УГОЛОВНО-ПРОЦЕССУАЛЬНОЕ ЗНАЧЕНИЕ ЦИФРОВЫХ СВЕДЕНИЙ В СИСТЕМЕ ДОКАЗАТЕЛЬСТВЕННОГО ПРАВА

Собиров Шохрухбек Таваккалович
Ведущий научный сотрудник Института законодательства и правовой политики при Президенте Республики Узбекистан

В эпоху стремительной цифровизации ландшафт уголовного судопроизводства значительно изменился. С появлением цифровых носителей появилась новая форма доказательств – цифровые доказательства, которые включают в себя любую информацию, сохраненную или переданную в цифровой форме, которая может быть использована в судебном процессе. К ним относятся, в частности, электронные письма, текстовые сообщения, сообщения в социальных сетях и цифровые фотографии. Повсеместное распространение цифровых устройств и огромное количество генерируемых ими данных сделали цифровые доказательства все более важным компонентом уголовных расследований и судебных процессов.

Однако интеграция цифровых доказательств в правовую систему не лишена трудностей. Уникальные характеристики цифровых доказательств, такие как их изменчивость, воспроизводимость и подверженность изменениям, создают значительные проблемы, связанные с их подлинностью, целостностью и допустимостью. Более того, быстрые темпы технического прогресса часто опережают развитие правовых норм и практики, что создает пробел, который необходимо устранить и эта тенденция обусловлена повсеместной цифровизацией общества.

Сегодня повседневная деятельность общества, работа, коммуникация и сделки все чаще происходят в цифровой сфере, что делает цифровые данные бесценным инструментом в расследовании и преследовании широкого спектра преступлений. Они варьируются от киберпреступлений, таких как хакерство и онлайн-мошенничество, до традиционных преступлений, таких как кражи, нападения и даже убийства.

Потенциальными источниками цифровых доказательств могут быть персональные устройства, такие как смартфоны, компьютеры, которые содержат огромное количество информации. Журналы звонков, текстовые сообщения, электронные письма, история просмотров, данные о местоположении и файлы и др.

Однако сегодня сфера применения цифровых доказательств выходит за рамки персональных устройств. Онлайн-платформы и цифровые каналы связи также служат важными источниками цифровых доказательств.

Платформы социальных сетей, например, могут предоставить доказательства в виде сообщений, комментариев, «лайков», «долей» и списков друзей. Цифровые каналы связи, такие как приложения для обмена сообщениями и службы электронной почты, могут содержать важнейшие доказательства в виде сообщений и вложений.

Кроме того, ценными источниками цифровых доказательств могут быть облачные хранилища, интернет-провайдеры и цифровые платежные платформы. Каждый из этих источников представляет собой уникальные проблемы и соображения с точки зрения извлечения, сохранения и допустимости цифровых данных.

Сбор цифровой информации (или цифровых улик) должен осуществляться в соответствии с правовыми принципами и процедурами, обеспечивающими их приемлемость в суде. Как правило, это предполагает получение санкции на обыск, а также соблюдение определенных процедур, обеспечивающих сбор доказательств таким образом, чтобы сохранить их целостность и подлинность. Несоблюдение этих процедур может привести к тому, что доказательства будут исключены из судебного разбирательства.

Сохранение цифровых улик – еще один важный аспект законодательной базы. Учитывая изменчивый характер цифровых данных, требуются специальные методы и процедуры для обеспечения сохранности цифровых улик в их первоначальном виде до представления судье. Это включает в себя создание криминалистических копий цифровых данных, соблюдение цепочки хранения и хранение доказательств в безопасной среде.

Анализ цифровых улик обычно проводится экспертами в области цифровой криминалистики, которые должны следовать установленным методикам и стандартам для обеспечения точности и надежности своих выводов. Результаты их анализа могут дать решающее представление об уликах и могут быть представлены в суде в качестве экспертных показаний.

Наконец, представление цифровых улик в качестве доказательств в суде предполагает демонстрацию их значимости, подлинности и надежности судье. Это часто требует объяснения сложных технических концепций в понятной для нетехнических специалистов манере.

Одной из основных технических проблем является обеспечение подлинности и целостности цифровых улик. Учитывая легкость, с которой цифровые данные могут быть манипулированы или изменены, установить достоверность цифровых улик бывает непросто. Это требует использования сложных методов и инструментов цифровой криминалистики, а также опыта специалистов в области цифровой криминалистики.

С юридической точки зрения приемлемость цифровых доказательств в суде может представлять собой серьезную проблему. Для этого необходимо продемонстрировать, что цифровые улики являются релевантными, подлинными и надежными, а также что они были собраны и сохранены в соответствии с правовыми принципами и процедурами. Быстрые темпы технологических изменений часто опережают развитие правовых норм и практики, что приводит к возникновению пробелов, которые необходимо устранить.

Техническая природа цифровых данных. Цифровые данные могут принимать различные формы, от текстовых сообщений и электронных писем до цифровых фотографий, видео и метаданных с двоичным кодом. Каждый вид цифровых данных требует определенных методов и инструментов для сбора, сохранения и анализа. Например:

1. Нестабильность. Цифровые доказательства часто хранятся в нестабильной памяти, например, в оперативной, что означает, что их можно легко потерять или изменить. После выключения компьютерной системы доказательства, хранящиеся в энергозависимой памяти, как правило, теряются. Это делает сохранение цифровых доказательств технически сложной задачей.

2. Объем. Объем потенциальных цифровых доказательств может быть просто ошеломляющим. При терабайтах данных, хранящихся на личных и корпоративных устройствах, выявление и извлечение соответствующих доказательств похоже на поиск иголки в стоге сена.

3. Разнообразие. Цифровые доказательства могут иметь самые разные форматы, от различных типов файлов и баз данных до различных интернет-протоколов и приложений. Каждый тип требует специальных технических знаний для надлежащей обработки.

4. Хрупкость. Цифровые доказательства могут быть легко изменены, повреждены или уничтожены как преднамеренно, так и непреднамеренно. Это делает работу с цифровыми доказательствами и их сохранение деликатным процессом.

5. Шифрование и анонимность. Технологии шифрования могут затруднить доступ к цифровым доказательствам, а сети и методы анонимности могут затруднить отслеживание цифровой деятельности.

6. Межюрисдикционные вопросы. Цифровые доказательства могут храниться или передаваться в разных юрисдикциях, что может создать технические и юридические проблемы при доступе и использовании доказательств.

7. Быстрые технологические изменения. Постоянное развитие технологий означает, что постоянно появляются новые типы цифровых доказательств, а старые типы устаревают. Это требует от специалистов по цифровой криминалистике постоянного обновления своих навыков и инструментов.

Отсутствие регламентированных стандартов сбора и анализа цифровых доказательств, увеличивает возможные риски, загрязнения при изъятии или обыске компьютерной системы, а также проблемы с установлением их подлинности.

Конфиденциальность – еще одна правовая проблема, связанная с цифровыми доказательствами. Сбор цифровых доказательств часто связан с доступом к личной или конфиденциальной информации, что вызывает серьезные опасения по поводу неприкосновенности частной жизни. Баланс между необходимостью эффективного правоприменения и правом на неприкосновенность частной жизни – сложный вопрос, требующий тщательного рассмотрения.

Правовая база, регулирующая использование цифровых доказательств. Эта система многогранна и включает в себя законы, нормативные акты и прецедентное право, связанные со сбором, сохранением, анализом и представлением цифровых доказательств в суде. Однако, быстрый темп технологических изменений часто опережает развитие правовых норм и практики, что приводит к пробелам, которые необходимо устранить. Это включает в себя необходимость определения понятий «цифровых доказательства» и разработки новой ***парадигмы теории цифровых доказательств***.

Практические проблемы включают в себя различия в возможностях работы с цифровыми доказательствами в разных юрисдикциях и между различными субъектами системы уголовного правосудия. Это может привести к несоответствиям в обращении с цифровыми доказательствами и повлиять на справедливость и эффективность уголовного судопроизводства.

В заключение следует отметить, что использование цифровых доказательств в уголовном судопроизводстве сопряжено с целым рядом сложностей и проблем, которые необходимо решать. Это требует постоянных исследований и разработки политики, а также сотрудничества между практикующими юристами, сотрудниками правоохранительных органов, экспертами в области цифровой криминалистики и политиками. Поступая таким образом, мы сможем обеспечить эффективное и справедливое использование цифровых доказательств в процессе отправления правосудия.