ПРАВОВЫЕ И КРИМИНАЛИСТИЧЕСКИЕ ОСОБЕННОСТИ ПОЛУЧЕНИЯ ОБРАЗЦОВ ДЛЯ КОМПЬЮТЕРНО-ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ ПРИ РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ

Парахатова Шахноза Ерназаровна
Докторант Ташкентского государственного юридического университета направления 12.00.09. Уголовный процесс. Криминалистика, оперативно-розыскное право и судебная экспертиза.
https://doi.org/10.5281/zenodo.18713187

Стремительное развитие информационно-коммуникационных технологий и их повсеместная интеграция во все сферы общественной жизни обусловили качественные изменения в характере и структуре преступности. В условиях цифровой трансформации общества киберпреступления становятся одной из наиболее динамично развивающихся форм противоправной деятельности, представляющих повышенную общественную опасность. Их отличительными особенностями являются трансграничность, анонимность, высокая латентность и сложность выявления следов преступления. Указанные характеристики существенно осложняют деятельность правоохранительных органов и требуют пересмотра традиционных криминалистических подходов к раскрытию и расследованию преступлений.

Особое место в системе противодействия киберпреступности занимает компьютерно-техническая экспертиза, являющаяся одним из ключевых средств получения и исследования цифровых доказательств. Эффективность данной экспертизы во многом определяется правильностью и законностью получения образцов для экспертного исследования, поскольку любые нарушения на данном этапе могут повлечь утрату доказательственной информации либо поставить под сомнение её допустимость и достоверность в уголовном процессе.

В уголовном процессе Республики Узбекистан институт получения образцов для экспертного исследования традиционно рассматривался применительно к материальным объектам, обладающим физическими и химическими свойствами. Однако цифровая среда принципиально отличается от материального мира, что обусловливает необходимость переосмысления понятия образцов, их процессуальной природы и порядка получения в рамках компьютерно-технической экспертизы. В этой связи актуализируется проблема научного осмысления правовых и криминалистических особенностей получения цифровых образцов, а также выработки рекомендаций, направленных на совершенствование правоприменительной практики при расследовании киберпреступлений.

Компьютерно-техническая экспертиза относится к классу инженерно-технических экспертиз и проводится в целях исследования электронных устройств, программного обеспечения и содержащейся в них информации. В рамках расследования киберпреступлений данный вид экспертизы позволяет установить статус объекта как компьютерного средства, определить его роль в механизме преступления, а также выявить, зафиксировать и проанализировать цифровую информацию, имеющую доказательственное значение. В научной литературе отсутствует единый подход к наименованию данного вида экспертизы: используются термины «компьютерная экспертиза», «программно-техническая экспертиза», «компьютерно-программная

экспертиза» и др. Однако независимо от терминологии, её сущность заключается в исследовании цифровых следов, образующихся в результате функционирования электронных устройств и информационных систем.

Особенность цифровых следов заключается в их нематериальной природе, изменяемости и высокой уязвимости к внешнему воздействию. В отличие от традиционных вещественных доказательств, цифровые данные могут быть уничтожены, искажены или изменены без видимых следов, в том числе дистанционно. Это обусловливает повышенные требования к процессу получения, фиксации и хранения цифровых образцов, предназначенных для экспертного исследования.

В соответствии со статьёй 204 Уголовно-процессуального кодекса Республики Узбекистан цифровыми доказательствами признаются электронные данные, содержащие сведения об обстоятельствах, имеющих значение для уголовного дела, включая электронные файлы, аудио- и видеозаписи, данные, размещённые в сети Интернет, а также иные электронные сведения[1]. Таким образом, законодатель признаёт цифровые данные самостоятельным видом доказательств, что свидетельствует о формировании в уголовном процессе новой доказательственной категории.

Вместе с тем, процессуальный статус образцов для компьютерно-технической экспертизы остаётся недостаточно разработанным. В теории уголовного процесса образцы традиционно рассматриваются как объекты, получаемые для экспертного исследования и обладающие обеспечительной функцией, поскольку их доказательственное значение реализуется через результаты экспертного заключения. Применительно к цифровой среде данная концепция требует уточнения, поскольку цифровые образцы не существуют в физическом смысле и представляют собой совокупность данных, извлекаемых из электронных носителей. В отличие от биологических, трасологических или почерковедческих образцов, цифровые образцы не обладают материальной формой, доступной для непосредственного восприятия человеком. Они представляют собой логически структурированную информацию, существующую в виде двоичного кода и воспроизводимую только с использованием технических средств.

Исходя из анализа концепции цифровых доказательств, цифровые образцы можно определить как электронные данные, полученные в установленном законом порядке и предназначенные для последующего экспертного исследования с целью установления обстоятельств, имеющих значение для уголовного дела. К таким образцам относятся образы жёстких дисков, логические и физические копии носителей информации, дампы оперативной памяти, журналы событий, сетевые логи, метаданные файлов и иные цифровые следы.

Специфика цифровых образцов проявляется в их высокой чувствительности к любым действиям с электронным устройством. Даже включение или выключение компьютера может привести к изменению системных файлов, временных меток и других параметров, что в дальнейшем может быть расценено как вмешательство в

[1] Уголовно-процессуальный кодекс Республики Узбекистан от 22.09.1994 г. (с изменениями и дополнениями от 26.03.2025 г., № 03/25/1050/0276) https://lex.uz/docs/111463

доказательственную информацию. В этой связи особое значение приобретает соблюдение принципа неизменности цифровых данных, который является одним из фундаментальных принципов цифровой криминалистики. Международная практика, в частности рекомендации Национального совета начальников полиции Соединённого Королевства, исходит из того, что никакие действия правоохранительных органов не должны приводить к изменению данных, которые впоследствии могут быть использованы в суде. Данный принцип предполагает использование специальных технических и организационных мер, направленных на сохранение целостности цифровых образцов.

Ключевым этапом является создание неизменяемой копии цифрового носителя, которая в криминалистической практике именуется «форензик-образом». Для этого используются специальные устройства — блокираторы записи, предотвращающие внесение изменений в исходные данные при их копировании. Подлинность и идентичность копии оригиналу подтверждается путём вычисления хэш-значений с применением криптографических алгоритмов. Совпадение хэш-значений свидетельствует о том, что копия полностью воспроизводит содержание оригинального носителя. Особое внимание должно уделяться изъятию мобильных устройств, поскольку они подвержены удалённому управлению, в том числе удалению данных или их изменению через сетевые соединения. В этой связи в практике цифровой криминалистики широко применяются пакеты и лаборатории на основе принципа клетки Фарадея, обеспечивающие изоляцию устройств от внешних электромагнитных воздействий. Использование таких средств позволяет сохранить цифровые данные в первоначальном виде и минимизировать риск вмешательства со стороны злоумышленников.

Следует отметить, что получение цифровых образцов требует наличия у должностных лиц специальных знаний и навыков. Непрофессиональные действия, такие как самостоятельный просмотр файлов, подключение носителей к незащищённым компьютерам или использование непроверенного программного обеспечения, могут привести к необратимым последствиям и поставить под сомнение результаты экспертизы.

Анализ практики расследования киберпреступлений в Республике Узбекистан показывает, что одной из основных проблем является недостаточная техническая оснащённость следственных органов и нехватка специалистов, обладающих междисциплинарной компетенцией в области права и информационных технологий. В условиях экспоненциального роста киберпреступности данные проблемы приобретают системный характер и требуют комплексного решения. Не менее важным является развитие специализированных лабораторий, оснащённых современными техническими средствами и построенных с учётом требований информационной безопасности. Международные стандарты, отражённые в O‘z DSt 3386:2019 (ISO/IEC 27035-1:2016, MOD)[2], подчёркивают необходимость структурированного подхода к управлению инцидентами информационной безопасности и обеспечению целостности

[2] Государственный стандарт Республики Узбекистан «Информационная технология. Методы обеспечения безопасности. Управление инцидентами информационной безопасности. Часть 1. Принципы управления инцидентами (ISO/IEC 27035-1:2016, MOD)» https://csec.uz/ru/docs/OzDSt_27035_2019_1.pdf

электронных доказательств. Их внедрение в практику правоохранительных органов позволит повысить доверие к результатам компьютерно-технической экспертизы и укрепить доказательственную базу по делам о киберпреступлениях.

Проведённое исследование позволяет сделать вывод о том, что получение образцов для компьютерно-технической экспертизы при расследовании киберпреступлений представляет собой самостоятельную и сложную криминалистическую деятельность, требующую специального правового регулирования, технического обеспечения и профессиональной подготовки кадров. Цифровые образцы обладают специфической природой, отличающей их от традиционных материальных объектов, что обусловливает необходимость разработки специализированных методик их получения и исследования.