Жамият ва инновациялар –
Общество и инновации –
Society and innovations
Journal home page:
https://inscience.uz/index.php/socinov/index

Boundaries of the Principle of Immediacy in the Use of Digital Evidence at the Pre-trial Stage

Malikabonu ABDULLAEVA[1]

Tashkent State Transport University

ARTICLE INFO

Article history:
Received September 2025
Received in revised form
5 September 2025
Accepted 10 October 2025
Available online
25 October 2025

Keywords:
Digital evidence,
principle of immediacy,
pre-trial proceedings,
data authentication,
forensic examination.

ABSTRACT

This article examines the limits of the principle of immediacy in the use of digital evidence at the pre-trial stage of criminal proceedings in Uzbekistan. The rapid digital transformation of law-enforcement practice has introduced challenges arising from the technical character of electronic data, the need for specialised expertise, cryptographic protections, authentication difficulties, and the imperative of preserving the integrity of digital media. The author analyses how digital technologies affect an investigator's ability to directly perceive evidence and highlights procedural risks associated with electronic data – its volatility, cross-border nature, and dependence on expert examinations. The study emphasises the necessity of modernising procedural legislation, introducing specific rules on the handling and admissibility of digital evidence, and striking a balance between technological capabilities and fundamental principles of criminal justice.

2181-1415/© 2025 in Science LLC.
DOI: https://doi.org/10.47689/2181-1415-vol6-iss10/S-pp438-447

Sudgacha bo‘lgan bosqichda raqamli dalillardan foydalanishda bevosita dalillarni tekshirish tamoyilining chegaralari

Kalit so‘zlar:
Raqamli dalillar,
bevositalik prinsipi,
dastlabki tergov,
ma’lumotlarni
autentifikatsiya qilish,
sud ekspertizasi.

ANNOTATSIYA

Maqola O‘zbekiston jinoyat-protsessida raqamli dalillardan foydalanishda bevositalik prinsipining amal qilish chegaralarini tahlil qilishga bag‘ishlangan. Huquqni qo‘llashning raqamlashtirilishi elektron axborotning texnik xususiyatlari, mutaxassis jalb qilish zarurati, ma’lumotlarning kriptografik himoyasi, raqamli dalillarni identifikatsiya qilish va ularning

[1] Acting Associate Professor, Department of Public International Law, Tashkent State Transport University.
E-mail: bonua077@gmail.com

o‘zgarmasligini ta’minlash bilan bog‘liq yangi muammolarni yuzaga keltirdi. Muallif surishtiruvchining dalillarni bevosita idrok etish imkoniyatiga raqamli texnologiyalarning ta’sirini, shuningdek elektron ma’lumotlar bilan ishlashda paydo bo‘ladigan protsessual xatarlarni – dalillarning “uchuvchanligi”, transchegaraviyligi va ekspert xulosalariga ortiqcha tayanishni tahlil qiladi. Tadqiqot jinoyat-protsessual qonunchilikni takomillashtirish, raqamli dalillar bo‘yicha maxsus normalarni joriy etish hamda texnik imkoniyatlar va protsessual tamoyillar o‘rtasidagi muvozanatni ta’minlash zarurligini asoslaydi.

Границы действия принципа непосредственности при использовании цифровых доказательств на досудебном стадии

Ключевые слова:
цифровые доказательства, принцип непосредственности, досудебное производство, аутентификация данных судебная экспертиза.

АННОТАЦИЯ

Статья посвящена анализу границ действия принципа непосредственности при использовании цифровых доказательств на досудебной стадии уголовного процесса Узбекистана. В условиях цифровизации правоприменительной деятельности возникает комплекс новых проблем, связанных с технической природой электронных данных, необходимостью привлечения специалистов, криптографической защитой информации, сложностями аутентификации и обеспечения неизменности цифровых носителей. Автор рассматривает влияние цифровых технологий на возможность следователя лично воспринимать доказательства, анализирует процессуальные риски, возникающие при работе с электронными данными, включая их «летучесть», трансграничность и зависимость от экспертных исследований. Исследование подчеркивает необходимость совершенствования процессуального законодательства, введения специальных норм о цифровых доказательствах и обеспечения баланса между технологическими возможностями и соблюдением основополагающих принципов уголовного судопроизводства.

Широкое применение информационных технологий является неотъемлемым элементом современного судопроизводства, что обусловлено необходимостью повышения информационной открытости, эффективного взаимодействия судов с гражданами и организациями.

Наиболее актуальные проблемы цифровизации в судопроизводстве стали очевидны в период карантина 2020 года, в результате которого произошла стремительная вынужденная «перестройка» работы следственных органов в пользу активного применения информационных технологий. При этом, первоочередными можно назвать вопросы воздействия информационных технологий на основополагающие принципы осуществления судопроизводства, в том числе, на принцип непосредственности.

Принцип непосредственности в уголовном процессе Узбекистана традиционно понимается как требование о том, чтобы суд основывал свои выводы на доказательствах, исследованных непосредственно в судебном заседании. Однако с развитием цифровых технологий и появлением электронных доказательств возникают новые вызовы для применения этого принципа на досудебной стадии производства по уголовному делу. Согласно статье 18 Уголовно-процессуального кодекса Республики Узбекистан, суд основывает приговор лишь на тех доказательствах, которые были непосредственно исследованы в судебном заседании, что создает особые требования к процедуре сбора и фиксации цифровых доказательств на досудебной стадии [1].

Цифровые доказательства представляют собой информацию, созданную, хранящуюся или передаваемую в электронной форме, которая может быть использована в суде для установления обстоятельств, имеющих значение для правильного разрешения уголовного дела. К таким доказательствам относятся данные с компьютеров, мобильных телефонов, серверов, облачных хранилищ, данные электронной переписки, записи видеонаблюдения в цифровом формате, данные геолокации и другая электронная информация. В досудебном производстве следователи и дознаватели органов внутренних дел, прокуратуры и Службы государственной безопасности Узбекистана регулярно сталкиваются с необходимостью изъятия, фиксации и исследования таких доказательств в рамках следственных действий.

Соблюдение принципа непосредственности является неотъемлемой составляющей судебного процесса, целью которого является вынесение законного и обоснованного решения, восстановление нарушенных прав и законных интересов лиц, участвующих в процессе. В научной литературе справедливо отмечается, что принцип непосредственности позволяет суду «установить фактические обстоятельства дела» [2, с. 110], «воспринимая их непосредственно и по возможности черпая сведения из первоисточников, отдавая «преимущество первоначальным доказательствам перед производными» [3, с. 181], стремиться исследовать «фактические обстоятельства дела по первоисточникам» [4, с. 87].

Сложности в реализации принципа непосредственности могут быть вызваны также появлением новых средств доказывания, обусловленных цифровизацией. Предметом исследования суда являются не только традиционные, бумажные носители информации или вещественные доказательства, но и электронные доказательства, полученные при использовании современных технологий (электронная почта, Интернет), документы, подписанные электронной подписью, и иные.

На практике возникают затруднения, связанные с тем, каким образом необходимо исследовать электронные доказательства: признать их письменными доказательствам, вещественными доказательствами или выделить в отдельную группу средств доказывания.

Отсутствует подробная процедура проверки достоверности электронных документов со стороны правоохранительных органов. Предоставляемая в качестве доказательств переписка по электронной почте, в мессенджерах, социальных сетях, страницы интернет-сайтов не имеют оригинал для сравнения; для проверки идентичности информации на бумажном носителе, представленном в качестве

образа имеющейся информации на электронном носителе, может потребоваться помощь специалиста. Существует проблема идентификации отправителя электронного документа, которую в качестве «одной из серьезных информационных и правовых проблем» отмечает АТ. Боннер, аналогичная проблема возникает и с идентификацией отправителя сообщения в мессенджерах, социальных сетях. При оценке документа, подписанного электронной цифровой подписью, у правоохранительных органов появляется обязанность идентифицировать данное лицо, установить принадлежность электронной цифровой подписи конкретному субъекту, а также срок действия и подлинность сертификата [5].

Кроме этого, на досудебной стадии принцип непосредственности проявляется через требование о том, чтобы следователь лично производил следственные действия по обнаружению и изъятию цифровых доказательств или непосредственно руководил этим процессом [6, С. 65]. Статья 98 УПК Республики Узбекистан определяет, что следственные действия производятся следователем, который несет ответственность за их законность и правильность оформления. При производстве обыска с изъятием электронных носителей информации, осмотре компьютерных систем или выемке электронной переписки следователь должен непосредственно присутствовать и фиксировать все обстоятельства обнаружения и изъятия цифровых данных в протоколе следственного действия.

Однако техническая сложность работы с цифровыми доказательствами часто требует привлечения специалистов, что создает определенное противоречие с принципом непосредственности. Согласно статье 127 УПК Узбекистана, следователь вправе привлечь специалиста для содействия в обнаружении, закреплении и изъятии доказательств, применения технических средств. В практике это означает, что специалист в области компьютерной криминалистики фактически осуществляет техническую работу по извлечению данных из электронных устройств, в то время как следователь может не обладать достаточными знаниями для оценки правильности этих действий в момент их совершения.

Проблема усугубляется тем, что многие цифровые доказательства находятся в зашифрованном виде или требуют специального программного обеспечения для их извлечения и интерпретации. Криптографические методы защиты информации, применяемые в современных устройствах и приложениях, делают невозможным непосредственное восприятие содержания цифровых данных без использования технических средств декодирования. Следователь не может непосредственно ознакомиться с содержимым зашифрованного файла или удаленной информации, что требует опосредованного исследования через заключение эксперта или пояснения специалиста [7, С.110].

Назначение судебной экспертизы в отношении цифровых доказательств становится обычной практикой на досудебной стадии. Статья 181 УПК Республики Узбекистан предусматривает, что экспертиза назначается в случаях, когда для разрешения вопросов, имеющих значение для дела, требуются специальные знания. Компьютерно-технические экспертизы проводятся в экспертных учреждениях Министерства юстиции, Министерства внутренних дел и других ведомств Узбекистана для исследования содержимого электронных носителей, восстановления удаленных данных, установления факта модификации файлов и решения других вопросов, связанных с цифровыми доказательствами.

Заключение эксперта по своей природе является производным доказательством, поскольку эксперт не наблюдает событие преступления непосредственно, а делает выводы на основании исследования представленных ему объектов. В случае с цифровыми доказательствами эксперт исследует электронные данные, которые сами по себе являются отображением определенной информации, что создает дополнительный уровень опосредования. Суд в судебном заседании будет исследовать не сами цифровые данные в их первоначальном виде, а заключение эксперта о содержании и характеристиках этих данных, что ограничивает действие принципа непосредственности.

Особую сложность представляет проблема идентичности цифровых доказательств на разных стадиях уголовного процесса. В отличие от материальных объектов, которые могут быть индивидуализированы по физическим признакам, электронные данные идентифицируются через технические характеристики, такие как хеш-суммы, метаданные, временные метки и другие атрибуты. Для обеспечения возможности последующей проверки подлинности цифровых доказательств в суде необходимо с момента их обнаружения применять специальные методы фиксации, включая вычисление криптографических хеш-функций изъятых данных, что требует специальных технических знаний и программных средств [8, С. 102].

Международная практика, отраженная в рекомендациях Совета Европы по киберпреступности, предполагает использование метода создания точной побитовой копии (forensic image) цифрового носителя с одновременным вычислением контрольной суммы для обеспечения неизменности данных. Такая копия создается с использованием специализированного оборудования и программного обеспечения, которое предотвращает любые изменения оригинальных данных в процессе копирования. Однако в практике правоохранительных органов Узбекистана такие технологии применяются не всегда последовательно, что создает риски для признания цифровых доказательств допустимыми в суде.

Проблема непосредственности также возникает при работе с цифровыми доказательствами, находящимися за пределами Узбекистана, например, в облачных хранилищах на серверах иностранных компаний. Согласно статье 466 УПК Республики Узбекистан, для получения доказательств, находящихся за границей, требуется направление запроса о правовой помощи иностранному государству. Процесс получения таких данных является длительным и многоступенчатым, что исключает непосредственное восприятие следователем обстоятельств обнаружения и фиксации этих доказательств, поскольку эти действия выполняются иностранными правоохранительными органами в соответствии с их национальным законодательством.

Законодательство Узбекистана в области электронных доказательств постепенно развивается. Закон Республики Узбекистан «Об электронном документообороте» от 29 апреля 2004 года устанавливает правовой режим электронных документов и их юридическую силу, определяя условия признания электронного документа равнозначным документу на бумажном носителе [9]. Однако специальные процессуальные нормы, регламентирующие работу с цифровыми доказательствами в уголовном процессе, остаются недостаточно детализированными, что создает пробелы в правовом регулировании применения принципа непосредственности к таким доказательствам.

Верховный суд Республики Узбекистан в своих разъяснениях обращает внимание судов на необходимость тщательной проверки допустимости доказательств, полученных с использованием технических средств. В постановлении Пленума Верховного суда «О судебном приговоре» подчеркивается, что суд обязан проверить соблюдение процессуального порядка получения каждого доказательства и исключить из совокупности доказательств те, которые получены с нарушением закона. Это требование приобретает особое значение для цифровых доказательств, процедура получения которых часто бывает сложной и многоэтапной [10].

Практика показывает, что нарушения процедуры изъятия и фиксации цифровых доказательств на досудебной стадии нередко приводят к признанию их недопустимыми в судебном разбирательстве. Типичными нарушениями являются отсутствие понятых при производстве следственных действий по изъятию электронных носителей, неправильное оформление протоколов осмотра с недостаточно подробным описанием технических характеристик изъятых устройств, отсутствие отметок о применении специальных технических средств для фиксации цифровых данных, несоблюдение процедуры опечатывания изъятых электронных носителей. Все эти нарушения препятствуют реализации принципа непосредственности в судебном разбирательстве, поскольку суд не может убедиться в том, что представленные доказательства идентичны тем, которые были изъяты на месте происшествия.

Вопрос о границах действия принципа непосредственности при работе с метаданными электронных документов также требует отдельного рассмотрения. Метаданные содержат служебную информацию о файле, включая дату создания, автора, историю изменений, но сами по себе не являются содержанием документа. Следователь на досудебной стадии может зафиксировать метаданные в протоколе осмотра или получить заключение эксперта об их содержании, однако суд при исследовании доказательств может не иметь возможности непосредственно ознакомиться с этими метаданными, если электронный носитель был изменен или исходный файл более недоступен. Это создает ситуацию, когда суд вынужден полагаться на производные доказательства, что противоречит строгому пониманию принципа непосредственности.

Особую категорию составляют данные, полученные в результате проведения оперативно-розыскных мероприятий. Закон Республики Узбекистан «Об оперативно-розыскной деятельности» от 29 августа 2001 года предусматривает возможность получения информации о соединениях между абонентами и абонентскими устройствами, прослушивания телефонных переговоров, снятия информации с технических каналов связи. Результаты таких мероприятий могут быть представлены в уголовный процесс, однако сам процесс их получения происходит вне процессуальной формы, без участия следователя и процессуальных гарантий, что значительно ограничивает применение принципа непосредственности к таким материалам [11].

Сравнительный анализ показывает, что в странах с развитой системой работы с цифровыми доказательствами разработаны детальные протоколы, обеспечивающие максимальную прозрачность и контролируемость процесса обращения с электронными данными от момента их обнаружения до

представления в суд. В США Федеральные правила по доказательствам (Federal Rules of Evidence) содержат специальные положения о порядке представления и аутентификации электронных доказательств, включая требования к документированию процесса извлечения данных и сохранения целостности информации. Опыт таких юрисдикций может быть полезен для совершенствования узбекского законодательства в этой сфере [12].

Развитие технологий блокчейн и распределенных реестров создает новые вызовы для принципа непосредственности. Информация, записанная в блокчейн, распределена между множеством узлов сети и не имеет единого физического местонахождения, что делает невозможным ее изъятие в традиционном понимании. Следователь не может непосредственно воспринять всю совокупность данных в распределенном реестре, а может лишь зафиксировать определенную запись через специальные программные инструменты. Это требует переосмысления процессуальной формы работы с такими доказательствами и адаптации принципа непосредственности к новым технологическим реалиям.

Искусственный интеллект и машинное обучение также влияют на границы применения принципа непосредственности. Когда цифровое доказательство представляет собой результат обработки данных алгоритмом машинного обучения, например, распознавание лиц на видеозаписи или анализ больших массивов информации для выявления связей между подозреваемыми, возникает вопрос о том, можно ли считать такой результат непосредственно воспринятым следователем или судом. Алгоритм действует как черный ящик, процесс принятия решения, которым не всегда может быть объяснен даже его разработчиками, что создает проблему для обеспечения прозрачности доказывания.

Процессуальная фиксация цифровых доказательств требует составления детальных протоколов следственных действий с указанием всех технических параметров. Согласно статье 111 УПК Узбекистана, в протоколе следственного действия должны быть указаны технические средства, примененные при производстве следственного действия, условия и порядок их использования, объекты, к которым эти средства были применены, и полученные результаты. Для цифровых доказательств это означает необходимость указания модели и серийного номера изъятого электронного устройства, использованного программного обеспечения для копирования данных, вычисленных хеш-сумм, примененных методов шифрования и других технических деталей, которые позволят впоследствии суду оценить подлинность представленных доказательств.

Право на защиту подозреваемого и обвиняемого также связано с принципом непосредственности при работе с цифровыми доказательствами. Статья 24 УПК Республики Узбекистан гарантирует обвиняемому право иметь защитника, который может участвовать в производстве следственных действий. При изъятии и осмотре цифровых доказательств присутствие защитника обеспечивает дополнительные гарантии соблюдения процессуальных прав, позволяя стороне защиты контролировать процесс фиксации доказательств и при необходимости заявлять ходатайства о проведении дополнительных действий по закреплению информации. Однако техническая сложность работы с электронными данными может затруднять эффективное участие защитника, не обладающего специальными познаниями в области компьютерной криминалистики.

Концепция «летучести» цифровых доказательств требует особого внимания на досудебной стадии. Некоторые виды электронной информации, такие как данные в оперативной памяти компьютера, активные сетевые соединения, временные файлы, могут быть утрачены в течение минут или часов, если не будут своевременно зафиксированы. Это создает необходимость в оперативных действиях следователя и невозможности отложить изъятие таких доказательств, что может вступать в противоречие с необходимостью получения судебного разрешения на производство некоторых следственных действий. Законодательство Узбекистана предусматривает возможность производства неотложных следственных действий до возбуждения уголовного дела в случаях, не терпящих отлагательства, что может быть применимо к ситуациям с летучими цифровыми доказательствами.

Трансграничный характер цифровой среды создает юрисдикционные проблемы для реализации принципа непосредственности. Когда данные передаются через серверы, расположенные в разных странах, или когда преступление совершается с использованием компьютерных систем, физически находящихся за пределами Узбекистана, следователь не может непосредственно получить доступ к этим системам без соблюдения процедур международного сотрудничества. Будапештская конвенция о киберпреступности 2001 года устанавливает механизмы международного сотрудничества в этой сфере [13], однако Узбекистан не является участником этой конвенции, что ограничивает возможности оперативного получения цифровых доказательств из-за рубежа.

Проблема аутентификации цифровых доказательств непосредственно связана с принципом непосредственности. Суд должен убедиться в том, что представленное доказательство является именно тем, за что его выдают, и что оно не было изменено с момента изъятия. Для традиционных доказательств это обеспечивается через индивидуальные признаки объекта и процедуру хранения вещественных доказательств. Для цифровых доказательств аутентификация требует технических методов подтверждения целостности данных, включая использование электронной подписи, блокировку носителей от записи, применение специализированных программ для создания защищенных копий. Отсутствие таких мер на досудебной стадии делает невозможным для суда непосредственно убедиться в подлинности доказательств.

Практика назначения повторных и дополнительных экспертиз по цифровым доказательствам свидетельствует о сложностях в реализации принципа непосредственности. Согласно статье 194 УПК Узбекистана, повторная экспертиза назначается в случае необоснованности заключения эксперта или сомнений в его правильности. Для цифровых доказательств такие ситуации возникают довольно часто из-за использования различных методик исследования, разночтений в интерпретации технических данных, быстрого устаревания технологий и методов анализа. Множественность экспертных исследований одного и того же объекта создает дополнительные уровни опосредования между судом и первоначальными доказательствами.

Использование видеозаписи процесса производства следственных действий с цифровыми доказательствами может служить дополнительной гарантией соблюдения принципа непосредственности. Статья 112 УПК Республики Узбекистан предусматривает возможность применения видеозаписи при производстве

следственных действий. Видеофиксация процесса изъятия электронных носителей, подключения к компьютерным системам, копирования данных позволяет суду впоследствии непосредственно ознакомиться с обстоятельствами получения доказательств и оценить соблюдение процессуальных требований. Однако на практике видеозапись следственных действий применяется не систематически, что снижает возможности судебного контроля.

Развитие института специалиста в области компьютерной криминалистики является важным направлением совершенствования работы с цифровыми доказательствами. В настоящее время в правоохранительных органах Узбекистана создаются специализированные подразделения по борьбе с киберпреступностью, сотрудники которых получают подготовку в области работы с электронными доказательствами. Однако системная подготовка следователей для самостоятельной работы с цифровыми доказательствами остается недостаточной, что приводит к чрезмерной зависимости от специалистов и экспертов и ограничивает возможность следователя непосредственно воспринимать и оценивать электронную информацию.

Цифровые доказательства динамичного характера, такие как данные в социальных сетях, содержимое веб-сайтов, онлайн-чаты, представляют особую сложность для фиксации. Эта информация может изменяться в режиме реального времени, удаляться пользователями или администраторами сервисов, становиться недоступной в результате технических сбоев. Следователь на досудебной стадии должен обеспечить фиксацию такой информации в момент ее обнаружения, используя скриншоты, архивирование веб-страниц, сохранение переписки, однако такие методы не всегда обеспечивают достаточную степень достоверности для суда, который не может непосредственно проверить, соответствовало ли зафиксированное состояние цифровой информации действительности на момент следственного действия.

Принцип непосредственности тесно связан с правом на справедливое судебное разбирательство, гарантированным статьей 26 Конституции Республики Узбекистан [14]. Возможность суда непосредственно исследовать доказательства является важнейшей гарантией справедливости, позволяя суду формировать собственное убеждение на основе непосредственного восприятия доказательств, а не полагаться на выводы других лиц. Для цифровых доказательств реализация этого права требует создания технических условий для демонстрации электронной информации в судебном заседании, обеспечения возможности для сторон задавать вопросы экспертам и специалистам, проводить альтернативные исследования представленных данных.

Стандарты доказывания при использовании цифровых доказательств требуют пересмотра с учетом их особенностей. Традиционный подход, при котором суд оценивает доказательства по своему внутреннему убеждению, основанному на всестороннем, полном и объективном рассмотрении всех обстоятельств дела в их совокупности, может быть недостаточным для цифровых доказательств, технические аспекты которых не всегда доступны для понимания судьями без специальной подготовки. Это создает риск формального подхода к оценке заключений экспертов без критического анализа их методологии и выводов, что противоречит принципу непосредственности.

Перспективы развития законодательства Узбекистана в области цифровых доказательств связаны с необходимостью внесения изменений в Уголовно-процессуальный кодекс, которые бы детально регламентировали процедуру работы с электронной информацией. Необходимо закрепление понятия цифрового доказательства, определение процессуального статуса электронных копий и их соотношения с оригиналами, установление требований к технологиям фиксации и хранения электронных данных, регламентация процедуры обеспечения целостности цифровой информации, определение квалификационных требований к специалистам и экспертам в области компьютерной криминалистики. Такие изменения должны обеспечить баланс между технологическими возможностями работы с цифровыми данными и процессуальными гарантиями прав участников уголовного процесса, включая реализацию принципа непосредственности на всех стадиях производства по уголовному делу.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ:

1. Уголовно-процессуальный кодекс Республики Узбекистан, от 01.04.1995г.
2. Васьковский Е.В. Учебник гражданского процесса. М., 2003
3. Гурвич М.А. Избранные труды I М.А. Гурвич; М^ им. М^. Ломоносова, Юрид. фак., Каф. Гражд. Процесса, Кубан. гос. ун-т, Юрид. фак., Каф. гражд. процесса и трудового права. – Краснодар: Совет. Кубань, 2006. – 544 с. – (Классика российской процессуальной науки. Т. 2)
4. Лебедь КА, Лукьянова И.Н. О гарантиях отдельных принципов гражданского и арбитражного процесса. В сб.: Новый этап судебной реформы: Конституционные возможности и вызовы I Под ред. Т.Е. Абовой, Т.К. Андревой, В.В. Зайцева, О.В. Зайцева, Г.Д. Улетовой. М., 2020. С. 356-367
5. Боннер АТ. Доказательственное значение информации, полученной из Интернета: Декабрь II Закон: Декабрь. – М., 2007, № 12. – С. 85-98.
6. Давронов А.Р. Перспективы внедрения технологий искусственного интеллекта в уголовный процесс Т.: Издание ТГЮУ, 2024. С. 65.
7. Давронов А. Новые виды киберпреступлений: современные методы их выявления и раскрытия. Монография. Т.: Издание ТГЮУ, 2024. 110
8. Хидоятов Б.Б., Давронов А.Р. Адвокат в уголовном процессе [текст]: учебник. Ташкент: Издательство ТГЮУ, 2024. – С. 102.
9. Закон Республики Узбекистан «Об электронном документообороте» от 29 апреля 2004 года
10. Постановление Пленума Верховного суда Республики Узбекистан «О судебном приговоре». от 23.05.2014 г. № 07. П. 6.
11. Закон Республики Узбекистан «Об оперативно-розыскной деятельности» от 29 августа 2001 года
12. Federal Rules of Evidence. The Federal Rules of Evidence became federal law on January 2, 1975, when President Ford signed the Act to Establish Rules of Evidence for Certain Courts and Proceedings, Pub. L. No. 93-595.
13. Будапештская конвенция о киберпреступности 2001 года.
14. Конституция Республики Узбекистан. Национальная база данных законодательства, 01.05.2023 г., № 03/23/837/0241. Ст. 26.