



УДК 343.14
МРНТИ 10.79.35

Б.Р. Рыскулбекова¹, Б.П. Жаксымбетов²

¹Университет Туран, г. Алматы, Республика Казахстан

²Казахский национальный аграрный исследовательский университет, г. Алматы, Республика Казахстан

ЦИФРОВЫЕ ДОКАЗАТЕЛЬСТВА В УГОЛОВНОМ ПРОЦЕССЕ: КАЗАХСТАН И ЕВРОПЕЙСКИЙ СОЮЗ

Аннотация. В статье рассматриваются особенности правового регулирования цифровых доказательств в уголовном процессе Республики Казахстан и Европейского союза. Актуальность темы обусловлена ростом цифровой преступности и расширением использования электронных данных в расследовании уголовных правонарушений. Анализируется правовая природа цифровых доказательств, их место в системе доказывания, а также особенности сбора, фиксации и оценки в уголовном судопроизводстве. Особое внимание уделяется сравнению подходов Казахстана, основанных на общих нормах Уголовно-процессуального кодекса Республики Казахстан и гибкости правоприменения, и Европейского союза, где доминирует детальная регламентация и стандартизация процедур. Выявляются проблемы правовой неопределенности, технической обеспеченности и трансграничного доступа к данным. В результате исследования формулируются выводы о необходимости совершенствования национального законодательства с учетом международного опыта, повышения процессуальных гарантий и внедрения единых стандартов работы с цифровыми доказательствами.

Ключевые слова: цифровые доказательства; Уголовно-процессуальный кодекс; анализ; Европейская модель; право; процесс; регулирование.

Б.Р. Рыскулбекова¹, Б.П. Жаксымбетов²

¹Тұран университеті, Алматы қ., Қазақстан Республикасы

²Қазақ ұлттық аграрлық зерттеу университеті, Алматы қ., Қазақстан Республикасы

ҚЫЛМЫСТЫҚ ПРОЦЕСТЕГІ ЦИФРЛЫҚ ДӘЛЕЛДЕМЕЛЕР: КАЗАҚСТАН ЖӘНЕ ЕУРОПАЛЫҚ ОДАҚ

Аннотация. Мақалада Қазақстан Республикасы мен Еуропалық Одақтағы қылмыстық процесте цифрлық дәлелдемелерді құқықтық реттеудің ерекшеліктері қарастырылады. Тақырыптың өзектілігі киберқылмыстылық деңгейінің артуымен және қылмыстық құқық бұзушылықтарды тергеу барысында электрондық деректерді кеңінен қолданумен байланысты. Цифрлық дәлелдемелердің құқықтық табиғаты, олардың дәлелдеу жүйесіндегі орны, сондай-ақ қылмыстық сот ісін жүргізу барысында жинау, тіркеу және бағалау ерекшеліктері талданады. Қазақстанның ҚПК-нің жалпы нормаларына және қолдану тәжірибесіндегі икемділікке негізделген тәсілі Еуропалық одақтағы егжей-тегжейлі құқықтық реттеу мен стандарттау жүйесімен салыстырылады. Құқықтық белгісіздікке, техникалық қамтамасыз ету деңгейіне және трансшекаралық деректерге қол жеткізуге байланысты мәселелер айқындалады. Зерттеу нәтижесінде ұлттық заңнаманы жетілдіру, процестік кепілдіктерді күшейту және бірыңғай стандарттарды енгізу қажеттілігі туралы қорытындылар жасалады.

Түйінді сөздер: цифрлық дәлелдемелер; Қазақстан Республикасының Қылмыстық-процестік кодексі; Қазақстан Республикасы; Еуропалық Одақ моделі; құқық; процесс; реттеу.

B.R. Ryskulbekova¹, B.P. Zhaksymbetov²

¹Turan University, Almaty, the Republic of Kazakhstan

²Kazakh National Agrarian Research University, Almaty, the Republic of Kazakhstan

DIGITAL EVIDENCE IN CRIMINAL PROCEEDINGS: KAZAKHSTAN AND THE EUROPEAN UNION

Abstract. The article examines the features of the legal regulation of digital evidence in criminal proceedings in the Republic of Kazakhstan and the European Union. The relevance of the topic is driven by the growing level of cybercrime and the increasing use of electronic data in criminal investigations. The legal nature of digital evidence, its role in the system of



proof, as well as the procedures for collection, fixation, and evaluation in criminal proceedings are analyzed. The study compares Kazakhstan's approach, based on general provisions of the Criminal Procedure Code and flexible law enforcement practice, with the European Union's model characterized by detailed regulation and standardization. Issues of legal uncertainty, technical capacity, and cross-border access to data are identified. The study concludes with recommendations on improving national legislation, strengthening procedural safeguards, and introducing unified standards for handling digital evidence.

Keywords: digital evidence; Criminal Procedure Code; analysis; European model; law; procedure; regulation.

DOI: 10.52425/25187252_2026_40_125

Введение. В условиях глобальной цифровизации общественных отношений происходит качественная трансформация не только форм и способов совершения преступлений, но и механизмов их выявления, расследования и доказывания. Информационно-коммуникационные технологии становятся неотъемлемой частью повседневной жизни, что закономерно отражается и на криминальной сфере: значительная часть противоправных деяний сегодня осуществляется с использованием цифровых инструментов, а их следы фиксируются в виде электронных данных. В результате цифровые доказательства постепенно занимают центральное место в системе уголовного судопроизводства, выступая важнейшим источником установления фактических обстоятельств дела.

Вместе с тем стремительное развитие технологий существенно опережает формирование адекватных правовых механизмов их регулирования. Данная проблема носит универсальный характер и наблюдается в большинстве правовых систем мира. Законодательство нередко оказывается не готовым к оперативному реагированию на появление новых форм цифровой информации, что приводит к фрагментарности регулирования и отсутствию единых подходов к определению правовой природы цифровых доказательств. В результате правоприменительная практика вынуждена адаптировать традиционные категории доказательственного права к новым цифровым реалиям, что не всегда обеспечивает необходимый уровень правовой определенности [1].

Особую сложность представляет специфика самих цифровых доказательств. В отличие от традиционных материальных объектов, они не обладают устойчивой физической формой, могут легко изменяться, копироваться или уничтожаться без видимых следов. Это требует применения специальных технических средств и процедур для их обнаружения, фиксации и исследования. Одновременно возрастает значение вопросов обеспечения их подлинности, целостности и достоверности, поскольку любые нарушения на этапе получения или обработки данных могут повлечь признание таких доказательств недопустимыми.

Дополнительные вызовы связаны с необходимостью соблюдения фундаментальных прав личности. Использование цифровых доказательств неизбежно затрагивает сферу частной жизни, включая доступ к переписке, персональным данным и иной конфиденциальной информации. В этой связи перед государствами стоит задача поиска баланса между эффективностью уголовного преследования и обеспечением правовых гарантий участников процесса, что приобретает особую актуальность в условиях расширения возможностей цифрового контроля.

Существенное значение имеет и трансграничный характер цифровых данных. Информация, представляющая интерес для расследования, может храниться на серверах, расположенных в других государствах, либо передаваться через международные сети, что усложняет ее получение и использование в национальном уголовном процессе. Отсутствие унифицированных международных механизмов взаимодействия в данной сфере создает дополнительные правовые и организационные барьеры.

На этом фоне особый интерес представляет опыт зарубежных правовых систем, в частности государств Европейского союза (далее – ЕС), где сформированы более комплексные



подходы к регулированию цифровых доказательств. Развитие концепции электронных доказательств и внедрение единых стандартов работы с цифровыми данными позволяют обеспечить более высокий уровень правовой определенности и доверия к результатам их использования в уголовном процессе.

Таким образом, проблема правового регулирования цифровых доказательств находится на стыке технологического прогресса и правового развития и требует комплексного научного осмысления. Ее актуальность обусловлена необходимостью адаптации уголовно-процессуального законодательства к новым цифровым реалиям, обеспечения надежности доказательственной базы и соблюдения прав и свобод человека в условиях цифровой трансформации общества.

Материалы и методы. В качестве нормативной базы исследования использованы положения уголовно-процессуального законодательства Республики Казахстан (далее – РК), прежде всего нормы Уголовно-процессуального кодекса РК (далее – УПК РК), регулирующего доказательства, их собирание и оценку, а также следственные действия, применяемые при работе с электронными носителями информации. Дополнительно рассмотрены акты законодательства о защите информации и персональных данных, имеющие значение для допустимости цифровых доказательств.

Также проанализированы нормативные акты Европейского союза, включая Общие правила защиты данных (General Data Protection Regulation), а также документы и инициативы ЕС в сфере электронных доказательств (e-evidence), определяющие подходы к их сбору и трансграничному использованию. Эмпирическую основу составили научные публикации и материалы правоприменительной практики по вопросам цифровых доказательств.

Методологическую основу исследования составляют сравнительно-правовой и формально-юридический методы, дополненные приемами анализа и обобщения, что позволило выявить особенности регулирования цифровых доказательств в Казахстане и ЕС.

Результаты, обсуждение. В уголовном процессе РК цифровые доказательства не выделены в самостоятельную категорию на уровне закона, однако их правовой статус достаточно четко прослеживается через общие положения доказательственного права, закрепленные в УПК РК. В частности, статья 111 УПК РК¹ определяет доказательства как законно полученные фактические данные, на основе которых органы уголовного преследования и суд устанавливают обстоятельства дела. Именно в рамках этой широкой конструкции на практике и функционируют цифровые доказательства: переписка, файлы, записи камер видеонаблюдения, данные из информационных систем рассматриваются как «иные документы» или результаты процессуальных действий [2, 163 стр.].

Ключевым моментом является не столько форма доказательства, сколько способ его получения и процессуального закрепления. Это прямо вытекает из статьи 125 УПК РК², согласно которой доказательство признается допустимым только при условии, что оно получено в порядке, установленном законом. Для цифровых данных это требование приобретает особую значимость: любая ошибка при извлечении информации – от неправильного копирования до отсутствия фиксации действий следователя – может поставить под сомнение ее достоверность. Более того, та же норма требует оценки доказательств по критериям относимости, допустимости и достоверности в совокупности, что усложняет работу с цифровыми следами, которые нередко носят фрагментарный характер [3, 130 стр.].

Сбор и закрепление цифровых доказательств в Казахстане осуществляется в рамках общих

¹Уголовно-процессуальный кодекс Республики Казахстан: от 4 июля 2014 г. № 231-V ЗРК [Электронный ресурс] – Режим доступа: <https://adilet.zan.kz/rus/docs/K1400000231> (дата обращения: 25.04.2026).

² Там же.



процессуальных механизмов. Согласно статье 122 УПК РК³, собирание доказательств включает их обнаружение, закрепление и изъятие. На практике это реализуется через традиционные следственные действия – осмотр, выемку, обыск, – которые адаптируются к цифровой среде. Однако именно здесь возникает одна из ключевых проблем: закон описывает процедуру в общем виде, не учитывая технологическую специфику электронных данных. В результате многое зависит не от нормы закона, а от навыков конкретного специалиста и используемых технических средств.

Еще одна особенность казахстанской модели заключается в том, что цифровые доказательства фактически «встраиваются» в уже существующую систему доказательств без создания отдельного института. Это обеспечивает гибкость, но одновременно порождает неопределенность. Например, электронная переписка может рассматриваться и как документ, и как результат осмотра, и как приложение к протоколу следственного действия. Такая вариативность, с одной стороны, удобна для следствия, но с другой – создает риски для стороны защиты, поскольку критерии допустимости не всегда применяются единообразно [4].

Серьезные трудности возникают и при работе с данными, находящимися за пределами Казахстана. УПК РК не содержит специальных норм, посвященных цифровым доказательствам трансграничного характера, и в таких случаях применяются общие механизмы международной правовой помощи. Однако они часто не соответствуют скорости оборота цифровой информации, что снижает эффективность их использования в уголовном процессе.

В отличие от Казахстана, в Европейском союзе подход к цифровым доказательствам носит более системный характер. Существенную роль здесь играет (Общие правила защиты данных) General Data Protection Regulation⁴, который устанавливает строгие правила обработки персональных данных, включая требования законности, прозрачности и минимизации данных. Эти принципы напрямую влияют на допустимость цифровых доказательств, поскольку любые нарушения при получении информации могут привести к признанию ее недопустимой [5].

Кроме того, в ЕС развивается специальное регулирование электронных доказательств (e-evidence)⁵, включая, например, механизмы европейских ордеров на предоставление и сохранение электронных данных. Эти инструменты направлены на упрощение доступа правоохранительных органов к информации, находящейся в других государствах-членах, и существенно ускоряют процесс ее получения. В отличие от классических процедур международной правовой помощи, такие механизмы учитывают специфику цифровой среды и позволяют работать с доказательствами в режиме, приближенном к реальному времени [6].

На формирование современных подходов к работе с цифровыми доказательствами заметное влияние оказала Будапештская конвенция о компьютерных преступлениях 2001 года. Хотя основной целью документа является противодействие киберпреступности, его положения затрагивают и вопросы получения, сохранения и передачи электронных данных, имеющих доказательственное значение. Конвенция стала одной из первых международных основ для развития сотрудничества государств при расследовании преступлений в цифровой среде и во многом предопределила дальнейшее развитие европейской концепции электронных доказательств⁶.

³ Уголовно-процессуальный кодекс Республики Казахстан: от 4 июля 2014 года № 231-V ЗРК [Электронный ресурс] – Режим доступа: <https://adilet.zan.kz/rus/docs/K1400000231> (дата обращения: 25.04.2026).

⁴ General Data Protection Regulation (GDPR) [Электронный ресурс] – Режим доступа: [https://gdpr-info.eu/#:~:text=The%20General%20Data%20Protection%20Regulation%20\(GDPR\)%20is,subject%20*%20**Chapter%204**%20Controller%20and%20processor](https://gdpr-info.eu/#:~:text=The%20General%20Data%20Protection%20Regulation%20(GDPR)%20is,subject%20*%20**Chapter%204**%20Controller%20and%20processor) (дата обращения: 25.04.2026).

⁵ E-evidence – cross-border access to electronic evidence [Электронный ресурс] – Режим доступа: https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en (дата обращения: 25.04.2026).

⁶ Convention on cybercrime / Budapest, 23.XI.2001 [Электронный ресурс] – Режим доступа: <https://www.europarl.europa.eu/cmsdata/179163/20090225ATT50418EN.pdf> (дата обращения: 25.04.2026).



Развитие цифровых технологий и трансграничный характер электронных данных обусловили необходимость создания специальных механизмов доступа к информации, находящейся за пределами национальной юрисдикции. В государствах Европейского союза существенным шагом в этом направлении стало принятие в 2023 году пакета нормативных актов в сфере электронных доказательств (e-Evidence Package), включающего положения о Европейском приказе на предоставление электронных доказательств (European Production Order) и Европейском приказе на сохранение электронных доказательств (European Preservation Order)⁷. Новые механизмы позволяют компетентным органам государств-членов напрямую обращаться к поставщикам цифровых услуг для получения либо сохранения необходимых данных, не прибегая к длительным процедурам международной правовой помощи. Такой подход направлен на повышение эффективности расследования преступлений, совершаемых в цифровой среде, где оперативность получения информации зачастую имеет решающее значение.

Одновременно европейское законодательство предусматривает комплекс процессуальных гарантий, направленных на защиту основных прав и свобод личности. Получение электронных данных должно соответствовать требованиям необходимости и соразмерности вмешательства, а обработка информации осуществляется с учетом стандартов защиты персональных данных, закрепленных в праве Европейского союза. В результате в ЕС сформирована достаточно целостная модель обращения с цифровыми доказательствами, сочетающая эффективность расследования с механизмами судебного и правового контроля.

Для Казахстана данный опыт представляет практический интерес в контексте совершенствования процедур получения цифровых доказательств, находящихся на зарубежных серверах или в распоряжении иностранных поставщиков цифровых услуг. В условиях роста трансграничной преступности вопросы международного сотрудничества и оперативного доступа к электронным данным постепенно приобретают такое же значение, как и традиционные механизмы сбора доказательств в рамках национальной юрисдикции.

Характерной чертой европейского подхода является также высокая степень стандартизации. В большинстве стран ЕС разработаны детальные методики цифровой криминалистики, предусматривающие обязательную фиксацию всех этапов работы с данными, использование сертифицированного программного обеспечения и строгий контроль за сохранением целостности информации. Это формирует устойчивую практику, при которой цифровые доказательства воспринимаются судом как надежный источник информации [7].

Таким образом, проведенный анализ показывает, что казахстанская и европейская модели регулирования цифровых доказательств формируются на основе различных правовых подходов и по-разному решают проблему адаптации уголовного процесса к цифровой среде. Казахстанская система в значительной степени опирается на общие положения УПК РК, регулирующие доказательства и следственные действия, что позволяет включать новые виды цифровой информации в существующую процессуальную конструкцию без необходимости детальной нормативной перестройки. Такой подход обеспечивает гибкость и адаптивность правового регулирования, позволяя правоприменителю реагировать на быстро меняющиеся технологические условия. Вместе с тем он неизбежно приводит к тому, что значительная часть вопросов решается на уровне практики, а единые стандарты работы с цифровыми доказательствами формируются постепенно и не всегда являются унифицированными.

Европейская модель, напротив, развивается в направлении детальной правовой регламентации и технологической стандартизации. Существенную роль в этом играют Общие

⁷ 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 [Электронный ресурс] – Режим доступа: <https://eur-lex.europa.eu/eli/reg/2023/1543/oj/eng> (дата обращения: 25.04.2026).



правила защиты данных (General Data Protection Regulation)⁸, закрепляющие строгие принципы обработки данных, включая законность, прозрачность и ограничение целей использования информации. В совокупности с развитием механизмов электронных доказательств (e-evidence)⁹ это формирует достаточно жестко структурированную систему, в которой детально определены требования к сбору, фиксации, хранению и передаче цифровых данных. Такой уровень регламентации способствует единообразию практики и снижает риск произвольного толкования норм [8, 15 стр.].

Различие подходов напрямую влияет на уровень правовой определенности и предсказуемости. В Европейском союзе более высокая степень стандартизации обеспечивает устойчивость правоприменительной практики, усиливает гарантии защиты прав участников процесса и повышает доверие к цифровым доказательствам как к источнику информации [9]. В Казахстане, напротив, сохраняется определенная зависимость качества правоприменения от технической оснащенности органов расследования и профессионального уровня специалистов, что может приводить к неоднородности практики и различиям в оценке одних и тех же категорий цифровых данных.

Вместе с тем гибкость казахстанской модели также имеет свои преимущества, поскольку позволяет быстрее адаптировать уголовный процесс к новым технологическим реалиям без ожидания масштабных законодательных реформ. Европейская же система, несмотря на высокую степень защищенности и структурированности, требует значительных институциональных и технических ресурсов для поддержания установленного уровня регламентации.

Заключение. Проведенное исследование показало, что дальнейшее развитие института цифровых доказательств в уголовном процессе РК требует не только совершенствования правоприменительной практики, но и последовательной модернизации уголовно-процессуального законодательства. Анализ опыта Европейского союза позволяет сделать вывод о том, что эффективность использования цифровых доказательств напрямую зависит от уровня нормативной определенности, технологической стандартизации и наличия специальных механизмов международного сотрудничества.

В этой связи представляется целесообразным внести ряд первоочередных изменений в Уголовно-процессуальный кодекс РК. Прежде всего требует нормативного закрепления понятие цифровых доказательств как самостоятельной категории доказательственной информации с определением их основных признаков и видов. Одновременно представляется необходимым установить специальные процессуальные требования к обнаружению, изъятию, копированию, хранению и исследованию цифровых данных, включая обязательную фиксацию всех действий с электронными носителями и обеспечение непрерывности цепочки хранения доказательств (chain of custody). Такой подход позволит снизить риск утраты или изменения информации и повысить уровень доверия к результатам цифровой экспертизы.

С учетом европейского опыта отдельного нормативного регулирования требуют вопросы получения электронных данных, размещенных за пределами национальной юрисдикции. В перспективе целесообразно разработать специальные процедуры трансграничного доступа к цифровой информации и расширить международное сотрудничество с иностранными поставщиками цифровых услуг. Кроме того, представляется обоснованным совершенствование законодательства о защите персональных данных в части использования информации,

⁸ General Data Protection Regulation (GDPR) [Электронный ресурс] – Режим доступа: [https://gdpr.info.eu/#:~:text=The%20General%20Data%20Protection%20Regulation%20\(GDPR\)%20is,subject%20*%20**Chapter%204**%20Controller%20and%20processor](https://gdpr.info.eu/#:~:text=The%20General%20Data%20Protection%20Regulation%20(GDPR)%20is,subject%20*%20**Chapter%204**%20Controller%20and%20processor) (дата обращения: 25.04.2026).

⁹ E-evidence – cross-border access to electronic evidence [Электронный ресурс] – Режим доступа: https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en (дата обращения: 25.04.2026).



полученной в ходе уголовного судопроизводства, с установлением дополнительных гарантий судебного контроля за доступом к конфиденциальным сведениям.

Наряду с законодательными изменениями необходимы институциональные и технические меры. В частности, представляется целесообразным создание специализированных подразделений цифровой криминалистики в системе правоохранительных органов, разработка единых национальных методик работы с цифровыми доказательствами и внедрение обязательной сертификации программно-технических средств, используемых при извлечении и анализе электронных данных. Практическое значение также имеет организация системной подготовки следователей, прокуроров, судей и судебных экспертов по вопросам цифровой криминалистики и электронных доказательств.

Таким образом, дальнейшее развитие казахстанской модели регулирования цифровых доказательств должно быть связано не только с расширением возможностей использования цифровой информации в уголовном процессе, но и с укреплением процессуальных гарантий ее достоверности, допустимости и законности получения. Реализация указанных мер позволит повысить эффективность расследования преступлений в цифровой среде и одновременно обеспечить более надежную защиту прав и законных интересов участников уголовного судопроизводства.

Список использованной литературы:

1. O.S. Kerr. Searches and seizures in a digital world [Электронный ресурс] – Режим доступа: <https://www.jstor.org/stable/4093493> (дата обращения: 12.05.2026).
2. Аскарлов, А.А. Цифровая собственность как новое доказательство: концептуальные основы исследования цифровых объектов в криминалистике Казахстана / А.А. Аскарлов, Р.А. Медиев // Құқық қорғау органдары академиясының жаршысы. – 2025. – № 4 (38). – С. 160-169.
3. Tolybayeva, A. Problems of electronic criminal procedure in Kazakhstan and comparative analysis of foreign digital investigation models / A. Tolybayeva, et al. // KazNU Bulletin. The legal series. – 2025. – Vol. 116. № 4. – Pp. 125-140.
4. N. Apsimet, et al. Challenges of using digital evidence in pretrial investigations of online fraud: lessons for Kazakhstan from international practice [Электронный ресурс] – Режим доступа: <https://dialnet.unirioja.es/servlet/articulo?codigo=10679411> (дата обращения: 25.04.2026).
5. Abdullah, H.O. Digital Evidence in Criminal Proceedings: Legal Standards, Chain of Custody, and Evidentiary Reliability in the Digital Era / H.O. Abdullah, M. Maqsood, A. Nadeem // Research Journal for Social Affairs. – 2025. – № 3 (5). – Pp. 795-805.
6. Juszczak, A. The Use of Electronic Evidence in the European Area of Freedom, Security, and Justice / A. Juszczak, E. Sason // Eucriim. – 2023. – Vol. 18 (2). – Pp. 182-200.
7. Ch. Ragni. Digital evidence in international criminal proceedings and human rights challenges [Электронный ресурс] – Режим доступа: <https://ojs.srce.hr/eclic/article/view/28255/14423> (дата обращения: 25.04.2026).
8. Bhatti, N. The Use of Digital Evidence in Criminal Proceedings / N. Bhatti // American Journal of Society and Law (AJSL). – 2026. – Vol. 5. № 1. – Pp. 10-19.
9. Ch.M. Miller. A survey of prosecutors and investigators using digital evidence: a starting point [Электронный ресурс] – Режим доступа: <https://pmc.ncbi.nlm.nih.gov/articles/PMC10311201/> (дата обращения: 25.04.2026).
10. Miha, E. Electronic evidence in the criminal process / E. Miha, I. Pekmezi // Academic journal of business, management, law and social sciences. – 2024. – Vol. 10. № 2. – Pp. 124-132.

References:

1. O.S. Kerr. Searches and seizures in a digital world [Elektronnyj resurs] – Rezhim dostupa: <https://www.jstor.org/stable/4093493> (data obrashheniya: 12.05.2026).
2. Askarov, A.A. Cifrovaya sobstvennost' kak novoe dokazatel'stvo: konceptual'nye osnovy issledovaniya cifrovyyh ob#ektov v kriminalistike Kazahstana / A.A. Askarov, R.A. Mediev // Құқық қорғау органдары академиясының жаршысы. – 2025. – № 4 (38). – С. 160-169.
3. Tolybayeva, A. Problems of electronic criminal procedure in Kazakhstan and comparative analysis of foreign digital investigation models / A. Tolybayeva, et al. // KazNU Bulletin. The legal series. – 2025. – Vol. 116. № 4. – Pp. 125-140.



4. N. Apsimet, et al. Challenges of using digital evidence in pretrial investigations of online fraud: lessons for Kazakhstan from international practice [Jelektronnyj resurs] – Rezhim dostupa: <https://dialnet.unirioja.es/servlet/articulo?codigo=10679411> (data obrashhenija: 25.04.2026).
5. Abdullah, H.O. Digital Evidence in Criminal Proceedings: Legal Standards, Chain of Custody, and Evidentiary Reliability in the Digital Era / H.O. Abdullah, M. Maqsood, A. Nadeem // Research Journal for Social Affairs. – 2025. – № 3 (5). – Pp. 795-805.
6. Juszczak, A. The Use of Electronic Evidence in the European Area of Freedom, Security, and Justice / A. Juszczak, E. Sason // Eu crim. – 2023. – Vol. 18 (2). – Pp. 182-200.
7. Ch. Ragni. Digital evidence in international criminal proceedings and human rights challenges [Jelektronnyj resurs] – Rezhim dostupa: <https://ojs.srce.hr/eclic/article/view/28255/14423> (data obrashhenija: 25.04.2026).
8. Bhatti, N. The Use of Digital Evidence in Criminal Proceedings / N. Bhatti // American Journal of Society and Law (AJSL). – 2026. – Vol. 5. № 1. – Pp. 10-19.
9. Ch.M. Miller. A survey of prosecutors and investigators using digital evidence: a starting point [Jelektronnyj resurs] – Rezhim dostupa: <https://pmc.ncbi.nlm.nih.gov/articles/PMC10311201/> (data obrashhenija: 25.04.2026).
10. Miha, E. Electronic evidence in the criminal process / E. Miha, I. Pekmezi // Academic journal of business, management, law and social sciences. – 2024. – Vol. 10. № 2. – Pp. 124-132.

АВТОРЛАР ТУРАЛЫ МӘЛІМЕТТЕР / СВЕДЕНИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Балжан Рашитовна Рыскулбекова – Тұран университетінің докторанты, e-mail: nur.raya@inbox.ru.

Рыскулбекова Балжан Рашитовна – докторант Университета Туран, e-mail: nur.raya@inbox.ru.

Ryskulbekova Balzhan Rashitovna – Doctoral Student at Turan University, e-mail: nur.raya@inbox.ru.

Бакитжан Пармешович Жаксымбетов – Қазақ ұлттық аграрлық зерттеу университетінің құқық кафедрасының аға оқытушысы, заң ғылымдарының кандидаты, e-mail: zhaksymbetova.zhanara@gmail.com.

Жаксымбетов Бакитжан Пармешович – старший преподаватель кафедры права Казахского национального аграрного исследовательского университета, кандидат юридических наук, e-mail: zhaksymbetova.zhanara@gmail.com.

Zhaksymbetov Bakitzhan Parmeshovich – Senior lecturer at the Department of Law of the Kazakh National Agrarian University, Candidate of Law Sciences, e-mail: zhaksymbetova.zhanara@gmail.com.