



Б.А. Жилхайдарова

*Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан,
г. Косшы, Республика Казахстан*

ОСМОТР, ОБЫСК И ВЫЕМКА В УСЛОВИЯХ ЦИФРОВИЗАЦИИ: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ

Аннотация. В статье рассматриваются особенности производства осмотра, обыска и выемки в условиях цифровизации уголовного процесса. Анализируются положения Уголовно-процессуального кодекса Республики Казахстан, регулирующие традиционные следственные действия, и оценивается их применимость к цифровым данным как объекту доказывания. Исследуются особенности электронных доказательств, связанные с риском их изменения или уничтожения, а также необходимость участия специалиста в работе с цифровыми носителями информации. Особое внимание уделяется зарубежному опыту, в частности, институту цифрового обыска в законодательстве Армении. По результатам исследования сформулированы предложения по совершенствованию уголовно-процессуального законодательства в сфере работы с цифровыми доказательствами, обеспечению их сохранности и повышению эффективности расследования уголовных правонарушений. Обосновывается необходимость адаптации традиционных следственных действий к условиям цифровой среды.

Ключевые слова: доказательства; осмотр; принцип; специалист; уголовный процесс; выемка; цифровой обыск; цифровые доказательства.

Б.А. Жилхайдарова

*Қазақстан Республикасы Бас прокуратурасының жанындағы Құқық қорғау органдары академиясы,
Қосшы қ., Қазақстан Республикасы*

ЦИФРЛАНДЫРУ ЖАҒДАЙЫНДАҒЫ ҚАРАП-ТЕКСЕРУ, ТІНТУ ЖӘНЕ АЛУ: ҚҰҚЫҚТЫҚ РЕТТЕУ ПРОБЛЕМАЛАРЫ МЕН ПЕРСПЕКТИВАЛАРЫ

Аннотация. Мақалада қылмыстық процесті цифрландыру жағдайындағы қарап-тексеруді, тінтуді және алуды жүргізудің ерекшеліктері қарастырылады. Дәстүрлі тергеу әрекеттерін реттейтін Қазақстан Республикасы Қылмыстық-процестік кодексінің ережелері талданып, олардың дәлелдеу объектісі ретіндегі цифрлық деректерге қолданылу мүмкіндігі бағаланады. Электрондық дәлелдемелердің өзгертілу немесе жойылу қаупіне байланысты ерекшеліктері, сондай-ақ цифрлық ақпарат жеткізгіштермен жұмыс істеу кезінде маманның қатысу қажеттілігі зерттеледі. Шетелдік тәжірибеге, атап айтқанда, Армения заңнамасындағы цифрлық тінту институтына ерекше назар аударылады. Зерттеу нәтижелері бойынша цифрлық дәлелдемелермен жұмыс істеу, олардың сақталуын қамтамасыз ету және қылмыстық құқық бұзушылықтарды тергеп-тексерудің тиімділігін арттыру саласындағы қылмыстық-процестік заңнаманы жетілдіру жөнінде ұсыныстар тұжырымдалады. Дәстүрлі тергеу әрекеттерін цифрлық орта жағдайына бейімдеу қажеттілігі негізделеді.

Түйінді сөздер: айғақтар; қарап-тексеру; қағидат; маман; қылмыстық процесс; алу жүргізу; цифрлық тінту; цифрлық дәлелдемелер.

B.A. Zhilkhaidarova

*The Law Enforcement Academy under the Prosecutor General's Office of the Republic of Kazakhstan,
Kosshy, the Republic of Kazakhstan*

INSPECTION, SEARCH, AND SEIZURE IN THE CONTEXT OF DIGITALIZATION: PROBLEMS AND PROSPECTS OF LEGAL REGULATION

Abstract. The article examines the peculiarities of inspection, search, and seizure procedures in the context of the digitalization of criminal proceedings. The provisions of the Criminal Procedure Code of the Republic of Kazakhstan regulating traditional investigative actions are analyzed, and their applicability to digital data as an object of proof is assessed.



The study explores the specific features of electronic evidence related to the risks of alteration or destruction, as well as the necessity of involving a specialist when handling digital storage devices. Particular attention is paid to foreign experience, especially the institution of digital search in the legislation of Armenia. Based on the research results, proposals are formulated for improving criminal procedural legislation in the field of digital evidence handling, ensuring data integrity, and increasing the effectiveness of criminal investigations. The necessity of adapting traditional investigative actions to the digital environment is substantiated.

Keywords: evidence; inspection; principle; expert; criminal procedure; seizure; digital search; digital evidence.

Введение. Современный этап общественного развития характеризуется активной цифровизацией общественных отношений, которые реализуются не только в физическом мире, но и в цифровой среде, охватывая такие сферы, как экономика, коммуникации и государственное управление. Одновременно с этим трансформируется и преступная деятельность: правонарушения все чаще совершаются с использованием информационно-коммуникационных технологий [1].

В настоящее время значительная часть информации создается, хранится и передается в электронной форме, что неизбежно влияет на механизмы выявления, расследования и доказывания правонарушений, совершаемых с использованием цифровых следов.

В условиях цифровой трансформации изменяются и методы собирания доказательств. Если ранее ключевое значение имели материальные объекты и их внешние признаки, то в настоящее время все большую роль играют электронные данные, существующие в нематериальной форме и зачастую не привязанные к конкретному физическому носителю. Это обуславливает необходимость переосмысления традиционных следственных действий, ориентированных преимущественно на работу с вещественными доказательствами.

Материалы и методы. Материальную основу исследования составили нормы Уголовно-процессуального кодекса Республики Казахстан (далее – УПК РК), а также уголовных кодексов Армении и Российской Федерации (далее – РФ). В исследовании использовались научные труды отечественных и зарубежных авторов по вопросам электронных доказательств. Методологическую основу составили формально-юридический, сравнительно-правовой, системно-структурный методы, а также методы анализа и обобщения.

Результаты, обсуждение. Действующее уголовно-процессуальное законодательство закрепляет такие классические следственные действия, как осмотр, обыск и выемка. Указанные институты исторически формировались исходя из материальной природы объектов доказывания и предполагают их обнаружение, визуальное исследование и изъятие.

Однако применение данных процессуальных форм к цифровой среде выявляет ряд существенных теоретических и практических проблем, в частности, отсутствие в национальном законодательстве самостоятельного процессуального механизма, прямо направленного на извлечение электронной информации. В результате правоприменительная практика вынуждена адаптировать существующие нормы к новым условиям, что приводит к неоднозначности их толкования и рискам нарушения прав участников процесса.

Согласно части 1 статьи 111 УПК РК доказательствами по уголовному делу являются законно полученные фактические данные, на основе которых органы преследования и суд устанавливают наличие или отсутствие преступления, причастность лица и иные обстоятельства, имеющие значение для правильного разрешения дела¹.

Собирание доказательств осуществляется в ходе досудебного расследования и судебного разбирательства посредством проведения процессуальных действий. Оно включает обнаружение, фиксацию и изъятие доказательств.

¹ Уголовно-процессуальный кодекс Республики Казахстан: от 4 июля 2014 г. № 231-V ЗРК [Электронный ресурс]. – Режим доступа: <https://adilet.zan.kz/rus/docs/K1400000231>.



К таким действиям относятся осмотр, обыск и выемка. В ряде государств данные следственные действия рассматриваются как в традиционном, так и в цифровом формате. В этой связи представляется целесообразным оценить, насколько традиционные формы осмотра, обыска и выемки способны обеспечивать эффективное выявление и сбор данных, имеющих значение для уголовного дела.

Как отмечает А. Шарипова, цифровые доказательства все чаще используются при расследовании традиционных преступлений, включая убийства, кражи и наркопреступления. Если ранее их значение недооценивалось, то в настоящее время цифровая криминалистика применяется при расследовании широкого круга деяний, выходя за пределы компьютерных преступлений. Технологическое развитие расширило источники доказательственной информации, включая мобильные устройства, навигационные системы и автомобильные электронные системы [2]. Это подтверждает универсальный характер цифровых следов и их значение для различных категорий уголовных дел.

Согласно части 1 статьи 219 УПК РК, с целью обнаружения и выявления следов уголовного правонарушения и иных материальных объектов, выяснения обстановки происшествия и установления обстоятельств, имеющих значение для дела, лицо, осуществляющее досудебное расследование, производит осмотр местности, помещений, предметов, документов, живых лиц, трупов, животных.

Анализ данной нормы показывает, что объектами осмотра могут выступать местность, помещения, предметы, документы, живые лица, трупы и животные.

Кроме осмотра трупа человека, осмотр всех остальных объектов осуществляется по общим правилам осмотра.

Как отмечает Л. Петросян, несомненно, носители электронной информации, содержащие цифровые данные, в конечном счете являются предметами. Однако доказательственное значение имеет не сам носитель информации с его внешними характеристиками, а его содержимое, закрепленные в нем данные. В этом контексте следует отметить, что, хотя электронная информация закреплена на материальном носителе, она имеет цифровой вид и является объектом виртуального мира, не имеющим материального выражения [3; 158].

С мнением Л. Петросян следует полностью согласиться, поскольку носители электронной информации, содержащие цифровые данные, относятся к объектам материального мира.

Одновременно подчеркивается, что цифровые данные обладают высокой уязвимостью, поскольку могут быть легко изменены или уничтожены [4; 186]. В связи с этим при их фиксации особое значение приобретает соблюдение процессуальных гарантий, включая применение научно-технических средств и участие понятых, что обеспечивает законность и достоверность доказательств.

Согласно общим правилам, осмотр проводится с применением научно-технических средств фиксации его хода и результатов, а в случаях принудительного проведения или неотложности – с участием понятых, что обеспечивает реализацию принципов законности и гласности.

Нарушение этих принципов, в зависимости от характера и существенности, влечет признание процессуальных действий незаконными, отмену принятых решений либо недопустимость полученных доказательств.

Таким образом, особенности природы цифровых данных и их уязвимость к изменению или уничтожению обуславливают необходимость использования специальных процессуальных и технических механизмов при их обнаружении, фиксации и изъятии.

Отдельное значение имеет участие специалиста и эксперта при работе с цифровыми данными, функции которых заключаются в обеспечении целостности информации, ее корректном



копировании и поиске значимых сведений [5].

В связи с этим при собирании и оценке цифровых доказательств особое значение приобретает обеспечение законности их получения и неизменности. В отличие от традиционных следов, которые фиксируются и удостоверяются подписями понятых, цифровые данные требуют дополнительных гарантий сохранности, исключающих возможность их изменения. В этой связи целесообразно использование специальных носителей информации, обеспечивающих сохранение данных в их первоначальном виде после записи.

Данная мера способствует обеспечению принципов уголовного процесса. В остальных случаях общие нормы, регулирующие порядок проведения осмотра, в полной мере позволяют осуществлять данное следственное действие.

Что касается обыска, то он производится с целью обнаружения и изъятия предметов или документов, имеющих значение для дела. В отличие от осмотра, основанием для его проведения является наличие достаточных данных полагать, что такие объекты могут находиться в определенном месте либо у конкретного лица. Таким образом, обыск, в отличие от осмотра, предполагает не только исследование обнаруженных объектов, но и их целенаправленный поиск в предполагаемом месте нахождения.

Близким по своему назначению к обыску является выемка, однако данные следственные действия различаются степенью определенности информации о разыскиваемом объекте. Если при обыске осуществляется поиск предметов или документов, местонахождение которых предполагается, то выемка производится при наличии точных сведений о конкретном предмете или документе и его местонахождении. В связи с их функциональной взаимосвязанностью обыск и выемку целесообразно рассматривать совместно, поскольку порядок их производства урегулирован статьей 254 УПК РК. При этом за исключением личного обыска производство указанных следственных действий осуществляется по общим правилам.

Особый интерес представляет зарубежный опыт, в частности законодательство Армении, где закреплён самостоятельный институт цифрового обыска. В соответствии со статьей 236 УПК Республики Армения цифровой обыск определяется как поиск цифровых данных, содержащихся в электронных устройствах или носителях. При этом данные, имеющие значение для уголовного производства, изымаются путем их копирования на иной носитель с обязательным обеспечением целостности как оригинальных данных, так и созданных копий.

Кроме того, законодатель Армении допускает изъятие не только данных, указанных в постановлении о производстве обыска, но и иной информации, обнаруженной в ходе следственного действия, если по своему содержанию она может быть связана с расследуемым либо иным предполагаемым преступлением. Также предусмотрена возможность распространения цифрового обыска на другие компьютерные системы, доступ к которым возможен из первоначального устройства, при наличии судебного решения и риска утраты либо уничтожения данных².

В отличие от законодательства Армении, в РФ цифровой обыск не был выделен в качестве самостоятельного следственного действия, а регулирование работы с электронной информацией сохранилось в рамках традиционного института обыска. Так, 28 июля 2012 года в часть 9.1 статьи 182 УПК РФ была введена норма, согласно которой изъятие электронных носителей информации осуществлялось с участием специалиста, что усиливало процессуальные гарантии и способствовало обеспечению сохранности доказательственной информации, минимизируя риски

² ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ ԶԵՆԱԿԱՆ ՂԱՏԱՎԱՐՈՒԹՅԱՆ ՕՐԵՆՍԳԻՐԶ: ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ ՕՐԵՆՔԸ Ընդունված է 2021 թվականի հունիսի 30-ին [Электронный ресурс]. – Режим доступа: https://www.irtek.am/views/act.aspx?aid=154481&fbclid=IwAR35mybRiQ-9I0ASsL6f9rLjBLHh8QnPfkMKkX3Wl_Jo9jdsGmmZduosGj0.



утраты или изменения цифровых данных. Однако впоследствии данная норма утратила силу на основании Федерального закона от 27 декабря 2018 года № 533-ФЗ³.

Вместе с тем положения, позволяющие привлекать специалиста и использовать научно-технические средства при производстве следственных действий, изначально присутствовали в УПК РК. Так, согласно части 4 статьи 254, в необходимых случаях обыск производится с участием специалиста, а выемка осуществляется с обязательным применением научно-технических средств фиксации хода и результатов, при необходимости также допускается участие специалиста. Это свидетельствует о более гибком характере отечественного уголовно-процессуального регулирования, позволяющем адаптировать традиционные следственные действия к работе с цифровыми доказательствами без введения самостоятельного института цифрового обыска.

В этой части отечественное уголовно-процессуальное законодательство в целом соответствует современным требованиям обеспечения сохранности цифровых доказательств и реализации процессуальных гарантий при работе с электронной информацией.

Также представляет интерес положение части 9 статьи 254 УПК РК, согласно которому при производстве обыска допускается вскрытие запертых помещений и хранилищ в случае отказа владельца добровольно их открыть при условии недопущения излишнего повреждения имущества. Как видно, законодатель прямо конкретизирует объекты, в отношении которых допускается вскрытие, указывая на помещения и хранилища.

Однако применительно к техническим устройствам, содержащим цифровые следы правонарушения, возникает вопрос о правомерности преодоления технических средств защиты информации, поскольку действующие нормы прямо этого не предусматривают. Фактически единственным предусмотренным законом механизмом получения доступа к защищенной информации остаются негласные следственные действия, предусмотренные статьей 245 УПК РК, в частности, негласное снятие информации с компьютеров, серверов и иных устройств, предназначенных для сбора, обработки, накопления и хранения информации. Вместе с тем цели негласных следственных действий существенно отличаются от целей обыска.

Таким образом, развитие цифровых следов и специфика работы с электронными устройствами требуют не только участия специалиста при изъятии информации, но и формирования более четкого нормативного регулирования порядка доступа к защищенным техническим системам в ходе обыска.

Отсутствие регулирования не только осложняет работу с цифровыми доказательствами, но и создает риски злоупотреблений и нарушений прав участников процесса [6].

В этой связи представляется целесообразным нормативно закрепить возможность преодоления технических средств защиты информации при проведении цифрового обыска при обязательном соблюдении процессуальных гарантий и судебного контроля.

В качестве наглядного примера можно привести уголовное дело К. Бишимбаева, в рамках которого возник вопрос о предоставлении суду пароля от мобильного телефона подсудимого. Первоначально он отказался предоставить пароль, однако впоследствии пароль был сообщен адвокату, что позволило исследовать содержимое телефона в судебном заседании. Этот случай демонстрирует практическую проблему получения доступа к цифровым данным, защищенным паролем⁴.

Проблема правового регулирования доступа к защищенным цифровым данным не

³ О внесении изменений в статьи 76.1 и 145.1 Уголовного кодекса Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 27 дек. 2018 г. № 533-ФЗ [Электронный ресурс]. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_314650/b004fed0b70d0f223e4a81f8ad6cd92af90a7e3b/#dst100039.

⁴ Прокурор Айжан Аймаганова о критической ошибке Куандыка Бишимбаева с паролем телефона / [Электронный ресурс]. – Режим доступа: <https://golbis.com/on-dal-nam-parol-ot-svoego-telefona-prokuror-ajzhan-ajmaganova-nazvala-fatalnuyu-oshibku-kuandyka-bishimbaeva/>.



является специфичной для Казахстана. Аналогичные вопросы рассматриваются и в правовых системах государств с развитой цифровой инфраструктурой, в частности в США и Республике Корея.

Например, по мнению Ли Сынджу, в Южной Корее не существует законного способа заставить человека, в отношении которого был проведен обыск, раскрыть пароль к своему мобильному телефону. Ранее был внесен законопроект, предусматривающий обязательства по сотрудничеству для лица, задержанного во время обыска мобильного телефона. Хотя этот вопрос остается спорным, на мой взгляд, такое законодательство не следует признавать неконституционным, в связи с чем его следует тщательно рассмотреть. В то же время конкретного правового принципа, касающегося принудительной разблокировки мобильного телефона с использованием биометрических данных, не существует. На практике были случаи, когда в ордерах на обыск в перечне «предметов, подлежащих изъятию», содержалось положение о «биометрической информации, такой как отпечатки пальцев, сканирование радужной оболочки глаза и Face ID, с целью разблокировки мобильных телефонов», однако законность этого метода оспаривается [7].

В американской судебной практике сохраняются различные подходы к вопросу о допустимости принудительной биометрической разблокировки мобильных устройств. Так, в 2024 году Девятый окружной апелляционный суд США в деле признал допустимым обыск мобильного телефона, разблокированного с использованием отпечатка пальца обвиняемого. Суд указал, что принудительное использование биометрического идентификатора не является свидетельским (testimonial) действием, поскольку не требует от лица раскрытия сведений, содержащихся в его сознании. В связи с этим Пятая поправка США о запрете самообвинения к такому действию не применялась⁵.

Вместе с тем правовое регулирование преодоления технических средств защиты информации должно учитывать принцип неприкосновенности частной жизни. Получение доступа к мобильному устройству может открыть значительный объем сведений о личной жизни лица. Поэтому возможность технического доступа не должна рассматриваться как основание для неограниченного исследования всего содержимого устройства.

Особое значение в данном случае приобретает принудительное использование биометрического идентификатора – отпечатка пальца, Face ID или иных биометрических данных – для преодоления технической защиты устройства. Такая мера затрагивает одновременно вопросы допустимости доказательств, права на неприкосновенность частной жизни. В связи с этим ее применение должно осуществляться исключительно в пределах конкретного процессуального решения и с соблюдением установленных законом целей и границ обыска.

Ключевую роль в обеспечении указанных гарантий должен играть суд как основной субъект процессуального контроля. Судебное разрешение должно определять не только возможность доступа к техническому устройству, но и пределы такого доступа, категорию подлежащих получению данных, способы их извлечения и последующего использования. Это позволит обеспечить баланс между необходимостью получения цифровых доказательств и защитой права лица на неприкосновенность частной жизни.

В связи с изложенным преодоление технических средств защиты информации может осуществляться не только посредством технической расшифровки данных, но и путем принудительного применения биометрического идентификатора для получения доступа к защищенному техническому устройству.

В этой связи представляется целесообразным закрепить соответствующее понятие в

⁵ United States v. Payne, 99 F.4th 495 (9th Cir. 2024) / [Электронный ресурс]. – Режим доступа: https://law.justia.com/cases/federal/appellate-courts/ca9/22-50262/22-50262-2024-04-17.html?utm_source=chatgpt.com.



пункте 47-1 статьи 7 УПК РК, определив преодоление технических средств защиты как законный способ принудительного получения доступа к защищенному техническому устройству или содержащейся в нем информации посредством расшифровки, устранения технических ограничений доступа либо применения биометрического идентификатора в порядке, установленном УПК.

Представляется целесообразным закрепить указанное понятие, а соответствующее полномочие по преодолению технических средств защиты информации предусмотреть в части 9 статьи 254 УПК РК. Такое дополнение позволит устранить существующую неопределенность при проведении обыска цифровых устройств и обеспечить единообразное применение данного механизма на практике.

Заключение. Проведенный анализ показал, что действующее регулирование, закрепленное в УПК РК, в полной мере не учитывает специфику цифровых данных как объекта доказывания и требует определенной модернизации.

Наиболее существенные проблемы выявляются в рамках института осмотра, который ориентирован на исследование материальных объектов и их внешних признаков. В условиях работы с цифровыми данными для обеспечения принципов законности, достоверности и неизменности доказательств представляется необходимым нормативное закрепление дополнительных гарантий их сохранности, в том числе использование специальных носителей информации, обеспечивающих фиксацию данных в неизменном виде после их извлечения.

В части обыска и выемки следует отметить, что их действующая конструкция в целом сохраняет свою применимость и не требует создания самостоятельного института цифрового обыска. Вместе с тем возникает необходимость уточнения отдельных процессуальных аспектов, связанных с получением цифровых данных, включая допустимость копирования информации и порядок работы с электронными устройствами.

Отдельного внимания заслуживает вопрос правомерности преодоления технических средств защиты информации. В целях устранения правовой неопределенности представляется целесообразным дополнить часть 9 статьи 254 УПК РК положением, предусматривающим возможность вскрытия технических устройств в случаях отказа владельца добровольно предоставить к ним доступ. В связи с этим часть 9 статьи 254 УПК РК предлагается изложить в следующей редакции:

«При производстве обыска могут вскрываться запертые помещения и хранилища, а также технические устройства, если владелец отказывается добровольно предоставить к ним доступ. При этом не должны допускаться не вызываемые необходимостью повреждения запоров дверей и других предметов».

Таким образом, совершенствование уголовно-процессуального законодательства должно осуществляться не путем радикального изменения существующих институтов, а посредством их адаптации к условиям цифровой среды с учетом особенностей электронных данных как самостоятельного объекта доказывания.

Список использованной литературы:

1. Абилезов, Е.Т. Криминология: окулык / Е.Т. Абилезов, и др. – Алматы: ҚР ИІМ М. Есболатов атындағы Алматы академиясының ҒЗЖРБЖҰБ, 2022. – 181 б.
2. Шарипова, А.Р. Новые источники уголовно-процессуальных и иных судебных доказательств в цифровой реальности / А.Р. Шарипова // Вестник Санкт-Петербургского университета. – 2023. – № 12 (14). – С. 73-89.
3. Petrosyan, L. Digital search as a new investigative action according to the new criminal procedure code of the Republic of Armenia / L. Petrosyan // State and Law. – 2022. – № 3 (94). – Pp. 158-169.
4. Бондарева, Г.В. Некоторые вопросы производства обыска и выемки электронных носителей информации / Г.В. Бондарева // Юрист-Правовед. – 2021. – № 4 (99). – С. 185-188.



5. Angel, O.E.M. Digital Evidence as a Means of Proof in Criminal Proceedings / O.E.M. Angel, et al. // Revista de Gestao Social e Ambiental. – 2024. – № 18 (4). – e04585.
6. Slipeniuk, T. Problematic Issues of Using Electronic Evidence in Criminal Proceedings (SDG's) [Электронный ресурс]. / T. Slipeniuk, et al. // Journal of Lifestyle and SDGs Review. – 2024. – Vol. 4 No. 1. – Режим доступа: <https://sdgsreview.org/LifestyleJournal/article/view/1867>.
7. 이승주. 휴대전화 압수수색 시 비밀번호 잠금 강제 해제 문제 / 이승주 // 형사소송 이론과 실무. – 2025. – № 17 (4). – Pp. 37-86.

References:

1. Abilezov, E.T. Kriminologija: oқулық / E.T. Abilezov, i dr. – Almaty: ҚР ИИМ М. Esbolatov atyndary Almaty akademijasynyn FZzhRBZhYB, 2022. – 181 b.
2. Sharipova, A.R. Novye istochniki ugovolno-processual'nyh i inyh sudebnyh dokazatel'stv v cifrovoj real'nosti / A.R. Sharipova // Vestnik Sankt-Peterburgskogo universiteta. – 2023. – № 12 (14). – S. 73-89.
3. Petrosyan, L. Digital search as a new investigative action according to the new criminal procedure code of the Republic of Armenia / L. Petrosyan // State and Law. – 2022. – № 3 (94). – Pp. 158-169.
4. Bondareva, G.V. Nekotorye voprosy proizvodstva obyska i vyemki jelektronnyh nositelej informacii / G.V. Bondareva // Jurist-Pravoved#. – 2021. – № 4 (99). – S. 185-188.
5. Angel O.E.M. Digital Evidence as a Means of Proof in Criminal Proceedings / O.E.M. Angel, et al. // Revista de Gestao Social e Ambiental. – 2024. – № 18 (4). – e04585.
6. Slipeniuk, T. Problematic Issues of Using Electronic Evidence in Criminal Proceedings (SDG's) [Elektronnyj resurs]. / T. Slipeniuk, et al. // Journal of Lifestyle and SDGs Review. – 2024. – Vol. 4 No. 1. – Rezhim dostupa: <https://sdgsreview.org/LifestyleJournal/article/view/1867>.
7. 이승주. 휴대전화 압수수색 시 비밀번호 잠금 강제 해제 문제 / 이승주 // 형사소송 이론과 실무. – 2025. – № 17 (4). – Pp. 37-86.

АВТОРЛАР ТУРАЛЫ МӘЛІМЕТТЕР / СВЕДЕНИЯ ОБ АВТОРАХ / INFORMATION ABOUT AUTHORS

Баян Аблаевна Жилхайдарова – Қазақстан Республикасы Бас прокуратурасының жанындағы Құқық қорғау органдары академиясының докторанты, e-mail: oboyashka7@gmail.com, orcid.org/0009-0007-5394-2316.

Жилхайдарова Баян Аблаевна – докторант Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан, e-mail: oboyashka7@gmail.com, orcid.org/0009-0007-5394-2316.

Zhilkhaidarova Bayan Ablayevna – Doctoral Student of the Law Enforcement Academy under the Prosecutor General's Office of the Republic of Kazakhstan, e-mail: oboyashka7@gmail.com, orcid.org/0009-0007-5394-2316.