях активного внедрения электронных технологий в сферу уголовного судопроизводства.

Таким образом, несмотря на наличие в статье 73 Уголовно-процессуального кодекса Российской Федерации прямого указания на необходимость установления способа совершения преступления и средств, использованных при этом, в сфере цифровых преступлений полноценное установление таких сведений возможно исключительно с использованием специальных знаний, позволяющих квалифицированно идентифицировать цифровые следы, проследить действия субъекта в информационной среде, восстановить последовательность событий и проверить подлинность полученной информации. Реализация обозначенных перспективных направлений, полагаем, будет способствовать обеспечению единообразия следственной практики, устранению неопределённости при производстве цифровых экспертиз, а также укреплению гарантий достоверности полученных доказательств.

Список использованных источников

1. Каипецкая А.А. Особенности применения специальных знаний при расследовании преступлений, совершенных с использованием информационно-коммуникационных технологий // Право, общество, государство: системные основы взаимодействия и развития. Москва, 2024. – С. 228-231. – EDN: ZLUSNE.

2. Миронова А.В. Использование специальных знаний в доказывании по делам о преступлениях, совершенных с использованием информационных технологий // Криминалистика: наука, практика, опыт. Москва: Московский университет МВД РФ им. В.Я. Кикотя, 2024. – С. 182-185.

3. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 07.06.2025) // Собрание законодательства РФ. – 2001. – № 52 (ч. I). – Ст. 4921.

4. Федеральный закон от 31.05.2001 № 73-ФЗ (ред. от 22.07.2024) «О государственной судебной-экспертной деятельности в Российской Федерации» // Собрание законодательства РФ. – 2001. – № 23. – Ст. 2291.

5. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 01.04.2025) «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. – 2006. – № 31 (1 ч.). – Ст. 3448.