МРНТИ 10.79.35
УДК 343.98
https://doi.org/10.51889/2959-6181.2026.84.2.009

К.Б.Молдагалиев [1], А.К.Камбаров [1]*

[1]НАО «Евразийский национальный университет имени Л.Н.Гумилева»
(e-mail: [*]mkb_010@mail.ru, kambarov_ak@enu.kz)

ЦИФРОВЫЕ СЛЕДЫ КАК ОБЪЕКТ СУДЕБНОЙ КОМПЬЮТЕРНО-ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ

Аннотация

В статье исследуются цифровые следы как значимый объект судебной компьютерно-технической экспертизы при расследовании преступлений, совершаемых в киберпространстве. Рассматриваются научные подходы к пониманию сущности цифровых следов, их характерных признаков и классификации. Авторы уделяет внимание особенностям работы с цифровой информацией, которая может выступать доказательством в суде, включая этапы ее выявления, фиксации, хранения и последующего экспертного исследования.

Особый акцент сделан на проблемах, возникающих при анализе цифровых доказательств в условиях распространения облачных сервисов, применения криптографических средств защиты информации и технологий сокрытия сетевой активности пользователей. Отмечается, что расследование киберпреступлений требует не только технической подготовки специалистов, но и соблюдения процессуальных требований, обеспечивающих достоверность и целостность цифровых данных.

По результатам исследования сделан вывод о необходимости совершенствования методологических подходов в сфере цифровой криминалистики и разработки единых научно-практических стандартов исследования цифровых следов в экспертной деятельности.

Ключевые слова: цифровые следы, судебная компьютерно-техническая экспертиза, киберпреступления, электронные доказательства, цифровая криминалистика, цифровые данные.

К.Б. Молдагалиев [1], А.Қ. Камбаров [1]
[1]КеАҚ «Л.Н. Гумилев атындағы Еуразия ұлттық университеті»

ЦИФЛЫҚ ІЗДЕР СОТ КОМПЬЮТЕРЛІК-ТЕХНИКАЛЫҚ САРАПТАМА НЫСАНЫ РЕТІНДЕ

Аңдатпа

Мақалада цифрлық іздер киберқылмыстарды тергеу барысында қолданылатын соттық компьютерлік-техникалық сараптаманың маңызды объектілерінің бірі ретінде қарастырылады. Цифрлық іздердің мәнін түсіндіруге қатысты ғылыми көзқарастар, олардың негізгі белгілері мен жіктелуі талданады. Авторлар қылмыстық іс жүргізуде дәлелдемелік маңызы бар цифрлық ақпаратты анықтау, тіркеу, сақтау және сараптамалық зерттеу ерекшеліктеріне ерекше назар аударады.

Сонымен қатар, бұлттық сервистердің кең таралуы, ақпаратты криптографиялық қорғау құралдарының қолданылуы және желідегі белсенділікті жасыру технологиялары жағдайында цифрлық дәлелдемелерді зерттеу барысында туындайтын мәселелер қарастырылады. Киберқылмыстарды тиімді тергеу мамандардың техникалық даярлығымен қатар, цифрлық деректердің тұтастығы мен сенімділігін қамтамасыз ететін процессуалдық талаптарды дұрыс сақтауға да байланысты екендігі атап өтіледі.

Зерттеу нәтижесінде цифрлық криминалистика саласындағы теориялық және әдіснамалық негіздерді жетілдіру, сондай-ақ сараптамалық тәжірибеде цифрлық іздерді зерттеудің бірыңғай ғылыми-практикалық тәсілдерін қалыптастыру қажеттілігі туралы қорытынды жасалады.

Түйін сөздер: цифрлық іздер, сот компьютерлік криминалистика, киберқылмыс, электрондық дәлелдемелер, цифрлық криминалистика, цифрлық деректер.

K.B.Moldagaliyev [1], A.K.Kambarov [1]
[1]JSC «L.N. Gumilyov Eurasian National University»

DIGITAL FOOTPRINTS AS AN OBJECT OF FORENSIC COMPUTER-TECHNICAL EXAMINATION

Abstract

The article examines digital traces as a significant object of forensic computer and technical examination in the investigation of crimes committed in cyberspace. Scientific approaches to understanding the essence of digital traces, their characteristic features, and classification are considered. The authors pay special attention to the specifics of working with digital information that may serve as evidence in criminal proceedings, including the stages of its identification, recording, storage, and subsequent forensic examination.

Particular emphasis is placed on the problems arising during the analysis of digital evidence in the context of the widespread use of cloud services, cryptographic methods of information protection, and technologies used to conceal users' network activity. It is noted that the investigation of cybercrimes requires not only technical training of specialists, but also compliance with procedural requirements that ensure the reliability and integrity of digital data.

Based on the results of the study, the authors conclude that there is a need to improve methodological approaches in the field of digital forensics and to develop unified scientific and practical standards for the examination of digital traces in expert practice.

Key words: digital footprints, forensic computer examination, cybercrime, electronic evidence, digital forensics, digital data.

Введение

Современное развитие информационного общества характеризуется тотальной цифровизацией всех сфер жизнидеятельности. Практически каждое действие пользователя в цифровой среде оставляет след, фиксируемый информационными системами. По оценкам современных исследований, более 90% преступлений имеют цифровой компонент, что радикально изменяет структуру доказательной базы уголовного процесса [1].

Киберпреступность в настоящее время является одной из наиболее быстро развивающихся форм преступной деятельности. Ее особенностями выступают высокая латентность, трансграничный характер, а также использование сложных технических и программных средств. В связи с этим особое значение приобретает судебная компьютерно-техническая экспертиза, которая выступает важным инструментом выявления, исследования и оценки цифровой информации, имеющей доказательственное значение.

Одним из ключевых объектов судебной компьютерно-технической экспертизы являются цифровые следы, возникающие в процессе функционирования информационных систем, сетевого взаимодействия пользователей и использования электронных устройств. В противоположность традиционных материальных следов преступления цифровые следы обладают специфическими свойствами: нематериальностью, высокой изменяемостью, возможностью удаленного хранения и быстрого уничтожения, а также зависимостью от программно-технической среды. Перечисленные особенности обусловливают необходимость создания научно обоснованных подходов к их обнаружению, фиксации, сохранению и исследованию.

Актуальность темы исследования определяется возрастанием роли цифровых доказательств в уголовном судопроизводстве и необходимостью совершенствования теоретических и методических основ судебной компьютерно-технической экспертизы. Практика расследования киберпреступлений свидетельствует о том, что эффективность раскрытия и доказывания противоправной деятельности во многом зависит от правильного выявления и интерпретации цифровых следов. Вместе с тем развитие технологий хранения и

передачи данных, использование облачных сервисов, средств шифрования и анонимизации существенно усложняют процесс экспертного исследования цифровой информации.

Несмотря на наличие научных работ, посвященных вопросам цифровой криминалистики и компьютерно-технической экспертизы, в современной юридической науке сохраняются дискуссионные вопросы, связанные с определением сущности цифровых следов, их классификацией, процессуальным статусом и методикой экспертного исследования. Недостаточная разработанность отдельных теоретических положений, а также отсутствие единых методических подходов предопределяют необходимость дальнейшего комплексного исследования данной проблематики.

Объектом исследования являются общественные отношения, возникающие в процессе выявления, фиксации и исследования цифровых следов при расследовании киберпреступ-лений. Предмет исследования составляют теоретические положения, методические основы и практические аспекты использования цифровых следов в судебной компьютерно-технической экспертизе.

Целью статьи является исследование сущности цифровых следов как объекта судебной компьютерно-технической экспертизы, а также определение их значения в процессе расследования и раскрытия киберпреступлений. Для достижения поставленной цели предполагается решение следующих задач: анализ понятия и признаков цифровых следов; рассмотрение их классификации; выявление особенностей обнаружения и фиксации цифровой информации; исследование проблем экспертного исследования цифровых доказательств в современных условиях.

Теоретическая и практическая значимость исследования заключается в возможности использования полученных выводов при совершенствовании методики судебной компьютерно-технической экспертизы, а также в правоприменительной деятельности органов расследования и судебно-экспертных учреждений.

Материалы и методы

В ходе исследования анализировались научные публикации отечественных и зарубежных авторов в области цифровой криминалистики и судебной компьютерно-технической экспертизы.

Методологическую основу исследования составляют общенаучные и специальные методы научного познания, включая диалектический, системно-структурный, сравнительно-правовой, формально-юридический и логический методы.

Системно-структурный метод позволил определить место цифровых следов в системе объектов судебной компьютерно-технической экспертизы и выявить взаимосвязь между этапами их обнаружения, фиксации и исследования.

Сравнительно-правовой метод применялся для сопоставления отечественного и зарубежного подходов к исследованию цифровых доказательств.

Логический и аналитический методы использовались при формулировании научных выводов, классификации цифровых следов и определении особенностей их экспертного исследования.

Применение указанных методов обеспечило всестороннее и объективное исследование поставленной проблемы, а также соответствие полученных результатов целям и задачам научной работы.

Результаты и обсуждение

Новый вид преступлений обусловил возникновение «информационных следов», ранее нехарактерных для следственной практики и требующих специального криминалистического научного изучения. В.Б. Вехов рассматривает виртуальные следы как промежуточную категорию между материальными и идеальными следами [2].

Цифровые следы представляют совокупность данных, возникающих в процессе функционирования информационных систем и отражающих действия пользователя или программных процессов. Они могут быть явными (файлы, переписка, документы) и скрытыми (метаданные, журналы событий, кеш-данные [3].

Е.Р. Россинская определяет цифровой след как «...криминалистически значимую компьютерную информацию о событиях или действиях, отраженную в материальной среде, в процессе ее возникновения, обработки, хранения и передачи» [4].

Цифровые следы представляют совокупность артефактов, оставляемых пользователем и устройствами в облачных и мобильных средах [1].

Пользовательская активность в цифровой среде формирует два аспекта цифрового следа: цифровую идентичность и онлайн-самосознание. Первый аспект связан с совокупностью цифровых данных, создаваемых пользователями и информационными системами, и соответствует пассивному цифровому следу. Второй аспект отражает проявление «Я» в социальных сетях и цифровом пространстве, характеризующееся саморефлексией, самовыражением и самоконтролем, и рассматривается как активный цифровой след [5].

Согласно научным подходам, цифровые следы рассматриваются как разновидность информационных следов, фиксирующих факт взаимодействия субъекта с цифровой средой [6].

Предлагается рассматривать цифровые следы как динамическую информационную систему, включающую:

- первичные следы, а именно действия пользователя;
- вторичные следы, которые автоматически генерируются системой;
- производные следы, включающие результаты обработки и взаимодействия данных.

Такой подход позволяет учитывать не только факт наличия данных, но и их происхождение и трансформацию.

Цифровые следы как объект судебной компьютерно-технической экспертизы обладают рядом специфических криминалистических особенностей, отличающих их от традиционных материальных следов преступления. К числу наиболее значимых особенностей цифровых следов относятся нематериальный характер, высокая изменяемость, зависимость от программно-технической среды, возможность удаленного хранения и копирования, а также сложности установления первоначального источника происхождения цифровой информации [7].

Одной из ключевых особенностей цифровых следов является их нематериальный характер. В отличие от традиционных криминалистических следов, имеющих физическую форму (отпечатки пальцев, следы обуви, биологические объекты), цифровые следы существуют исключительно в виде информационных данных, представленных в электронно-кодированной форме. Они не обладают самостоятельным материальным выражением и воспринимаются только посредством технических устройств и программного обеспечения.

Нематериальная природа цифровых следов предопределяет специфику их обнаружения и фиксации. Для работы с ними требуется использование специальных программно-технических средств, позволяющих визуализировать, копировать и анализировать цифровую информацию. При этом непосредственное восприятие следов человеком невозможно без соответствующей цифровой среды.

Кроме того, цифровые следы нередко существуют сразу в нескольких одинаковых копиях, полностью совпадающих между собой. Именно этим они существенно отличаются от традиционных материальных следов. В подобных ситуациях определить первоначальный источник информации и установить, какой носитель является оригинальным, бывает достаточно сложно.

Одной из характерных особенностей цифровых следов является их изменчивость и нестабильность. Сложность заключается в том, что изменения могут происходить даже без действий со стороны пользователя. Современные операционные системы автоматически создают временные файлы, обновляют системные журналы, изменяют метаданные и перезаписывают отдельные участки памяти устройства. По этой причине цифровая информация способна быстро утрачивать свое первоначальное состояние. С точки зрения

криминалистики это значительно осложняет обеспечение сохранности и достоверности электронных доказательств.

Особую проблему представляет быстрое устаревание технологий. На практике часть цифровых следов со временем становится недоступной из-за прекращения поддержки определенных программ, устройств, хостинга или форматов хранения данных. В связи с этим исследование цифровых следов требует от специалиста не только знаний в области права и криминалистики, но и хорошей технической подготовки в сфере информационных технологий.

В отличие от обычных материальных объектов цифровые данные могут быть практически мгновенно скопированы, перемещены либо удалены. При этом созданные копии зачастую полностью совпадают с оригиналом, что затрудняет установление первоисточника информации и последовательности ее распространения.

Дополнительные трудности возникают при использовании облачных сервисов, распределенных систем хранения данных и виртуальных серверов. В таких условиях физический носитель информации фактически может находиться вне доступа пользователя, а работа с данными осуществляется дистанционно через сеть Интернет.

Цифровые следы могут выступать объектами исследования при проведении различных видов судебных экспертиз, включая фототехническую, видеотехническую, портретную, фоноскопическую, бухгалтерскую и другие. Вместе с тем цифровая форма такой информации требует применения специальных методов компьютерно-технического исследования, позволяющих корректно извлекать, обрабатывать и анализировать необходимые данные.

В научной литературе цифровые следы обычно подразделяются на несколько основных категорий: следы, содержащиеся на локальных устройствах (компьютерах, ноутбуках, смартфонах), сетевые следы (IP-адреса, журналы подключений), данные облачных сервисов, коммуникационные следы (электронная почта, мессенджеры, социальные сети), метаданные файлов, а также сведения о финансовых операциях, включая транзакции с криптовалютой. Подобная классификация позволяет более системно подходить к исследованию объектов судебной компьютерно-технической экспертизы и подбирать соответствующие методы их анализа [8].

На основе анализа современной практики предлагается расширенная классификация (табл.1):

Таблица 1

Классификация цифровых следов

№	Вид цифровых следов	Основные элементы	Криминалистическое значение
1	Локальные цифровые следы	данные на устройствах; журналы системы; временные файлы и кэш	дают возможность зафиксировать действия юзера на определённом устройстве, воссоздать последовательность событий и факт применения программ
2	Сетевые следы	IP-адреса и соединения; сетевые логи; маршрутизация трафика	применяются для определения сетевой активности, источника подключения и пути передачи данных
3	Облачные следы	данные облачных сервисов; распределённые базы данных; синхронизированные копии	позволяют обнаружить удаленное хранение данных, копии и работу с облачными системами
4	Коммуникационные следы	социальные сети; мессенджеры; электронная почта	выступают основой для анализа взаимодействий, установления контактов между субъектами и обнаружения преступных связей

5	Финансово-цифровые следы	банковские транзакции и операции	применяются для мониторинга денежных потоков, фиксации финансовых операций и потенциального узаконивания поступлений
6	IoT-следы (интернет вещей)	информация с «умных» устройств; сенсорные реестры; сведения много дома и используемых гаджетов	применяются для воссоздания действий пользователя и регистрации автоматических событий в физической среде
7	AI-генерируемые следы	сценарии взаимодействия с ИИ-системами; обращения к нейросетям; автоматизированные решения алгоритмов	дают возможность установить факт применения ИИ-сервисов, запросов и алгоритмов

Примечание: составлено авторами.

Представленная классификация цифровых следов отражает современное состояние цифровой среды и показывает, насколько изменилось понимание компьютерно-технических следов в условиях развития цифровой криминалистики. Если ранее основное внимание уделялось только данным, находящимся на компьютере или в сети, то сегодня исследование охватывает значительно более широкий круг цифровых объектов и источников информации.

Прежде всего, базовыми по-прежнему остаются локальные и сетевые следы, поскольку именно они формируют основную доказательственную базу. Локальные следы позволяют установить действия пользователя на конкретном устройстве, а сетевые помогают восстановить взаимодействие в информационной среде, определить каналы связи и зафиксировать сетевую активность.

Вместе с тем все большую роль начинают играть облачные и коммуникационные следы. Это связано с тем, что значительная часть информации сегодня хранится не на физических носителях пользователя, а в облачных сервисах, мессенджерах и социальных сетях. В подобных условиях данные могут находиться сразу на нескольких удалённых серверах, что заметно усложняет их обнаружение, изъятие и последующее экспертное исследование.

Особое значение в современной практике приобретают мобильные, IoT- и AI-генерируемые следы. Мобильные устройства позволяют фиксировать действия пользователя практически в режиме реального времени. IoT-устройства, подключенные к сети, расширяют возможности криминалистического анализа за счет получения данных с физических объектов. В свою очередь, AI-следы отражают влияние алгоритмов и систем искусственного интеллекта на формирование цифровой активности пользователей.

В связи с этим становится очевидной необходимость пересмотра традиционных подходов к судебной компьютерно-технической экспертизе и перехода к более комплексным моделям исследования цифровой информации.

Судебная компьютерно-техническая экспертиза направлена на изучение цифровых данных для установления обстоятельств, имеющих значение по делу. При этом цифровые следы выступают одним из основных объектов такого исследования.

Несмотря на активное развитие цифровой криминалистики, исследование цифровых следов до сих пор сопровождается рядом серьезных проблем. Среди них можно выделить использование технологий шифрования и VPN-сервисов, удаленное хранение информации в облачных системах, высокую скорость изменения цифровых данных, отсутствие единых международных стандартов исследования, а также сложности, связанные с установлением личности реального пользователя. Указанные обстоятельства существенно осложняют проведение судебной компьютерно-технической экспертизы и подтверждают необходимость дальнейшего совершенствования ее методологической базы [9].

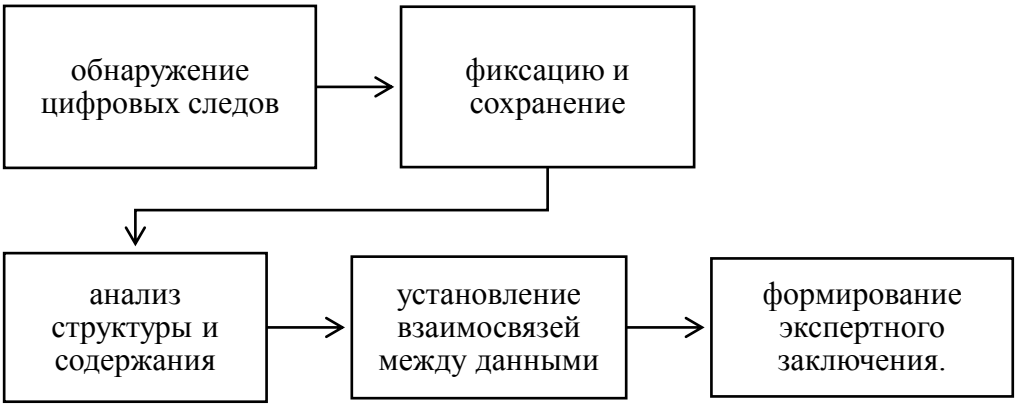

Рисунок 1. Последовательность судебной компьютерно-технической экспертизы в работе с цифровыми следами

В рамках судебной компьютерно-технической экспертизы деятельность эксперта связана с поиском, фиксацией, сохранением и дальнейшим исследованием цифровых следов, способных выступать доказательствами по делу [10]. Работа с такими данными имеет свою специфику, поскольку цифровая информация не обладает материальной формой, может быстро изменяться и напрямую зависит от технических характеристик устройства и используемого программного обеспечения.

По этой причине при обнаружении и фиксации цифровых следов специалисту необходимо учитывать особенности программно-технической среды, а также обеспечивать сохранность исходного состояния информации. На рисунке 1 представлен общий алгоритм работы с цифровыми следами.

Заключение

Таким образом, цифровые следы сегодня выступают одним из ключевых объектов судебной компьютерно-технической экспертизы при расследовании киберпреступлений, поскольку содержат значительный объем информации, способной иметь доказательственное значение.

Проведенный анализ научных подходов, особенностей классификации цифровых следов и специфики работы с электронными данными показывает, что их обнаружение, фиксация, сохранение и исследование требуют соблюдения специальных методик и обеспечения сохранности цифровой информации. Установлено, что использование современных технологий, включая облачные сервисы, средства шифрования и инструменты анонимизации, значительно осложняет процесс получения и анализа цифровых доказательств, создавая дополнительные практические и методологические сложности.

В связи с этим эффективность расследования киберпреступлений во многом зависит от уровня развития судебной компьютерно-технической экспертизы, а также от качества и правильности применяемых экспертных методик.

Вклад авторов

Молдагалиев К.Б. разработал концепцию исследования и подготовил теоретико-правовой анализ темы.

Камбаров А.К. проанализировал практические аспекты цифровых следов и участвовал в формулировании выводов.

Список использованной литературы:

1 Quick D., Choo K.-K.R. (2018). IoT Device Forensics and Data Reduction. // IEEE Access. Vol. 6, 47566-47574 pp. DOI: https://doi.org/10.1109/ACCESS.2018.2867466

2 Вехов В.Б. Преступления в сфере цифровой экономики: совершенствование расследования на основе положений электронной криминалистики // Пермский юридический альманах. Ежегодный научный журнал. 2019. №2. – С. 630-640. – URL: http://almanack.psu.ru/wp-content/uploads/2019.pdf

3 Nayerifard, T., Amintoosi, H., Bafghi, A. G., & Dehghantanha, A. (2023). Machine Learning in Digital Forensics: A Systematic Literature Review. arXiv.org. DOI: https://doi.org/10.48550/arXiv.2306.04965

4 Россинская Е.Р. Система теории цифровизации судебно-экспертной деятельности. Теория и практика судебной экспертизы. 2024. 19(3). – С. 20-32. DOI: https://doi.org/10.30764/1819-2785-2024-3-20-32

5 Jamal, N., & Zain, J. M. (2022). A review on nature, cybercrime and best practices of digital footprints. 2022 International Conference on Cyber Resilience (ICCR). DOI: https://doi.org/10.1109/iccr56254.2022.9995834

6 Цифровой след как объект судебной экспертизы: материалы Международной научно-практической конференции. – Москва: РГ-Пресс, 2020. – 272 с. ISBN 978-5-9988-0932-3

7 Apsimet, N., Alimkulov, Y., & Duisenbayeva, G. (2024). The collection of digital traces in the investigation of online crimes. // BULLETIN of L.N. Gumilyov Eurasian National University Law Series, 149(4), 170-185. https://doi.org/10.32523/2616-6844-2024-149-4-170-185

8 Klasén, L., Fock, N., & Forchheimer, R. (2024). The invisible evidence: Digital forensics as key to solving crimes in the digital age // Forensic Science International, 362, 112-133. DOI: https://doi.org/10.1016/j.forsciint.2024.112133

9 Руденкова Ю.С., Хазиев Ш.Н., Усов А.И. Искусственный интеллект и судебная компьютерно-техническая экспертиза // Теория и практика судебной экспертизы. 2024. Т. 19. №2. – С. 76-87. DOI: https://doi.org/10.30764/1819-2785-2024-2-76-87

10 Vladimirov D.M. (2024). Detection and removal of digital traces of extremist crimes // Forensics: yesterday, today, tomorrow. No. 3. 38-44 pp. URL: https://kvsz.ru/en/nauka/article/90726/view?utm

References:

1 Quick D., Choo K.-K.R. (2018). IoT Device Forensics and Data Reduction. // IEEE Access. Vol. 6, 47566-47574 pp. DOI: https://doi.org/10.1109/ACCESS.2018.2867466

2 Vehov V.B. (2019) Prestuplenija v sfere cifrovoj jekonomiki: sovershenstvovanie rassledovanija na osnove polozhenij jelektronnoj kriminalistiki (Crimes in the Digital Economy: Improving Investigations Based on the Principles of Electronic Forensics) // Permskij juridicheskij al'manah. Ezhegodnyj nauchnyj zhurnal. №2. 630-640 pp. – URL: http://almanack.psu.ru/wp-content/uploads/2019.pdf

3 Nayerifard T., Amintoosi H., Bafghi A.G., & Dehghantanha A. (2023). Machine Learning in Digital Forensics: A Systematic Literature Review // arXiv.org. DOI: https://doi.org/10.48550/arXiv.2306.04965

4 Rossinskaja E.R. (2024) The System of Forensic Activity Digitalization Theory // Theory and Practice of Forensic Science. 19(3). 20-32 pp. DOI: https://doi.org/10.30764/1819-2785-2024-3-20-32

5 Jamal, N., & Zain, J. M. (2022). A review on nature, cybercrime and best practices of digital footprints. 2022 International Conference on Cyber Resilience (ICCR). DOI: https://doi.org/10.1109/iccr56254.2022.9995834

6 Cifrovoj sled kak obekt sudebnoj jekspertizy: materialy Mezhdunarodnoj nauchno-prakticheskoj konferencii (Digital Trace as an Object of Forensic Examination: Proceedings of the International Scientific and Practical Conference). – Moskva: RG-Press, 2020. 272 p. ISBN 978-5-9988-0932-3

7 Apsimet, N., Alimkulov, Y., & Duisenbayeva, G. (2024). The collection of digital traces in the investigation of online crimes. // BULLETIN of L.N. Gumilyov Eurasian National University Law Series, 149(4), 170-185. https://doi.org/10.32523/2616-6844-2024-149-4-170-185

8 Klasén, L., Fock, N., & Forchheimer, R. (2024). The invisible evidence: Digital forensics as key to solving crimes in the digital age // Forensic Science International, 362, 112-133. DOI: https://doi.org/10.1016/j.forsciint.2024.112133

9 Rudenkova Ju.S., Haziev Sh.N., Usov A.I. (2024). Iskusstvennyj intellekt i sudebnaja komp'juterno-tehnicheskaja jekspertiza (Artificial Intelligence and Forensic Computer-Technical Examination) // Theory and Practice of Forensic Science. Vol. 19. №2. 76-87 pp. DOI: https://doi.org/10.30764/1819-2785-2024-2-76-87

10 Vladimirov D.M. (2024). Detection and removal of digital traces of extremist crimes // Forensics: yesterday, today, tomorrow. No.3. 38-44 pp. – URL: https://kvsz.ru/en/nauka/article/90726/view?utm

МРНТИ 10.79.01
УДК 343.1 https://doi.org/10.51889/2959-6181.2026.84.2.010

*Б.Х. Толеубекова[1]**

[1]Казахский национальный педагогический университет имени Абая
*(e-mail: * madina_khv@mail.ru)*

ТРАНСФОРМАЦИОННАЯ МОДЕЛЬ ПРИНЦИПОВ УГОЛОВНОГО СУДОПРОИЗВОДСТВА В КОНТЕКСТЕ НОВОЙ КОНСТИТУЦИИ РЕСПУБЛИКИ КАЗАХСТАН

Аннотация

Принятая в результате референдума 15 марта 2026 года новая Конституция Республики Казахстан изменила законодательные представления о системе и структуре судопроизводственных принципов. Признание принципов судопроизводства в качестве фундаментальных основ процессуальных отраслей в национальной системе права являлось и остается ключевым фактором в деле построения регулятивных механизмов отправления правосудия. Первичность принципов и их всеобъемлющее влияние на всю систему и структуру отраслевого права неоспоримо и является стандартизирующим критерием в правовых системах мира. Это означает, что изменения в конституционных подходах, относящиеся к системе правовых принципов, являются основанием для дальнейшего развития теоретико-методологических исследований по вопросам нового осмысления как самой системы принципов судопроизводства, так и сопровождающих их гарантий. В настоящих условиях сформировался социальный запрос на доказательное обоснование нового понимания сущности правовых принципов в целом, судопроизводственных – в частности. Новая Конституция вызвала к жизни новые потребности, обусловленные необходимостью приведения в соответствие с нею все отрасли права. Не исключается возможность разработки и принятия новых законов, включая Уголовно-процессуальный кодекс РК.

Ключевые слова: конституция, методология права, уголовный процесс, принципы судопроизводства, гарантии соблюдения принципов, конституционно-правовые основы судопроизводства.