12.00.09 - Уголовный процесс. Криминалистика. Оперативно-розыскное право и судебная экспертиза

Трансграничное получение цифровых доказательств в уголовном процессе: Процессуальные проблемы и пути их решения

Гулимов Шухрат Шавкатович

Старший прокурор отдела по надзору за соблюдением законодательства в органах внутренних дел прокуратуры Ташкентской области.

gulimov.w@gmail.com

+998901670009

Аннотация. Данные, необходимые для доказывания по обычному уголовному делу, всё чаще находятся на серверах иностранных поставщиков услуг, тогда как процессуальный инструментарий рассчитан на изъятие объектов, расположенных внутри страны. Проблема исследования состоит в разрыве между темпом утраты электронных данных и сроками классической взаимной правовой помощи, а также в неопределённости процессуального статуса данных, полученных по иностранной процедуре. В статье выделены четыре модели трансграничного получения данных, различающиеся адресатом требования и субъектом контроля законности; описаны шесть процессуальных проблем, среди которых конфликт темпов, риск автоматической недопустимости данных, полученных за рубежом по иной процедуре, разрыв цепи непрерывного владения через границу и неопределённость статуса добровольного предоставления данных иностранным провайдером; показано, что Закон от 21 ноября 2024 года № ЗРУ-1003, институционализировавший цифровые доказательства, не создал ни одного трансграничного инструмента. Научная новизна заключается в обосновании критерия допустимости иностранных цифровых доказательств, основанного на проверяемости, а не на тождестве процедур. Практическое значение — девять предложений по совершенствованию законодательства, увязанных с подписанием Республикой Узбекистан Конвенции ООН против киберпреступности.

Ключевые слова: цифровые доказательства; трансграничный доступ к данным; взаимная правовая помощь; ускоренное сохранение данных; поставщик услуг; допустимость доказательств; цепь непрерывного владения; юрисдикция; Будапештская конвенция; Конвенция ООН против киберпреступности.

Annotatsiya

Oddiy jinoyat ishi bo‘yicha isbotlash uchun zarur ma’lumotlar tobora ko‘proq xorijiy xizmat ko‘rsatuvchilarning serverlarida saqlanmoqda, protsessual vositalar esa mamlakat hududidagi obyektlarni olib qo‘yishga mo‘ljallangan. Tadqiqot muammosi elektron ma’lumotlarning yo‘qolish tezligi bilan an’anaviy o‘zaro huquqiy yordam muddatlari o‘rtasidagi tafovutda, shuningdek xorijiy tartibda olingan ma’lumotlarning protsessual maqomi noaniqligida ifodalanadi. Asosiy natijalar: talab qaratilgan subyekt va qonuniylikni nazorat qiluvchi subyektga ko‘ra farqlanadigan to‘rtta model ajratildi; oltita protsessual muammo tavsiflandi, jumladan tezliklar ziddiyati, xorijda boshqa tartibda olingan ma’lumotlarning avtomatik nomaqbul deb topilishi xavfi, chegara orqali dalilni saqlash zanjirining uzilishi va xorijiy provayder ma’lumotni ixtiyoriy taqdim etishining maqomi noaniqligi; 2024-yil 21-noyabrdagi O‘RQ-1003-son Qonun raqamli dalillarni institutsionallashtirgan bo‘lsa-da,

birorta transchegaraviy vosita yaratmagani ko‘rsatildi. Ilmiy yangilik xorijiy raqamli dalillarning maqbulligi mezonini tartiblarning aynanligiga emas, tekshiriluvchanlikka asoslashda ifodalanadi. Amaliy ahamiyati — O‘zbekistonning BMT Kiberjinoyatchilikka qarshi konvensiyasini imzolagani bilan bog‘langan to‘qqizta taklif.

Kalit so‘zlar: raqamli dalillar; ma’lumotlarga transchegaraviy kirish; o‘zaro huquqiy yordam; ma’lumotlarni tezkor saqlash; xizmat ko‘rsatuvchi; dalillarning maqbulligi; dalilni saqlash zanjiri; yurisdiksiya; Budapesht konvensiyasi; BMTning kiberjinoyatchilikka qarshi konvensiyasi.

Abstract

The data required to prove an ordinary criminal case increasingly reside on servers of foreign service providers, while procedural tools remain designed for the seizure of objects located within the country. The research problem lies in the gap between the speed at which electronic data are lost and the timeframes of classical mutual legal assistance, and in the uncertain procedural status of data obtained under a foreign procedure. The methodology combines formal-legal, comparative-legal, systemic-structural and logical methods. Main results: four models of cross-border acquisition are distinguished according to the addressee of the demand and the authority controlling its lawfulness; six procedural problems are described, including the conflict of tempos, the risk that data lawfully obtained abroad under a different procedure will be automatically inadmissible, the rupture of the chain of custody across borders, and the undefined status of voluntary disclosure by a foreign provider; it is shown that Law No. ZRU-1003 of 21 November 2024, which institutionalised digital evidence, created no cross-border instrument whatsoever. The novelty lies in grounding the admissibility of foreign digital evidence in verifiability rather than in identity of procedures. Practical significance: nine legislative proposals linked to Uzbekistan’s signature of the United Nations Convention against Cybercrime.

Keywords: digital evidence; cross-border access to data; mutual legal assistance; expedited preservation; service provider; admissibility; chain of custody; jurisdiction; Budapest Convention; UN Convention against Cybercrime.

Введение

Трансграничность перестала быть признаком исключительных уголовных дел. Мошенничество, совершённое в отношении жителя одного города через мессенджер, оставляет следы на серверах компании, зарегистрированной в другом государстве; переписка соучастников хранится в облачном сервисе, юрисдикция которого определяется не местом преступления, а корпоративной архитектурой. При этом уголовно-процессуальный инструментарий по-прежнему построен на территориальном принципе: выемка, обыск и осмотр рассчитаны на объекты, находящиеся в пределах государства.

Законом Республики Узбекистан от 21 ноября 2024 года № ЗРУ-1003 национальное законодательство сделало принципиальный шаг во внутреннем измерении: в Уголовно-процессуальный кодекс включены статьи 204¹ «Электронные данные» и 204² «Цифровые доказательства», цифровые доказательства внесены в часть вторую статьи 81 в качестве самостоятельного источника, а электронные данные включены в предмет осмотра, выемки, обыска и экспертизы [1; 2]. Однако ни одного механизма трансграничного получения данных этот Закон не создал: в нём нет ни института срочного сохранения данных, ни правил взаимодействия с иностранными поставщиками услуг, ни специальных норм о статусе информации, полученной за рубежом.

Внешнеполитический контекст при этом изменился. 25 октября 2025 года в Ханое открылась для подписания Конвенция Организации Объединённых Наций против киберпреступности, принятая Генеральной Ассамблеей 24 декабря 2024 года; в первые дни её подписали свыше семидесяти государств и Европейский союз, в их числе — Республика Узбекистан [10; 11; 12]. Тем самым вопрос о процедурах трансграничного получения цифровых доказательств переходит из плоскости теоретической дискуссии в плоскость подготовки национального законодательства к исполнению будущих договорных обязательств.

1. Особенности трансграничности цифровых доказательств

Классическая правовая помощь исходит из того, что искомый объект находится в известном месте на территории известного государства. Применительно к данным это допущение не работает по четырём причинам.

Первая - утрата привязки к территории. Данные могут храниться фрагментированно, дублироваться в нескольких центрах обработки и перемещаться между ними автоматически, без участия и ведома пользователя. Место физического хранения перестаёт быть устойчивым признаком и потому непригодно как единственное основание юрисдикции; именно эту проблему фиксировала группа по облачным доказательствам Совета Европы, отмечая, что органы расследования нередко не в состоянии установить, где находятся нужные данные [16].

Вторая - конфликт темпов. Электронные данные удаляются или перезаписываются в сроки, измеряемые днями и неделями, тогда как исполнение поручения о правовой помощи занимает месяцы. Инструмент, рассчитанный на передачу документов и допрос свидетелей, оказывается непригодным для объекта, который может исчезнуть до того, как поручение дойдёт до адресата.

Третья - смена адресата требования. В классической схеме государство обращается к государству. В цифровой среде фактическим держателем данных выступает частная компания, и эффективность расследования зависит от её готовности исполнить требование. Возникает трёхсторонняя конструкция «запрашивающее государство — запрашиваемое государство — поставщик услуг», в которой процессуальные гарантии распределены между разными правопорядками.

Четвёртая - коллизия обязанностей. Поставщик услуг может одновременно находиться под обязанностью раскрыть данные по требованию одного государства и под запретом их передавать по праву другого, включая законодательство о защите персональных данных. Для него это не теоретическая коллизия, а риск ответственности в обеих юрисдикциях.

Из перечисленного следует, что трансграничное получение цифровых доказательств не сводится к ускорению существующих процедур. Меняется сама конструкция: вопрос «где находятся данные» вытесняется вопросом «кто ими правомерно распоряжается и кто контролирует законность доступа».

2. Модели трансграничного получения данных

Сопоставление действующих инструментов позволяет выделить четыре модели, различающиеся адресатом требования и субъектом контроля его законности.

Первая модель — классическая межгосударственная. Требование адресовано иностранному государству, законность проверяет запрашиваемая сторона по своему праву. Для государств — участников Содружества Независимых Государств базовым инструментом

остаётся Конвенция о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам 1993 года [5], дополняемая двусторонними договорами. Модель обеспечивает наиболее полный контроль суверенитета и наиболее слабую оперативность.

Вторая модель — договорно-ускоренная. Конвенция Совета Европы о киберпреступности 2001 года ввела в межгосударственное сотрудничество институты, специально приспособленные к свойствам данных: срочное сохранение хранящихся компьютерных данных, ускоренное раскрытие сохранённых данных о трафике, взаимную помощь в доступе к хранящимся данным и круглосуточную сеть контактных пунктов, обеспечивающую немедленное реагирование [6]. Второй дополнительный протокол 2022 года пошёл дальше и допустил прямое обращение к субъектам другой стороны: запрос о сведениях о регистрации доменного имени (статья 6), прямой запрос абонентской информации у поставщика услуг на территории другой стороны (статья 7), придание силы распоряжению другой стороны об ускоренном предоставлении абонентской информации и данных о трафике (статья 8) и ускоренное раскрытие данных в чрезвычайной ситуации через контактный пункт круглосуточной сети (статья 9) [7; 14; 15].

Третья модель — прямое принуждение в рамках интеграционного объединения. Регламент (ЕС) 2023/1543, применяемый с 18 августа 2026 года, наделяет судебный орган одного государства-члена правом направить европейское распоряжение о предоставлении или о сохранении электронных доказательств непосредственно поставщику услуг, предлагающему услуги в Союзе, минуя органы государства его местонахождения; сроки исполнения исчисляются днями, а в чрезвычайных случаях — часами, тогда как сохранение данных обеспечивается на ограниченный срок с возможностью продления [8; 26]. Директива (ЕС) 2023/1544 дополняет этот механизм обязанностью поставщика назначить в Союзе адресата таких распоряжений [9]. Модель максимально оперативна, но предполагает высокий уровень взаимного доверия и общий стандарт защиты прав.

Четвёртая модель — экстерриториальная односторонняя. Законодательство США о разъяснении правомерного использования данных за рубежом (CLOUD Act, 2018) исходит из критерия контроля: провайдер, подпадающий под юрисдикцию США, обязан предоставить данные, находящиеся под его владением, охраной или контролем, независимо от места их хранения; параллельно предусмотрена возможность заключения исполнительных соглашений с иностранными государствами [13]. К этой же модели примыкает трансграничный доступ без разрешения другой стороны, допускаемый Будапештской конвенцией лишь в двух узких случаях — когда данные общедоступны либо когда получено правомерное и добровольное согласие лица, уполномоченного их раскрыть [6].

Отдельное место занимает формирующаяся универсальная модель. Конвенция ООН против киберпреступности воспроизводит на глобальном уровне логику второй модели: процессуальные полномочия по ускоренному сохранению данных и их предоставлению, механизм взаимной правовой помощи и круглосуточную сеть контактных пунктов [10]. Конвенция вступит в силу на девяностый день после сдачи на хранение сороковой ратификационной грамоты и остаётся открытой для подписания до 31 декабря 2026 года [11]. Её практическая ценность будет определяться не текстом, а тем, насколько национальные законодательства окажутся способны исполнять предусмотренные ею процедуры.

3. Процессуальные проблемы

Уголовно-процессуальный кодекс Республики Узбекистан не знает распоряжения о сохранении данных — меры, не раскрывающей содержание, но запрещающей уничтожение

информации на срок, необходимый для получения доступа в установленном порядке. Между тем часть девятая статьи 161 УПК требует судебного решения для выемки и обыска личных электронных данных [1; 2]. Возникает разрыв: пока готовится и рассматривается ходатайство, данные у поставщика услуг могут быть уничтожены в силу его обычной политики хранения. Именно поэтому сохранение выделено в самостоятельный институт и в Будапештской конвенции, и в Конвенции ООН [6; 10].

Введённая Законом № ЗРУ-1003 часть четвёртая статьи 95^1 УПК признаёт недопустимыми электронные данные, полученные при выемке или осмотре без участия специалиста [2]. Норма разумна во внутреннем измерении, но при буквальном применении к материалам, полученным по поручению о правовой помощи, порождает тупик: иностранный орган действует по своему процессуальному закону, который может не знать фигуры специалиста в том значении, в каком её понимает национальное право. Формальное сопоставление процедур ведёт к отказу от доказательства, полученного правомерно. Требуется правило о том, что действия за рубежом совершаются по праву запрашиваемого государства, а оценке подлежит не тождество процедур, а проверяемость результата.

При трансграничной передаче данных цепь «изъятие — копирование — передача — приобщение» проходит через несколько правопорядков, и ни один из них не отвечает за неё целиком. Национальный закон требует обеспечения целостности и идентичности копии (часть вторая статьи 204^2 УПК), но не определяет способа проверки [2], а иностранная сторона документирует свои действия по собственным стандартам. В результате суд получает материал, происхождение которого подтверждается сопроводительным письмом, а не проверяемыми техническими данными. В литературе именно неадаптированность процессуальных гарантий к цифровой среде рассматривается как системная угроза справедливости разбирательства [21; 22].

Статья 201^1 УПК допускает представление электронных данных по собственной инициативе граждан и должностных лиц предприятий, учреждений и организаций [2]. Норма сформулирована без территориального ограничения, что теоретически охватывает и иностранного поставщика услуг, откликнувшегося на прямой запрос. Однако закон не определяет, каким документом удостоверяется полномочие представившего лица, как проверяется относимость и подлинность переданного массива и подлежит ли такая передача судебному контролю. Практика прямого добровольного взаимодействия с провайдерами широко распространена, и именно её процессуальное оформление образует наиболее уязвимое звено доказывания.

Часть вторая статьи 140 УПК допускает осмотр с применением технических средств, в том числе в сетях телекоммуникации и во всемирной информационной сети Интернет [2]. Норма сформулирована безотносительно к тому, где физически расположен исследуемый ресурс. Тем самым внутреннее следственное действие способно де-факто затронуть данные, находящиеся под юрисдикцией другого государства. Международный стандарт ограничивает такой доступ случаями общедоступности данных или наличия правомерного согласия уполномоченного лица [6]; национальное законодательство подобного критерия не содержит, что создаёт риск как дипломатических претензий, так и оспаривания доказательства.

Данные, полученные за рубежом, затрагивают частную жизнь так же, как и полученные внутри страны, однако гарантии при этом распределены между правопорядками. Второй дополнительный протокол решает эту проблему включением специальных положений о защите передаваемых персональных данных [7]. В национальном праве требование судебного решения по части девятой статьи 161 УПК формально относится к выемке и обыску и не

распространяется прямо на получение тех же данных через каналы международного сотрудничества, что порождает неравенство гарантий в зависимости от способа получения одной и той же информации.

4. Регулирование в Республике Узбекистан: состояние и пробелы

Внутренний блок регулирования после Закона № ЗРУ-1003 можно считать сформированным: определены электронные данные и цифровые доказательства, установлен порядок их осмотра, изъятия, представления, хранения и исследования, введён судебный контроль за доступом к личным электронным данным, электронные данные включены в объекты судебной экспертизы [1; 2]. Внешний блок отсутствует полностью. В Кодексе нет норм о сохранении данных по запросу иностранного государства, о направлении и исполнении запросов, касающихся электронных данных, о статусе материалов, полученных от иностранных поставщиков услуг, о круглосуточном контактном пункте и о трансграничном доступе к общедоступным данным.

Организационные вопросы взаимодействия с компетентными органами иностранных государств решаются на уровне международных договоров и разъяснений: постановление Пленума Верховного суда Республики Узбекистан от 25 мая 2012 года № 6 определяет порядок обращения уполномоченных органов — Верховного суда, Генеральной прокуратуры, Министерства внутренних дел, Службы государственной безопасности — с запросами об оказании правовой помощи [3]. Однако этот акт создавался до появления в законодательстве категории цифровых доказательств и не учитывает ни срочности сохранения данных, ни специфики их удостоверения.

Институциональные предпосылки для развития направления созданы: постановлением Президента Республики Узбекистан от 21 июня 2024 года № ПП-229 предусмотрена организация научно-исследовательской деятельности и повышения квалификации в сфере цифровой криминалистики [4]. Подписание Конвенции ООН против киберпреступности означает, что в перспективе национальное право должно будет обеспечить исполнение предусмотренных ею процессуальных полномочий и форм сотрудничества [10; 12]. Присоединение к Будапештской конвенции, открытой для любых государств, дало бы доступ к уже действующей и практически отработанной инфраструктуре сотрудничества [17], однако выбор конкретной договорной стратегии выходит за пределы настоящего исследования; принципиально то, что оба пути требуют одних и тех же изменений внутреннего процессуального закона.

5. Научная дискуссия

В доктрине конкурируют три подхода к основанию трансграничного доступа. Первый — территориальный: юрисдикция определяется местом физического хранения данных, любой доступ к данным за рубежом без согласия соответствующего государства недопустим. Подход последовательно защищает суверенитет, но исходит из предпосылки, которая технически более не выполняется: место хранения нестабильно и часто неизвестно даже самому оператору [16].

Второй — подход контроля над данными: значение имеет не место хранения, а наличие у субъекта фактической возможности распоряжаться данными; на этом критерии построено законодательство США [13]. Подход обеспечивает оперативность, но переносит центр тяжести на одностороннее решение и потому воспринимается другими государствами как экстерриториальное вмешательство.

Третий — процедурный: допустим прямой доступ, но лишь в объёме, согласованном в договоре, при чётко описанных категориях данных и при встроенных гарантиях; по этой логике построен Второй дополнительный протокол, разделяющий абонентскую информацию, данные о трафике и содержание сообщений и устанавливающий для них разные режимы [7; 14; 15].

Авторская позиция состоит в поддержке третьего подхода с уточнением, значимым для государств, не входящих в интеграционные объединения. Для Республики Узбекистан прямое принуждение по модели Регламента (ЕС) 2023/1543 недостижимо, поскольку предполагает взаимное признание решений внутри единого правового пространства. Реалистичной является связка «сохранение — запрос — проверяемость»: национальное право должно обеспечить возможность немедленно закрепить данные, оперативно направить запрос по договорному каналу и, что важнее всего, проверить полученный результат по собственным критериям. Именно проверяемость, а не совпадение процедур, должна выступать критерием допустимости иностранных цифровых доказательств.

6. Научная новизна

1. Предложена классификация моделей трансграничного получения цифровых доказательств по двум связанным критериям — адресату требования и субъекту контроля его законности, что позволяет оценивать применимость каждой модели к конкретному государству исходя из его договорного положения, а не из технических возможностей.

2. Обоснован критерий допустимости иностранных цифровых доказательств: оценке подлежит проверяемость результата (идентифицируемость источника, документированность порядка получения, возможность технической проверки целостности), а не тождество иностранной процедуры национальной.

3. Выявлено противоречие между частью четвёртой статьи 95¹ УПК Республики Узбекистан, устанавливающей формальное основание недопустимости, и природой международного сотрудничества, при котором следственное действие совершается по праву запрашиваемого государства; предложен способ его устранения.

4. Показано, что статья 201¹ УПК, допускающая представление электронных данных по собственной инициативе, при отсутствии территориального ограничения фактически создаёт непроработанный канал прямого взаимодействия с иностранными поставщиками услуг, требующий процессуального оформления.

5. Установлено, что национальное законодательство, институционализировав цифровые доказательства во внутреннем измерении, не создало ни одного трансграничного инструмента, вследствие чего внутренняя реформа не обеспечивает доказывания по делам, данные о которых находятся за рубежом.

7. Предложения по совершенствованию законодательства

1. Ввести институт срочного сохранения электронных данных. Проблема: данные утрачиваются до получения судебного решения по части девятой статьи 161 УПК. Предлагается дополнить Кодекс нормой о вынесении мотивированного постановления, обязывающего оператора или поставщика услуг сохранить определённые данные на ограниченный срок без раскрытия их содержания, с последующим получением доступа в установленном порядке. Эффект: устраняется противоречие между гарантией судебного контроля и риском утраты данных.

2. Установить правило о праве, применимом к действиям за рубежом. Проблема: буквальное применение части четвёртой статьи 95¹ УПК к материалам правовой помощи ведёт к отказу от правомерно полученных доказательств. Предлагается закрепить, что процессуальные действия, совершённые компетентным органом иностранного государства по его закону, не признаются недопустимыми по мотиву несоответствия национальной форме, если соблюдены основные гарантии и результат поддаётся проверке. Эффект: снимается формальное основание для утраты доказательств.

3. Определить требования к материалам, поступающим из-за рубежа. Проблема: происхождение переданных данных подтверждается только сопроводительным письмом. Предлагается предусмотреть, что к материалам прилагаются сведения об источнике, времени и способе получения, использованных средствах и значении контрольной суммы, а при их отсутствии — обязанность истребовать недостающие сведения. Эффект: восстанавливается проверяемость цепи владения.

4. Урегулировать получение данных от иностранных поставщиков услуг. Проблема: статья 201¹ УПК допускает добровольное представление данных, не определяя порядка его оформления. Предлагается установить, что такие данные принимаются с составлением протокола по правилам статьи 202, с осмотром первичного носителя или удостоверенной провайдером выгрузки с участием специалиста и с приобщением документа, подтверждающего полномочия представившего лица.

5. Закрепить критерии одностороннего трансграничного доступа. Проблема: часть вторая статьи 140 УПК допускает осмотр в сети Интернет безотносительно к юрисдикции ресурса. Предлагается установить, что осмотр данных, находящихся за пределами Республики Узбекистан, допускается, если данные общедоступны либо получено правомерное согласие лица, уполномоченного их раскрыть; в остальных случаях применяются каналы международного сотрудничества. Эффект: национальная норма приводится в соответствие с международным стандартом [6].

6. Создать круглосуточный контактный пункт. Проблема: обмен по обычным дипломатическим и ведомственным каналам не обеспечивает реагирования в течение часов. Предлагается определить уполномоченный орган, действующий в режиме непрерывной готовности для приёма и направления запросов о сохранении и о неотложном раскрытии данных, — этот институт предусмотрен и Будапештской конвенцией, и Конвенцией ООН [6; 10].

7. Дифференцировать режимы по категориям данных. Проблема: закон оперирует единой категорией электронных данных, тогда как абонентская информация, данные о трафике и содержание сообщений различаются по степени вторжения в частную жизнь. Предлагается закрепить различие и связать с ним объём требуемых гарантий, следуя логике Второго дополнительного протокола [7; 14; 15]. Эффект: обеспечивается соразмерность ограничений.

8. Распространить судебный контроль на международный канал. Проблема: требование судебного решения относится к выемке и обыску, но не к получению тех же данных через правовую помощь. Предлагается установить, что запрос, направленный в целях получения личных электронных данных, требует того же судебного решения, что и их выемка внутри страны. Эффект: устраняется неравенство гарантий в зависимости от способа получения.

9. Подготовить исполнение договорных обязательств. Проблема: подписание Конвенции ООН против киберпреступности предполагает наличие внутренних процедур, способных обеспечить исполнение её положений [10; 12]. Предлагается предусмотреть в Кодексе главу о

международном сотрудничестве при получении электронных данных, объединяющую предложения 1—8, и разработать межведомственный порядок взаимодействия с учётом методических материалов международных организаций [18; 19; 20].

Заключение

Трансграничное получение цифровых доказательств не является частным случаем правовой помощи. Изменились все три элемента классической конструкции: объект утратил устойчивую связь с территорией, срок его существования стал короче срока исполнения поручения, а фактическим держателем информации стал частный субъект, находящийся вне отношений между государствами. Поэтому ускорение прежних процедур проблему не решает — необходим иной набор инструментов.

Анализ показал, что действующие в мире решения группируются в четыре модели, различающиеся адресатом требования и субъектом контроля законности, и что для государства, не входящего в интеграционное объединение, реалистична связка «сохранение — запрос — проверяемость». Ключевым выводом является предложенный критерий допустимости: иностранное цифровое доказательство должно оцениваться по проверяемости результата, а не по совпадению иностранной процедуры с национальной формой.

Применительно к Республике Узбекистан установлено, что внутренняя реформа, проведённая Законом от 21 ноября 2024 года № ЗРУ-1003, создала развитый национальный режим цифровых доказательств, но не сопровождалась созданием трансграничных механизмов; в результате по делам, доказательства по которым находятся за рубежом, новые нормы применяться не могут. Подписание Конвенции ООН против киберпреступности задаёт естественный горизонт для устранения этого пробела. Сформулированные девять предложений — от института срочного сохранения данных до главы о международном сотрудничестве при получении электронных данных — образуют минимально необходимый комплекс, при котором национальное уголовное судопроизводство окажется способным работать с доказательствами, физически находящимися вне его юрисдикции.

Список использованных источников

1. Уголовно-процессуальный кодекс Республики Узбекистан, утверждённый Законом Республики Узбекистан от 22 сентября 1994 года № 2013-XII. URL: https://lex.uz/ru/docs/111463

2. 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». URL: https://lex.uz/ru/docs/7228823

3. Постановление Пленума Верховного суда Республики Узбекистан от 25 мая 2012 года № 6 «О некоторых вопросах международного сотрудничества в сфере судопроизводства по гражданским и уголовным делам» (в редакции постановления Пленума от 30 ноября 2018 года № 34). URL: https://lex.uz/ru/docs/2028822

4. Постановление Президента Республики Узбекистан от 21 июня 2024 года № ПП-229 «О мерах по организации научно-исследовательской деятельности в сфере цифровой криминалистики». URL: https://lex.uz/ru/docs/6977762

5. Конвенция о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам (Минск, 22 января 1993 года).

6. Council of Europe. Convention on Cybercrime (Budapest Convention), ETS No. 185, Budapest, 23 November 2001. URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention

7. Council of Europe. Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, CETS No. 224, Strasbourg, 12 May 2022.

8. Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings. URL: https://eur-lex.europa.eu/eli/reg/2023/1543/oj

9. Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings. URL: https://eur-lex.europa.eu/eli/dir/2023/1544/oj

10. Конвенция Организации Объединённых Наций против киберпреступности. Резолюция Генеральной Ассамблеи ООН A/RES/79/243 от 24 декабря 2024 года. URL: https://www.un.org/ru/documents/treaty/A-RES-79-243

11. UNODC. United Nations Convention against Cybercrime: status, signature and ratification. URL: https://www.unodc.org/unodc/en/cybercrime/convention/home.html

12. UNODC. UN Convention against Cybercrime opens for signature in Hanoi, Viet Nam. Press release, 25 October 2025. URL: https://www.unodc.org/unodc/en/press/releases/2025/October/un-convention-against-cybercrime-opens-for-signature-in-hanoi--viet-nam.html

13. Clarifying Lawful Overseas Use of Data Act (CLOUD Act), Pub. L. No. 115-141, div. V (2018) (United States).

14. Eurojust, SIRIUS Project. Article 7 of the Second Additional Protocol to the Budapest Convention on Cybercrime: Disclosure of Subscriber Information. 2023. URL: https://www.eurojust.europa.eu/publication/article-7-second-additional-protocol-budapest-convention-cybercrime-disclosure

15. Eurojust, SIRIUS Project. Article 8 of the Second Additional Protocol to the Convention on Cybercrime: Giving Effect to Orders from Another Party for Expedited Production of Subscriber Information and Traffic Data. 2024. URL: https://www.eurojust.europa.eu/publication/article-8-second-additional-protocol-convention-cybercrime-giving-effect-orders-another

16. Council of Europe, T-CY Cloud Evidence Group. Criminal justice access to electronic evidence in the cloud: Final report. Strasbourg, 16 September 2016.

17. Council of Europe. Joining the Convention on Cybercrime: Benefits. Version of 9 July 2025. URL: https://rm.coe.int/cyber-buda-benefits-2025-9-july-en/1680b6b132

18. UNODC. Comprehensive Study on Cybercrime. Vienna: United Nations Office on Drugs and Crime, 2013.

19. UNODC. Education for Justice (E4J). Cybercrime Module 7: International Cooperation against Cybercrime. URL: https://www.unodc.org/e4j/

20. ISO/IEC 27037:2012. Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. Geneva: ISO, 2012.

21. Stoykova R. Digital evidence: Unaddressed threats to fairness and the presumption of innocence // Computer Law & Security Review. 2021. Vol. 42. Art. 105575. DOI: 10.1016/j.clsr.2021.105575

22. Stoykova R. The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations // Computer Law & Security Review. 2023. Vol. 49. Art. 105801. DOI: 10.1016/j.clsr.2023.105801

23. Miller C. M. A survey of prosecutors and investigators using digital evidence: A starting point // Forensic Science International: Synergy. 2023. Vol. 6. Art. 100296. DOI: 10.1016/j.fsisyn.2022.100296

24. Varbanova G. Electronic Evidence as an Independent Legal Phenomenon: Theoretical Framework and European Practice // Journal of Digital Technologies and Law. 2025. Vol. 3, No. 3. P. 497–511. DOI: 10.21202/jdtl.2025.20

25. Sokol P., Rózenfeldová L., Lučivjanská K., Harašta J. IP addresses in the context of digital evidence in the criminal and civil case law of the Slovak Republic // Forensic Science International: Digital Investigation. 2020. Vol. 32. Art. 300972. DOI: 10.1016/j.fsidi.2019.300972

26. E-evidence Regulation and Directive Published // eucrim — The European Criminal Law Associations' Forum. 2023. URL: https://eucrim.eu/news/e-evidence-regulation-and-directive-published/