“ADOLAT”
MILLIY HUQUQIY AXBOROT MARKAZI
Guvohnoma № 636478
Litsenziya C-5669732

“HUQUQ va BURCH+” —
«ПРАВО и ДОЛГ+» —
"RIGHT and DUTY+"
Journal home page:
https://adolatmarkazi.uz/magazine/electron?id=382

2026-yil
8-son
avgust
ISSN 3093-8546

Стратегия «собирания доказательств» в условиях цифровых коммуникаций (Telegram, email) для судебных споров

Рашид Шарапов,
Преподаватель
сектора Гражданского процессуального и экономического процессуального права ТГЮУ
e-mail: sharapov.rashid@gmail.com

Аннотация. Ushbu maqolada Telegram messenjeri va elektron pochta kabi raqamli kommunikatsiyalar sharoitida sud jarayonlari uchun dalillarni to‘plash strategiyasining huquqiy va amaliy jihatlari tahlil qilinadi. O‘zbekiston Respublikasining amaldagi qonunchiligida raqamli dalillardan foydalanish bilan bog‘liq muammolar, ularning maqbulligi, ishonchliligi hamda identifikatsiyasi masalalari ko‘rib chiqiladi. Shuningdek, xorijiy tajriba va xalqaro standartlar asosida raqamli dalillarni yig‘ish, saqlash va tekshirish mexanizmlarini takomillashtirish bo‘yicha takliflar ishlab chiqilgan.

Калит сўзлар. raqamli dalillar; elektron dalillar; Telegram; elektron pochta; fuqarolik protsessi; sud dalillari; raqamli kriminalistika; metama'lumotlar.

Аннотация. В статье исследуются правовые и практические аспекты стратегии собирания цифровых доказательств в условиях использования современных средств электронной коммуникации, включаяTelegramи электронную почту. Проанализированы особенности правового регулирования цифровых доказательств в Республике Узбекистан, рассмотрены проблемы их допустимости, достоверности и идентификации участников коммуникации. Особое внимание уделено зарубежному опыту, международным стандартам цифровой криминалистики и современным методам обеспечения сохранности электронных данных. На основании проведенного анализа сформулированы предложения по совершенствованию законодательства и правоприменительной практики в сфере использования цифровых доказательств.

Ключевые слова. цифровые доказательства; электронные доказательства; Telegram; электронная почта; гражданский процесс; судебные доказательства; цифровая криминалистика; метаданные.

Annotation. This article examines the legal and practical aspects of developing a strategy for collecting digital evidence in disputes involving modern electronic communications, particularly Telegram and email. It analyzes the current legal framework of the Republic of Uzbekistan governing digital evidence and identifies challenges related to its admissibility, authenticity, reliability, and participant identification. The study also reviews international legal practice and digital forensic standards, including evidence preservation and verification methods. Based on the findings, recommendations are proposed to improve legislative regulation and judicial practice concerning the collection, preservation, and assessment of digital evidence in civil proceedings.

Keywords. digital evidence; electronic evidence; Telegram; email; civil procedure; forensic evidence; digital forensics; metadata.

Введение

В условиях всеобщей цифровизации общественных отношений происходит интенсивная трансформация форм взаимодействия субъектов гражданского оборота. Значительная часть юридически значимых действий и договоренностей осуществляется посредством электронных средств связи, включая электронную почту и мессенджеры, такие как Telegram. В этой связи следует говорить о необходимости изменения традиционных подходов к доказыванию и разработке новой стратегии сбора доказательств в судебном процессе.

Обоснованием актуальности темы исследования является то, что цифровые коммуникации в настоящее время становятся одним из основных источников получения доказательственной информации в ходе рассмотрения гражданских и хозяйственных споров.

Однако современное законодательство Республики Узбекистан не учитывает все особенности электронных доказательств, что приводит к неоднозначной их правовой оценке и создает серьезные трудности в правоприменительной практике. В связи с этим целью данного исследования является всесторонний анализ стратегии сбора доказательств в цифровых коммуникациях с выявлением технических обстоятельств, проблем законодательного характера и иных проблем с практическими способами их устранения.

Основная часть

В самом начале следует отметить, что доказательства в любом деле играют чрезвычайно важную роль, и в гражданском процессе доказательствами считаются “все фактические данные, на основании которых суд в установленном законом порядке устанавливает наличие или отсутствие обстоятельств, обосновывающих требования и возражения сторон, а также иных обстоятельств, имеющих

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

значение для правильного разрешения дела”.

С развитием цифровых технологий в этом контексте были введены понятия электронных доказательств и цифровых доказательств. В этом отношении цифровые доказательства обладают рядом свойств, которые отличают их от традиционных письменных доказательств, в том числе нематериальностью, зависящей от технических средств хранения и передачи информации, и уязвимостью перед уничтожением или изменением.

С письменными доказательствами следует обращаться к статье 84 ГПК, которая рассматривает письменные доказательства как любые документы и материалы в форме цифровой или графической записи, включая те, которые были получены посредством факсимильной, электронной или иной связи, либо иным способом, которым можно установить подлинность документа, содержащие сведения о фактах, имеющих значение для дела.

В сегодняшних условиях переписка через мессенджеры и электронную почту зачастую выступает в роли письменного подтверждения сделок между сторонами, в том числе согласования условий договора, признания долга и исполнения обязательств.

Нормативно-правовое регулирование цифровых доказательств

В Узбекистане доказательства регулируются положениями Гражданского процессуального кодекса, а также специальным законодательством, регулирующим электронный документооборот и использование электронной цифровой подписи.

Особое значение для судебной практики имело Постановление Пленума Верховного суда № 35 от 19 декабря 2020 года, в котором, в частности, разъяснено, что доказательствами могут являться сведения, полученные в электронной форме, при условии, что они являются относимыми, допустимыми и достоверными. Таким образом, в данном разъяснении содержится фактическое признание возможности использования цифровых коммуникаций, в том числе переписки в Telegram и по электронной почте, в качестве доказательств.

Обзор действующего законодательства и нормативно-правовых актов, в том числе постановления Кабинета Министров Республики Узбекистан № 722, показывает, что подзаконное регулирование в части цифровых доказательств еще не сложилось. Отсюда можно говорить о наличии пробелов в законодательном регулировании данного вопроса.

С точки зрения зарубежного опыта, в США правила сохранения электронных доказательств в гражданском судопроизводстве прописаны в Правилах 34 и 37 Федеральных правил гражданского судопроизводства (Federal Rules of Civil

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

Procedure). Юридический термин электронно хранимая информация (electronically stored information, ESI) был введен уже в 2006 году. Стороны обязаны предпринимать меры для сохранения оригиналов электронных данных с момента возникновения оснований полагать, что начнется судебное разбирательство (litigation hold).

Особенности Telegram и электронной почты как источников доказательств

Использование различных цифровых каналов связи в качестве доказательств обусловливает необходимость учета их технических и функциональных особенностей.

Мессенджер Telegram характеризуется высокой степенью защиты данных, возможностью удаления сообщений, а также отсутствием обязательной идентификации пользователя. Указанные особенности существенно усложняют процесс установления авторства сообщений и подтверждения их достоверности.

Однако следует отметить тот факт, что Telegram Web (версия мессенджера Telegram для браузеров) сохраняет доказательственно значимые артефакты, такие как история переписки, медиа файлы и метаданные, в кэше

браузера даже после удаления сообщений пользователем. Это одновременно подтверждает уязвимость цифровых данных и открывает возможности для их последующего восстановления.

В отличие от этого, электронная почта обладает рядом преимуществ с точки зрения доказательственной силы. Электронные письма имеют реквизиты, заголовок, идентификатор отправителя, позволяющие установить откуда и каким образом была передана информация.

В связи с этим в судебной практике электронная почта, как правило, воспринимается как более надежный источник доказательственной информации по сравнению с перепиской в мессенджерах.

С технической точки зрения, ценность электронного письма во многом определяется содержащимися в нём метаданными, которые включают IP-адреса серверов-ретрансляторов, временные метки, уникальный идентификатор сообщения (Message-ID), а также сведения об используемом программном обеспечении отправителя. Более того, заголовок электронного письма является ключевым при выявлении источника передачи сообщения и факта подмены, о чем гласит Руководство Национального института стандартов и технологий США NIST SP 800-45 (“Guidelines on Electronic Mail Security”).

Стратегия сбора цифровых доказательств

В условиях цифровой среды особое значение приобретает выработка комплексной стратегии собирания доказательств, направленной на обеспечение их допустимости и

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

достоверности.

В международной криминалистической практике применяется методология Национального института стандартов и технологий (NIST), включающая последовательные этапы сбора (collection), исследования (examination), анализа (analysis) и составления отчёта (reporting) о цифровых доказательствах. Применительно к мессенджеру Telegram данная методология позволяет извлекать и верифицировать доказательственную информацию, включая содержание переписки, дату и время отправки сообщений, а также идентификационные данные участников коммуникации4. Данный подход свидетельствует о необходимости внедрения подобного рода методов и в правоприменительной практике Республики Узбекистан.

Ключевыми элементами такой стратегии являются:

во-первых, фиксация доказательств. Данный этап включает нотариальное удостоверение переписки, составление протоколов осмотра электронных ресурсов, а также сохранение оригинальных цифровых данных. Рассматривая опыт России можно сделать вывод об актуальности данной практики, так как по данным Федеральной нотариальной палаты в 2025 году российские нотариусы зафиксировали почти 30 тысяч интернет-документов (скриншоты чатов, веб-страниц). Такой рост по сравнению с показателями пяти лет назад (на 24%) подчеркивает важность профессионального сбора доказательств перед началом судебных разбирательств;

во-вторых, обеспечение неизменности доказательств. Это достигается путем архивирования информации, создания резервных копий и фиксации временных параметров, также др. методами. Например, Национальный институт стандартов и технологий США утверждает, что эксперты – криминалисты должны использовать средства блокировки записи во время сбора данных, чтобы предотвратить любые изменения исходных доказательств. Это означает создание криминалистических образов, которые фиксируют точную, неизменённую копию цифровых носителей;

в-третьих, установление авторства сообщений, которое на практике подтверждается нотариально зафиксированной перепиской, данными о номере/аккаунте и подтверждением последующих действий сторон;

в-четвертых, систематизация доказательств, предполагающая их логическое и хронологическое упорядочивание, а также сопоставление с иными доказательствами по делу. Одним из методов систематизации цифровых доказательств является тайм-лайнинг (time-lining), представляющий собой метод сортировки событий по временным меткам.

Проблемы законодательства и правоприменительной практики

Проблема допустимости цифровых доказательств

С развитием информационных технологий цифровые доказательства становятся сложно идентифицировать, вследствие чего в судебной практике наблюдается много случаев отклонения доказательств на основании их недопустимости или недостоверности.

Согласно позиции Пленума Верховного суда, сведения, происхождение которых невозможно установить, не могут признаваться доказательствами2. Это существенно ограничивает использование скриншотов и иных форм фиксации переписки без дополнительного подтверждения. В зарубежных процессуальных законодательствах соответствие цифровых доказательств обеспечивается путем соотношения их пяти критериям, которые включают в себя относимость (доказательство должно иметь непосредственное отношение к предмету спора), аутентичность (доказательство не должно быть изменено или фальсифицировано), полнота (доказательство должно давать полную и достоверную картину фактических обстоятельств), достоверность (доказательство должно быть надёжным) и соблюдение надлежащего порядка хранения (chain of custody). Однако на практике цифровые файлы могут быть изменены, метаданные отредактированы, а временные метки – подделаны, что делает проверку происхождения сведений проблематичной.

Наиболее ярким примером является законодательство США, где доказательственное право регулируется специальным актом, а именно Федеральными правилами о доказательствах США (Federal Rules of Evidence). Правило 901(b)(9) данного акта предусматривает, что доказательства, связанные с результатами процесса или автоматизированной системы, могут быть проверены посредством описания данной системы и демонстрации её надлежащего функционирования.

Проблема достоверности

Цифровые доказательства подвержены риску фальсификации по причине того, что у пользователя есть возможность редактирования сообщений, создания фиктивных аккаунтов и использования сторонних технических средств, что несомненно ставит под сомнение их достоверность. Условное применение так называемых Deepfake-технологий, позволяющих подделать условные черты лица человека, и иных алгоритмов искусственного интеллекта затрудняет определение правдивости контента.

Проблема обеспечения целостности цифровых данных (data integrity) признана одной из ключевых и в технической науке, так как исследования фиксируют, что сообщения в Telegram могут быть изменены или полностью удалены до начала расследования. Это делает заблаговременную профессиональную фиксацию переписки критически важным условием её последующей допустимости в качестве доказательства. Отсутствие четких критериев проверки

подлинности цифровых данных усугубляет данную проблему.

Отдельную угрозу для достоверности доказательств представляет применение генеративного искусственного интеллекта для синтеза текстовых сообщений, имитирующих стиль конкретного лица. По результатам исследования, опубликованное в IEEE Journal of Selected Topics in Signal Processing, выяснилось, что точность систем обнаружения дипфейков и синтетического контента значительно ухудшается при небольшом редактировании файла (сжатии, обрезке или перекодировании). Данное факт подтверждает необходимость проведения криминалистических расследований с оригинальными файлами, а не их дубликатами.

Проблема идентификации участников коммуникации

Особую сложность представляет установление личности пользователя в мессенджерах ввиду того факта, что в них отсутствует обязательная верификация личности, как, например в Telegram, что затрудняет определение стороны правоотношений. Более того, отсутствуют так называемые метаданные, в которых фиксируется информация о том, когда и кем файл был изменен и с помощью какой программы он был создан или модифицирован, что является важным для следствия при определении достоверности цифровых доказательств.

В международной практике для опознания пользователей используется анализ IP-адресов, а также идентификация IMEI-номеров мобильных устройств, порядок сбора и идентификации которых предусмотрен в Руководстве NIST SP 800-101 Rev.1 по криминалистическому исследованию мобильных устройств, согласно которому идентификаторы устройства, такие как вышеназванный IMEI, MAC-адрес, а также данные SIM-карты являются основными артефактами при привязке цифровых коммуникаций конкретному лицу. Однако для осуществления такого вида идентификации потребуется внести поправки в процессуальное законодательство, так как потребуется особая экспертиза.

Практические проблемы использования цифровых доказательств

К числу наиболее распространенных практических проблем относятся:

1. Удаление переписки. Большинство современных мессенджеров, таких как WhatsApp, Telegram и др. поддерживают так называемые “исчезающие сообщения”, которые удаляются после истечения определенного времени, которое задается пользователем. Подобного рода функции представляют серьёзную угрозу для сохранности доказательств, а известные способы сохранения таких сообщений (пересылка, цитирование, скриншоты) не являются криминалистически состоятельными и нарушают стандарты надлежащего обращения с доказательствами;

2. Сквозное шифрование. Во многих мессенджерах наподобие Signal, Telegram, WhatsApp применяется технология сквозного шифрования (end-to-end encryption), что затрудняет проведение криминалистической экспертизы. Такие сложности с извлечением доказательств могут заставить следственные органы использовать иные методы сбора данных, такие как получение ордера, обязывающего компании предоставить данные. Различия в региональных нормах регулирования данных и законах о конфиденциальности также создают дополнительные препятствия.

Указанные обстоятельства могут повлечь признание цифровых доказательств недопустимыми.

Предложения по совершенствованию правового регулирования

В целях повышения эффективности использования цифровых доказательств представляется целесообразным:

1. Определить минимальные реквизиты для цифровых доказательств. Несмотря на дополнение статей процессуального законодательства касаемо электронных данных, цифровых доказательств и порядка их хранения, требования к их оформлению пока не регламентированы. Рекомендуется внедрить базовые реквизиты, такие как источник, дата получения, способ извлечения, носитель, лицо, производившее фиксацию, и сведения о целостности.

2. Внедрить современные технологические решения, включая цифровые подписи и иные средства подтверждения подлинности информации. Необходимо законодательно закрепить юридическое понятие метаданных, а также обязать суды проверять цифровые доказательства на их соответствие, например, проверять идентификатор аккаунта, номер устройства, время создания, хэш и признаки редактирования. Для фотографий обязательно указание EXIF метаданных об авторстве, времени, месте съемки, а также об устройстве съемки.

2. Внедрить в процессуальную практику обязательное

использование криптографических хэш-функций (алгоритм, отображающий данные произвольной длины в битовую строку фиксированной длины, именуемой хэш-значением), таких как SHA-256 при изъятии и фиксации цифровых улик, чтобы гарантировать их неизменность с момента сбора до судебного заседания. Данный алгоритм шифрования определяет входные данные и преобразует их в шифр, состоящий из 64 символов. Хэш-функция детерминирована (предопределена), то есть одни и те же входные данные будут давать один и тот же результат, что помогает убедиться в том, что копия и оригинал цифрового доказательства соответствуют друг другу.

Заключение

Таким образом, цифровизация общественных отношений привела к повышению роли электронных доказательств в судебной практике. Однако, как выяснилось, действующее

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

законодательство Республики Узбекистан не в полной мере адаптировано к особенностям цифровой среды, в частности не предусмотрены требования к маркировке цифровых доказательств и не регламентирован процесс шифрования (хэширование) оригиналов и копий доказательств для обеспечения неизменности.

Эффективная стратегия собирания доказательств должна носить комплексный характер и предусматривать меры по систематизации, сохранению и подтверждению подлинности информации. Особое значение приобретает превентивный подход, при котором доказательства формируются еще до возникновения спора.

Дальнейшее развитие правового регулирования в данной сфере должно быть направлено на устранение существующих пробелов и создание соответствующих технических мер для идентификации и шифрования цифровых доказательств.

Список использованной литературы:

1. Гражданский процессуальный кодекс Республики Узбекистан.
2. Закон Республики Узбекистан “Об электронном документообороте”.
3. Закон Республики Узбекистан “Об электронной цифровой подписи”.
4. Постановление Пленума Верховного суда Республики Узбекистан №35 от 19.12.2020.
5. Постановление Кабинета Министров Республики Узбекистан №722 от 29.12.2023.
6. Kuner, C. (2020). Digital Evidence and Privacy. Oxford University Press.
7. Prasetio, M., & Riadi, I. (2022). Investigation Telegram based-on Web using National Institute of Standards and Technology Method. International Journal of Computer Applications, 183(50), 1–8. https://doi.org/10.5120/IJCA2022921092