International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-14| Issue-4| 2026 Published: |22-04-2026|

ЦИФРОВЫЕ СЛЕДСТВЕННЫЕ ДЕЙСТВИЯ: ПРАВОВЫЕ ОСНОВАНИЯ И ПРОЦЕССУАЛЬНЫЙ ПОРЯДОК В УГОЛОВНОМ ПРОЦЕССЕ РЕСПУБЛИКИ УЗБЕКИСТАН

https://doi.org/10.5281/zenodo.20003177

Эшкуватова Диёра Узок кизи
Магистрант Ташкентского государственного юридического университета

Аннотация

Статья посвящена анализу цифровых следственных действий в уголовном процессе Республики Узбекистан в контексте недавних законодательных реформ, закрепивших понятия электронных данных и цифровых доказательств. Рассматриваются общие и специальные правовые основания работы с цифровой информацией, включая нормы Уголовно-процессуального кодекса, законы о цифровых доказательствах и об электронной цифровой подписи, а также акты судебного толкования. Особое внимание уделено процессуальному порядку представления, осмотра, выемки, обыска, прослушивания переговоров, снятия информации с телекоммуникационных устройств, ареста корреспонденции и хранения цифровых доказательств. Показана ключевая роль специалиста и следственного судьи в обеспечении допустимости электронных данных и судебного контроля за вмешательством в цифровую сферу частной жизни. На основе анализа законодательства и научных исследований выделены основные проблемы правоприменения и предложены направления дальнейшего совершенствования регулирования цифровых следственных действий.

Ключевые слова

цифровые следственные действия; электронные данные; цифровые доказательства; уголовный процесс; УПК Республики Узбекистан; судебный контроль; специалист; цифровая криминалистика.

RAQAMLI TERGOV HARAKATLARI: O‘ZBEKISTON RESPUBLIKASI JINOYAT PROTSESSIDA HUQUQIY ASOSLAR VA PROTSESSUAL TARTIB

Eshquvatova Diyora Uzoq qizi
Toshkent davlat yuridik universiteti magistranti

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-14| Issue-4| 2026 Published: |22-04-2026|

Annotatsiya. Maqolada O‘zbekiston Respublikasi jinoyat-prosessual qonunida raqamli izlanish harakatlari tushunchasining shakllanishi va raqamli dalillar bilan ishlashga oid so‘nggi islohotlar tahlil qilinadi. Elektron ma'lumotlar va raqamli dalillar tushunchalari, jinoyat-prosessual kodeks normalari, raqamli dalillar to‘g‘risidagi qonun, elektron raqamli imzo to‘g‘risidagi qonun hamda sudiy talqinining asosiy qoidalari ko‘rib chiqiladi. Elektron ma'lumotlarni ixtiyoriy taqdim etish, ularni ko‘zdan kechirish, olib qo‘yish, tintuv o‘tkazish, telefon va boshqa telekommunikasiya vositalari orqali uzatilayotgan axborotni eshitish va yozish, xat-xabarlarni ushlab qolish hamda raqamli dalillarni saqlash tartibiga alohida e'tibor qaratilgan. Elektron ma'lumotlarning yo‘l qo‘yiluvchanligini ta'minlash va shaxsning raqamli shaxsiy hayotiga aralashuv ustidan sudiy nazoratini amalga oshirishda mutaxassis va tergov sudyasining o‘rni ochib beriladi. Qonunchilik va ilmiy tadqiqotlar tahlili asosida qo‘llash amaliyotidagi asosiy muammolar aniqlanadi va raqamli izlanish harakatlarini tartibga solishni takomillashtirish yo‘nalishlari taklif etiladi.

Kalit so‘zlar

raqamli izlanish harakatlari; elektron ma'lumotlar; raqamli dalillar; jinoyat prosessi; O‘zbekiston Respublikasi Jinoyat-prosessual kodeksi; sudiy nazorat; mutaxassis; raqamli kriminalistika.

DIGITAL INVESTIGATIVE ACTIONS: LEGAL GROUNDS AND PROCEDURAL ORDER IN THE CRIMINAL PROCEDURE OF THE REPUBLIC OF UZBEKISTAN

Eshkuvatova Diyora Uzok kizi
Master’s student of Tashkent State University of Law

Abstract

The article examines digital investigative actions in the criminal procedure of the Republic of Uzbekistan in the context of recent legislative reforms that have introduced the concepts of electronic data and digital evidence. It analyses both general and special legal grounds for working with digital information, including the norms of the Criminal Procedure Code, the Law on Digital Evidence, the Law on Electronic Digital Signature, and judicial interpretative acts. Particular attention is paid to the procedural rules governing the submission, inspection, seizure, search, interception of communications, collection of data from telecommunication

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-14| Issue-4| 2026 Published: |22-04-2026|

devices, interception of correspondence, and storage of digital evidence. The crucial role of technical specialists and the investigating judge in ensuring the admissibility of electronic data and in maintaining judicial control over interferences with the digital sphere of private life is highlighted. Based on an assessment of legislation and scholarly works, the article identifies key enforcement problems and proposes directions for further improvement of the regulation of digital investigative actions.

Keywords

digital investigative actions; electronic data; digital evidence; criminal procedure; Criminal Procedure Code of Uzbekistan; judicial control; specialist; digital forensics.

ВВЕДЕНИЕ

Цифровизация общественных отношений закономерно изменила и сферу уголовного судопроизводства. Преступления все чаще совершаются с использованием информационно-коммуникационных технологий, а сведения о юридически значимых обстоятельствах фиксируются не только в традиционных предметах и документах, но и в электронных данных: файлах, переписке, логах, записях камер наблюдения, метаданных, сведениях из телекоммуникационных сетей и Интернета[96].

Для уголовного процесса Республики Узбекистан данная трансформация имела принципиальное значение, поскольку долгое время электронные сведения использовались в практике фрагментарно, через традиционные категории вещественных и письменных доказательств. Закон Республики Узбекистан от 21 ноября 2024 года № ЗРУ-1003 институционализировал цифровые доказательства, закрепил понятие электронных данных, установил порядок их представления, осмотра, копирования, хранения и исследования, а также ввел специальные гарантии допустимости таких доказательств[97].

В этих условиях особую актуальность приобретает исследование цифровых следственных действий как комплекса процессуальных действий, направленных на обнаружение, собирание, фиксацию, изъятие, осмотр, проверку и оценку электронных данных, имеющих значение для уголовного дела. Хотя сам термин «цифровые следственные действия» в Уголовно-

[96] Уголовно-процессуальный кодекс Республики Узбекистан от 22 сентября 1994 г. № 2013-XII (введён в действие с 1 апреля 1995 г., с изм. и доп.). Национальная база данных законодательства Республики Узбекистан. https://lex.uz/docs/111463#186126

[97] Республика Узбекистан. (б. д.). Закон Республики Узбекистан о внесении изменений и дополнений в некоторые законодательные акты Республики Узбекистан, направленных на совершенствование системы работы с цифровыми доказательствами. LEX.UZ. https://lex.uz/docs/7228823

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-14| Issue-4| 2026 Published: |22-04-2026|

процессуальном кодексе Республики Узбекистан не используется в качестве самостоятельной главы, его содержание выводится из совокупности норм о доказательствах, осмотре, выемке, обыске, прослушивании переговоров, снятии информации с телекоммуникационных устройств, представлении электронных данных и судебном контроле за вмешательством в частную жизнь.

Настоящая статья направлена на комплексный анализ правовых оснований и процессуального порядка цифровых следственных действий в уголовном процессе Республики Узбекистан с учетом новейших законодательных изменений и научных подходов, сформулированных современными исследователями цифровой криминалистики.

Понятие и признаки цифровых следственных действий

Под цифровыми следственными действиями в широком смысле следует понимать урегулированные уголовно-процессуальным законом действия дознавателя, следователя, прокурора и суда, направленные на получение, закрепление и исследование электронных данных и цифровых доказательств с использованием специальных правовых и технических средств. Такая интерпретация основана на том, что действующий УПК Узбекистана прямо признает электронные данные самостоятельным объектом представления, осмотра, изъятия, хранения и приобщения к делу, а цифровые доказательства — самостоятельным видом доказательственной информации[98].

Цифровые следственные действия обладают рядом признаков. Во-первых, их предметом являются электронные данные, создаваемые, обрабатываемые и хранимые с использованием электронных устройств, информационных систем и информационных технологий. Во-вторых, для их надлежащего проведения нередко требуется участие специалиста, поскольку извлечение и осмотр цифровой информации связаны с обеспечением целостности, идентичности и воспроизводимости данных. В-третьих, такие действия существенно затрагивают конституционно значимые права личности, включая право на частную жизнь, тайну переписки и переговоров, что требует повышенного уровня процессуальных гарантий и судебного контроля.

В научной литературе подчеркивается, что цифровые доказательства отличаются высокой изменяемостью, зависимостью от носителя и программной среды, наличием метаданных, а также необходимостью

[98] См. там же

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-14| Issue-4| 2026 Published: |22-04-2026|

поддержания непрерывной цепочки хранения и фиксации доказательственного объекта. Исследователи цифровой криминалистики отмечают, что без специальных процедур верификации, копирования и документирования происхождения данных возрастает риск их утраты, искажения либо оспаривания в суде[99].

Следовательно, цифровые следственные действия представляют собой не просто «техническую разновидность» традиционных следственных действий, а процессуально и криминалистически особую сферу деятельности, в которой классические правила доказывания должны сочетаться с требованиями цифровой криминалистики[100].

Нормативные основания цифровых следственных действий

Правовую основу цифровых следственных действий в Республике Узбекистан образуют, прежде всего, Уголовно-процессуальный кодекс Республики Узбекистан, Закон Республики Узбекистан от 21 ноября 2024 года № ЗРУ-1003, Закон Республики Узбекистан «Об электронной цифровой подписи», а также акты судебного толкования и специальные положения о судебной экспертизе.

Общие процессуальные основания вытекают из статей 1, 11, 18, 22, 26 и 27 УПК Республики Узбекистан. Они закрепляют обязательность производства по уголовным делам исключительно в порядке, установленном законом; требование законности; охрану прав и свобод граждан; обязанность устанавливать истину только на основе сведений, обнаруженных, проверенных и оцененных в предусмотренном Кодексом порядке; принцип непосредственного исследования доказательств; а также право участников на обжалование процессуальных действий и решений.

Особое значение имеет статья 18 УПК, согласно которой личная жизнь граждан, неприкосновенность жилища, тайна переписки, телеграфных сообщений и телефонных переговоров охраняются законом, а обыск, выемка, осмотр жилища, арест корреспонденции, прослушивание переговоров и снятие передаваемой по телекоммуникационным устройствам информации допускаются только в случаях и порядке, предусмотренных Кодексом. Данная норма служит базовой гарантией законности цифровых следственных

[99] Мелсова, К. Б. (2025). Цифровые доказательства в уголовном процессе Республики Узбекистан: правовые неясности и вызовы становления цифровой криминалистики. Global Science Review, 10(1), 128–138. https://global-science-review.com/ojs/index.php/gsr/article/view/2906

[100] Научно-исследовательский институт цифровой криминалистики. (б. д.). [Название страницы]. ProAcademy. https://proacademy.uz/ru/branches/view?alias=nauchno-issledovatelskij-institut-tsifrovoj-kriminalistik

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-14| Issue-4| 2026 Published: |22-04-2026|

действий, поскольку именно они наиболее часто предполагают вторжение в приватную цифровую сферу лица.

Закон № ЗРУ-1003 закрепил понятия «электронные данные» и «цифровые доказательства». Электронными данными признаются данные, создаваемые, обрабатываемые и хранимые с использованием электронных устройств и информационных систем; цифровыми доказательствами — электронные данные, содержащие сведения об обстоятельствах, имеющих значение для дела, включая электронные файлы, аудио- и видеозаписи, сведения из сети Интернет и иные электронные данные.

Существенной новеллой стало закрепление правила о том, что электронные данные, полученные при производстве следственных действий по выемке или осмотру без участия специалиста, признаются недопустимыми доказательствами. Данное положение прямо связывает допустимость цифровых доказательств с соблюдением процессуальной формы и служит важнейшей антиискажающей гарантией.

Кроме того, Закон «Об электронной цифровой подписи» устанавливает юридическую значимость электронной цифровой подписи, позволяющей идентифицировать владельца ключа и подтвердить отсутствие искажения информации в электронном документе. Для уголовного процесса это имеет значение при оценке происхождения электронных документов, их подлинности и неизменности.

Постановление Пленума Верховного суда Республики Узбекистан о некоторых вопросах применения норм доказательственного права разъясняет, что обязательным условием признания представленных предметов и электронных данных допустимыми доказательствами является вынесение постановления либо определения о приобщении их к делу после составления протокола осмотра. Следовательно, даже достоверные по содержанию цифровые сведения не приобретают процессуального статуса доказательства автоматически — необходима их формальная процессуализация[101].

Классификация цифровых следственных действий

Цифровые следственные действия можно классифицировать по нескольким основаниям. По характеру вмешательства в информационную сферу они делятся на действия по добровольному получению электронных

[101] Верховный суд Республики Узбекистан. (2018, 24 августа). Постановление Пленума № 24 «О некоторых вопросах применения норм уголовно-процессуального закона о допустимости доказательств» (с изм. от 23.06.2025). LEX.UZ. https://www.lex.uz/ru/docs/3896598

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-14| Issue-4| 2026 Published: |22-04-2026|

данных, действия по принудительному изъятию и осмотру цифровых объектов, а также действия по скрытому получению информации из телекоммуникационных каналов.

К первой группе относятся представление электронных данных по инициативе участников процесса и иных лиц, их прием, осмотр первичного носителя, копирование и последующее приобщение к делу. Ко второй группе относятся осмотр предметов, документов и электронных данных, выемка, обыск, осмотр телекоммуникационных сетей и Интернет-источников, изъятие электронных носителей, а также проверка показаний на месте, если она связана с цифровыми доказательствами. К третьей группе относятся прослушивание переговоров, снятие информации с телефонов и других телекоммуникационных устройств, арест корреспонденции и осмотр задержанных отправлений, содержащих электронные данные.

По субъекту санкционирования цифровые следственные действия подразделяются на действия, проводимые по постановлению дознавателя или следователя в пределах их компетенции, и действия, требующие судебного разрешения. К последним относятся, в частности, обыск, прослушивание переговоров, снятие передаваемой информации, арест почтово-телеграфных отправлений, а также выемка и обыск личных электронных данных, которые законодатель прямо поставил в зависимость от закона и решения суда.

По степени использования специальных знаний цифровые следственные действия делятся на действия, обязательное проведение которых связано с участием специалиста, и действия, в которых участие специалиста зависит от сложности объекта. С учетом прямого указания закона к первой категории фактически относятся выемка и осмотр электронных данных, поскольку их проведение без специалиста влечет недопустимость результатов.

Представление электронных данных и их процессуализация

Одним из наиболее важных нововведений узбекского законодательства стало специальное регулирование представления электронных данных по собственной инициативе. Статья 201(1) УПК предусматривает право граждан, руководителей и иных должностных лиц предприятий, учреждений и организаций представлять электронные данные должностному лицу, осуществляющему доследственную проверку, дознавателю, следователю, прокурору или суду.

Данный механизм имеет двойное значение. С одной стороны, он способствует состязательности и расширяет возможности защиты, потерпевшего, свидетеля и других лиц представлять цифровую информацию

без необходимости ожидать ее принудительного изъятия. С другой стороны, именно на стадии приема и первичного осмотра закладываются основы допустимости доказательства, поскольку закон требует участия специалиста и осмотра первичного электронного носителя, на котором содержатся представленные данные.

Статья 202 УПК в новой редакции требует составления протокола представления предметов, документов и электронных данных. В протоколе должны быть отражены сведения о лице, представившем данные, его ходатайство о приобщении, ход и результаты осмотра представленных объектов и факт передачи либо возврата представленного материала. Такая процессуальная форма препятствует подмене источника происхождения данных и обеспечивает последующую проверяемость их получения.

Статья 204(1) УПК специально закрепляет, что свидетель, потерпевший, подозреваемый, обвиняемый, подсудимый и иные лица вправе представлять электронные данные путем их копирования с одного электронного носителя на другой. Однако должностное лицо принимает такие данные только с участием специалиста и после осмотра первичного носителя. Это означает, что простая передача файла на флеш-накопителе без проверки первичного источника не отвечает требованиям закона о надлежащем собирании доказательств.

Отсюда вытекает важный практический вывод: процессуальная ценность электронных данных зависит не только от их содержания, но и от возможности установить исходный носитель, способ копирования, неизменность файла и соблюдение протокольной формы. В научной литературе именно эти элементы рассматриваются как ядро «цепочки сохранности» цифрового доказательства[102].

Осмотр цифровых объектов

Осмотр является одним из центральных процессуальных способов выявления и фиксации цифровых доказательств. В редакции после принятия Закона № ЗРУ-1003 статья 140 УПК прямо допускает производство осмотра с применением технических средств, в том числе в сетях телекоммуникации и во всемирной информационной сети Интернет, если это не влечет утрату или повреждение предметов, документов либо электронных данных.

[102] Мелсова, К. Б. (2025). Цифровые доказательства в уголовном процессе: становление и проблемы развития цифровой криминалистики в Республике Узбекистан. Global Science Review, 10(1), 128–138. https://global-science-review.com/ojs/index.php/gsr/article/view/2906

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-14| Issue-4| 2026 Published: |22-04-2026|

Эта формулировка показывает, что узбекский законодатель признает осмотр не только материальных носителей, но и удаленной цифровой среды. Следователь вправе фиксировать содержание веб-страниц, аккаунтов, сообщений, облачных данных или сетевой инфраструктуры, однако лишь при условии соблюдения общих требований законности, протоколирования и недопустимости повреждения данных.

Процессуальный порядок осмотра цифровых объектов должен включать: определение объекта осмотра; обеспечение доступа к нему; участие специалиста; применение технических средств фиксации; подробное отражение в протоколе свойств объекта, интерфейса, времени доступа, последовательности действий, используемых программно-технических средств, обнаруженных файлов и метаданных; при необходимости — копирование данных с подтверждением их идентичности. Хотя не все эти элементы детализированы в УПК буквально, они следуют из общих требований к полноте и объективности исследования доказательств и из специальных правил о целостности и идентичности цифрового доказательства.

Особенно важно, что закон прямо признает недопустимыми электронные данные, полученные при осмотре без участия специалиста. Следовательно, специалист в цифровом осмотре выступает не факультативным помощником, а процессуально значимой гарантией корректного обращения с технически сложным объектом.

В научных исследованиях подчеркивается, что цифровой осмотр должен минимизировать влияние исследователя на состояние объекта. Это означает необходимость отказа от действий, способных изменить временные метки, журналы событий, сетевую конфигурацию или содержимое устройства без документированной причины, поскольку подобные изменения способны поставить под сомнение аутентичность доказательства.

Выемка и обыск электронных данных

Значительный массив цифровых следственных действий связан с выемкой и обыском. После законодательных изменений статьи 161–163 УПК стали прямо регулировать изъятие предметов, документов и электронных данных, а также электронных носителей, содержащих электронные данные.

Часть пятая и последующие положения статьи 161 УПК устанавливают, что при выемке дознаватель или следователь после предъявления постановления либо определения предлагает добровольно выдать предметы, документы и электронные данные, подлежащие изъятию; при отказе выемка

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-14| Issue-4| 2026 Published: |22-04-2026|

производится принудительно. При обыске также сначала предлагается добровольная выдача, а при ее отсутствии либо неполноте производится поиск и изъятие указанных объектов, включая обнаруженные иные электронные данные, имеющие значение для дела.

Особое внимание законодатель уделил протоколированию: все изымаемые предметы, документы и электронные данные предъявляются понятым и другим присутствующим лицам, подробно описываются в протоколе, при необходимости упаковываются и опечатываются. В статье 163 дополнительно закреплено требование указывать, в каком месте и при каких обстоятельствах были обнаружены соответствующие объекты, были ли они выданы добровольно или изъяты принудительно, а также перечислять их с точным указанием индивидуальных признаков.

Принципиальной гарантией прав личности является новелла о том, что выемка и обыск личных электронных данных производятся на основании закона и решения суда. Эта норма прямо усиливает судебный контроль за вторжением в цифровую приватность лица и согласуется с общей статьей 18 УПК о защите тайны переписки, переговоров и личной жизни.

Практически это означает, что изъятие мобильного телефона, ноутбука, облачного аккаунта или иных персональных цифровых массивов должно оцениваться не только как изъятие вещи, но и как доступ к личным электронным данным. Следовательно, процессуальное решение должно учитывать объем вмешательства, связь объекта с предметом доказывания, пропорциональность меры и возможность менее инвазивного способа получения информации.

Прослушивание переговоров и снятие информации

К числу наиболее чувствительных цифровых следственных действий относятся прослушивание переговоров, ведущихся с телефонов и иных телекоммуникационных устройств, а также снятие передаваемой по ним информации. УПК Республики Узбекистан относит рассмотрение соответствующих ходатайств к полномочиям суда, а после введения института следственного судьи — к полномочиям следственного судьи в досудебном производстве.

Статьи 29 и 31(1) УПК закрепляют, что суд и следственный судья рассматривают ходатайства о прослушивании переговоров и снятии передаваемой информации. Это подтверждает, что названные действия допускаются исключительно в порядке судебного контроля и не могут

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-14| Issue-4| 2026 Published: |22-04-2026|

осуществляться по усмотрению следственного органа без внешней процессуальной санкции.

Связь данных мер с цифровыми доказательствами усилилась после того, как Закон № ЗРУ-1003 признал цифровыми доказательствами в том числе аудио- и видеозаписи, а также иные электронные данные, содержащие сведения об обстоятельствах дела. Следовательно, результаты прослушивания и снятия информации подлежат не только оперативному получению, но и последующему процессуальному осмотру, протоколированию, хранению и оценке как цифровые доказательства.

При этом судебный контроль здесь выполняет не формальную, а материальную функцию: он должен предотвращать произвольное вмешательство в тайну переговоров, обеспечивать соразмерность ограничения права и устанавливать пределы собираемой информации. В противном случае возникает риск признания доказательства недопустимым вследствие нарушения фундаментальных процессуальных гарантий.

Арест корреспонденции и осмотр почтово-телеграфных отправлений

Арест почтово-телеграфных отправлений и их осмотр представляют собой переходную форму между традиционными и цифровыми следственными действиями. УПК Узбекистана относит арест корреспонденции к действиям, проводимым только в случаях и порядке, предусмотренных Кодексом, а соответствующие ходатайства — к предмету судебного разрешения.

В обновленной редакции статьи 167 УПК установлено, что при осмотре задержанных почтово-телеграфных отправлений дознаватель или следователь с участием понятых, а при необходимости — специалиста, вправе обнаруживать сведения, предметы, документы и электронные данные, имеющие значение для дела; в таком случае производится выемка соответствующих отправлений либо снятие с них копий. Если значимые сведения отсутствуют, корреспонденция подлежит вручению адресату либо дальнейшему задержанию до установленного срока.

Эта норма важна тем, что прямо допускает обнаружение электронных данных в составе корреспонденции, то есть цифровой компонент может находиться не только в памяти устройств, но и в передаваемых отправлениях, носителях, вложениях, цифровых накопителях. Соответственно, порядок работы с такими объектами должен сочетать правила корреспондентской тайны и правила обращения с электронными данными.

Проверка показаний на месте и цифровая среда

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-14| Issue-4| 2026 Published: |22-04-2026|

Интересной новеллой стало дополнение статьи 132 УПК положением о том, что при проверке показаний, связанных с цифровыми доказательствами, на месте события могут использоваться информационные системы для дистанционной проверки достоверности показаний. Кроме того, сама проверка показаний на месте теперь прямо ориентирована на обнаружение не только предметов и документов, но и электронных данных.

Законодатель фактически признал, что место события в современных уголовных делах может иметь смешанный — физико-цифровой — характер. Например, проверка может касаться местонахождения камеры видеонаблюдения, маршрута передачи файлов, точки доступа к сети, местонахождения устройства в момент создания записи или доступа к определенному аккаунту. Использование информационных систем для дистанционной верификации позволяет соотнести показания лица с данными геолокации, маршрутами, логами доступа или другими цифровыми следами.

Такой подход расширяет традиционную криминалистическую модель проверки показаний на месте. Вместо исключительно пространственной реконструкции события формируется комбинированная проверка, где физическая обстановка сопоставляется с электронными данными, что особенно важно при расследовании киберпреступлений, онлайн-мошенничества и преступлений, совершенных с использованием мобильных приложений и платформ.

Копирование, целостность и допустимость цифрового доказательства

Одной из центральных проблем цифрового доказывания является соотношение подлинника и копии. Статья 204(2) УПК закрепляет, что копирование цифрового доказательства допускается при условии сохранения его целостности и идентичности, а допустимость копии обеспечивается наличием подлинника цифрового доказательства, с которого была произведена данная копия.

Данная конструкция имеет принципиальное значение для практики, поскольку в цифровой среде работа с оригиналом зачастую невозможна или нежелательна: его изъятие может нарушить деятельность организации, а непосредственное исследование — изменить свойства данных. Поэтому процессуальная ценность копии зависит от доказуемой связи с исходным объектом и от подтверждения того, что копия не была изменена при переносе.

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-14| Issue-4| 2026 Published: |22-04-2026|

Закон также устанавливает, что лица вправе представлять копии цифровых доказательств, распечатанные на бумаге, но бумажная форма цифрового доказательства не может считаться письменным доказательством. Это устраняет распространенную ошибку, при которой скриншоты, распечатки переписки или веб-страниц ошибочно приравниваются к обычным документам; в действительности они остаются формой представления цифрового доказательства и должны оцениваться с учетом его электронного происхождения.

С криминалистической точки зрения сохранение целостности предполагает документирование способа извлечения данных, времени копирования, идентификаторов носителя, технических параметров файла и, при необходимости, контрольных значений. Хотя УПК не перечисляет все такие технические реквизиты, научные работы по цифровой криминалистике последовательно обосновывают необходимость их применения для обеспечения проверяемости доказательства.

Хранение цифровых доказательств

Статья 208 УПК в новой редакции закрепляет правила хранения и пересылки вещественных, письменных и цифровых доказательств. При хранении и направлении на экспертизу должны приниматься меры, предупреждающие утрату, повреждение, порчу, взаимоприкосновение или смешение доказательств; при передаче дела все такие доказательства перечисляются в сопроводительном письме или описи, а при получении осматриваются с составлением протокола.

Для цифровых доказательств указанная норма имеет особую практическую значимость. В отличие от традиционных материальных объектов, электронные данные могут быть повреждены не только физически, но и логически: путем удаления, перезаписи, изменения структуры каталогов, обновления системного времени, автоматической синхронизации с облаком, дистанционного доступа или вредоносного воздействия. Поэтому требование предотвращать утрату и смешение цифровых доказательств должно толковаться расширительно — как обязанность обеспечивать безопасную среду хранения и контроль доступа.

Закон прямо предусматривает, что копия цифрового доказательства хранится вместе с материалами дела. Это важно для обеспечения возможности повторной проверки доказательства судом, сторонами и экспертами, а также для защиты от утраты исходного носителя.

Судебный контроль и роль следственного судьи

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-14| Issue-4| 2026 Published: |22-04-2026|

Развитие цифровых следственных действий обусловило усиление судебного контроля в досудебном производстве. В УПК Республики Узбекистан введена статья 31(1), закрепившая полномочия следственного судьи, который единолично осуществляет судебный контроль за соблюдением прав, свобод и законных интересов лица на стадии досудебного производства.

К полномочиям следственного судьи отнесено рассмотрение ходатайств об обыске, аресте почтово-телеграфных отправлений, прослушивании переговоров, снятии информации с телекоммуникационных устройств и иных мерах, сопряженных с существенным ограничением прав личности. Для цифровой сферы это особенно важно, поскольку доступ к устройствам, аккаунтам и коммуникациям позволяет получить большой массив сведений о частной жизни человека, далеко выходящий за пределы конкретного эпизода преступления.

Появление следственного судьи усиливает состязательные начала и институциональные гарантии допустимости цифровых доказательств. Судебный контроль на ранней стадии позволяет оценивать необходимость, соразмерность и процессуальную форму предполагаемого вмешательства еще до получения данных, что снижает риск произвольного сбора цифровой информации и последующего оспаривания результатов.

Специалист и эксперт в системе цифровых следственных действий

Роль специалиста в цифровых следственных действиях является ключевой. Законодатель прямо связал допустимость электронных данных, полученных при осмотре и выемке, с участием специалиста, а при осмотре почтово-телеграфных отправлений также допустил его привлечение при необходимости.

Специалист обеспечивает корректное извлечение данных, использование технических средств, предупреждение повреждения носителя, идентификацию источника информации, описание способа доступа и фиксацию значимых параметров цифрового объекта. В отличие от эксперта, который проводит самостоятельное исследование и дает заключение, специалист содействует следственному действию в момент его проведения и помогает соблюсти технически правильную процессуальную форму[103].

Значение судебной экспертизы также возрастает. Закон Республики Узбекистан «О судебной экспертизе» после изменений относит к объектам

[103] Научно-исследовательский институт цифровой криминалистики. (б. д.). [Название страницы]. ProAcademy. https://proacademy.uz/ru/branches/view?alias=nauchno-issledovatelskij-institut-tsifrovoj-kriminalistik

исследования вещественные, письменные и цифровые доказательства, информационные системы, электронные носители, содержащие электронные данные, и электронные данные, хранящиеся в источниках сети Интернет. Это создает нормативную основу для компьютерно-технических, телекоммуникационных и иных цифровых экспертиз.

Дополнительным подтверждением институционального развития данной сферы является создание в 2024 году Научно-исследовательского института цифровой криминалистики в структуре Академии правоохранительных органов, задачами которого названы исследования в области цифровых доказательств, методов расследования киберпреступлений, сбора данных из Интернета и применения специального программного обеспечения.

Проблемы правоприменения

Несмотря на серьезное обновление законодательства, правоприменительная практика цифровых следственных действий в Узбекистане сталкивается с рядом проблем. Во-первых, не все процессуальные операции с электронными данными детально регламентированы на уровне УПК: закон устанавливает базовые требования, но многие технические аспекты — например, алгоритм форензического копирования, использование хэш-значений, порядок работы с облачными сервисами и удаленными серверами — остаются в сфере методических рекомендаций и экспертной практики.

Во-вторых, сохраняется риск смешения цифровых доказательств с письменными документами, особенно когда в дело представляются распечатки переписки, скриншоты, фотографии экрана или экспортированные текстовые файлы. Закон уже разграничил эти категории, указав, что бумажная форма цифрового доказательства не превращает его в письменное доказательство, однако данная новелла требует единообразного понимания со стороны следователей, прокуроров, адвокатов и судов.

В-третьих, проблема кадрового и технического обеспечения остается одной из центральных. Научные исследования отмечают, что полноценная инфраструктура цифровой криминалистики в национальной системе уголовного судопроизводства находится в стадии становления, а эффективная работа с цифровыми следами требует специализированной подготовки, оборудования и унифицированных процедур.

В-четвертых, в условиях расширения цифрового наблюдения возрастает опасность несоразмерного вмешательства в частную жизнь. Изъятие

смартфона или доступа к аккаунту способно раскрыть не только сведения по делу, но и значительный объем личной информации, не относящейся к предмету доказывания. Поэтому принцип пропорциональности должен стать одним из основных ориентиров правоприменителя наряду с формальной законностью.

Научные подходы и направления совершенствования

Современная доктрина исходит из того, что цифровое доказательство требует самостоятельного теоретического осмысления, а цифровая криминалистика постепенно оформляется как особое направление уголовно-процессуальной и криминалистической науки. Исследователи подчеркивают необходимость интеграции процессуальных требований допустимости с техническими стандартами извлечения, копирования, хранения и анализа электронных данных.

Представляется, что дальнейшее совершенствование законодательства Республики Узбекистан должно развиваться по следующим направлениям:

детализация процессуального порядка форензического копирования и верификации цифровых носителей;

нормативное закрепление минимальных требований к протоколу осмотра электронных данных, включая описание программно-технических средств и параметров доступа;

разработка ведомственных стандартов сохранения цифровой цепочки хранения доказательства;

расширение судебного контроля за доступом к облачным аккаунтам, мессенджерам и иным удаленным сервисам;

усиление специализации следователей, прокуроров, адвокатов, судей, специалистов и экспертов в сфере цифровой криминалистики.

Отдельного внимания заслуживает выработка единых подходов к оценке аутентичности цифровых доказательств в суде. Судебная практика должна исходить не только из формального факта изъятия файла или устройства, но и из прослеживаемости происхождения данных, наличия первичного источника, соблюдения порядка копирования, участия специалиста и отсутствия признаков искажения информации.

ЗАКЛЮЧЕНИЕ

Цифровые следственные действия в уголовном процессе Республики Узбекистан представляют собой формирующийся, но уже достаточно отчетливо очерченный процессуальный институт. Его нормативная база складывается из общих принципов УПК, специальных норм о защите частной

жизни, судебном контроле, доказательствах и следственных действиях, а также новелл Закона № ЗРУ-1003, закрепивших понятия электронных данных и цифровых доказательств, порядок их представления, осмотра, копирования, хранения и приобщения к делу.

Ключевой особенностью современного регулирования является сочетание двух начал: с одной стороны, расширение возможностей следствия и суда по работе с цифровой информацией, включая данные Интернета, телекоммуникационных сетей и электронных носителей; с другой — усиление гарантий законности, выраженных в судебном контроле, обязательности участия специалиста и строгих требованиях к допустимости полученных электронных данных.

Именно поэтому цифровые следственные действия нельзя рассматривать лишь как технологическое приложение к традиционным институтам уголовного процесса. Они требуют самостоятельной процессуальной культуры, основанной на уважении прав человека, научно обоснованных методах цифровой криминалистики и точном соблюдении формы собирания и исследования доказательств. Только при таком подходе цифровизация уголовного судопроизводства будет служить не ослаблению, а укреплению законности и справедливости.

СНОСКИ:

Уголовно-процессуальный кодекс Республики Узбекистан от 22 сентября 1994 года № 2013-XII (в действующей редакции) // LEX.UZ. URL: https://lex.uz/docs/111463

Закон Республики Узбекистан от 21 ноября 2024 года № ЗРУ-1003 «О внесении изменений и дополнений в некоторые законодательные акты Республики Узбекистан, направленных на совершенствование системы работы с цифровыми доказательствами» // LEX.UZ. URL: https://lex.uz/docs/7228823

Закон Республики Узбекистан «Об электронной цифровой подписи» от 12 октября 2022 года № ЗРУ-793 // LEX.UZ. URL: https://www.lex.uz/acts/64424

О некоторых вопросах применения норм доказательственного права: Постановление Пленума Верховного суда Республики Узбекистан от 24 августа 2018 года № 24 // LEX.UZ. URL: https://www.lex.uz/ru/docs/3896598

Цифровые доказательства в уголовном процессе: становление и проблемы развития цифровой криминалистики в Республике Узбекистан // Global Science Review. 2025. URL: https://global-science-review.com/ojs/index.php/gsr/article/view/2906

Научно-исследовательский институт цифровой криминалистики // Academy of Law Enforcement of the Republic of Uzbekistan. URL: https://proacademy.uz/ru/branches/view?alias=nauchno-issledovatelskij-institut-tsifrovoj-kriminalistiki

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

Уголовно-процессуальный кодекс Республики Узбекистан от 22 сентября 1994 года № 2013-XII (в действующей редакции) // LEX.UZ. [Электронный ресурс]. URL: https://lex.uz/docs/111463

Закон Республики Узбекистан от 21 ноября 2024 года № ЗРУ-1003 «О внесении изменений и дополнений в некоторые законодательные акты Республики Узбекистан, направленных на совершенствование системы работы с цифровыми доказательствами» // LEX.UZ. [Электронный ресурс]. URL: https://lex.uz/docs/7228823

Закон Республики Узбекистан «Об электронной цифровой подписи» от 12 октября 2022 года № ЗРУ-793 // LEX.UZ. [Электронный ресурс]. URL: https://www.lex.uz/acts/64424

О некоторых вопросах применения норм доказательственного права: Постановление Пленума Верховного суда Республики Узбекистан от 24 августа 2018 года № 24 // LEX.UZ. [Электронный ресурс]. URL: https://www.lex.uz/ru/docs/3896598

Цифровые доказательства в уголовном процессе: становление и проблемы развития цифровой криминалистики в Республике Узбекистан // Global Science Review. 2025. [Электронный ресурс]. URL: https://global-science-review.com/ojs/index.php/gsr/article/view/2906

Научно-исследовательский институт цифровой криминалистики // Academy of Law Enforcement of the Republic of Uzbekistan. [Электронный ресурс]. URL: https://proacademy.uz/ru/branches/view?alias=nauchno-issledovatelskij-institut-tsifrovoj-kriminalistiki

В Узбекистане подписан закон о цифровых доказательствах // Gazeta.uz. 26.11.2024. [Электронный ресурс]. URL: https://www.gazeta.uz/ru/2024/11/26/digital-evidence/