УДК 343.98

ЦИФРОВОЕ АЛИБИ В ЭПОХУ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: ТРАНСФОРМАЦИЯ ДОКАЗЫВАНИЯ В УГОЛОВНОМ ПРОЦЕССЕ РОССИИ И ЗАРУБЕЖНЫХ СТРАН

А.Ф. Реховский[1]

[1]*Владивостокский государственный университет, г. Владивосток, Российская Федерация*

Аннотация. Настоящая статья представляет собой комплексное исследование трансформации концепции цифрового алиби в условиях внедрения технологий искусственного интеллекта, блокчейн и Интернета вещей в уголовно-процессуальное доказывание. Цифровое алиби анализируется как динамично развивающийся институт, объединяющий геолокационные данные мобильных устройств, метаданные социальных сетей, записи носимых гаджетов и информацию из систем видеонаблюдения для установления местонахождения лица в определенный момент времени. За период 2015-2025 годов концепция цифрового алиби претерпела фундаментальную эволюцию от использования простых данных сотовых операторов до применения сложных многоуровневых систем верификации на основе искусственного интеллекта и распределенных реестров. Компаративный анализ российской и зарубежной практики выявляет существенные различия в нормативном регулировании электронных доказательств: западные правовые системы характеризуются наличием специализированных стандартов аутентификации и развитой судебной практикой, тогда как российское законодательство демонстрирует отсутствие самостоятельного вида доказательств «электронные доказательства» в УПК РФ. Исследование идентифицирует критические вызовы современной эпохи: распространение deepfake-технологий, спуфинг GPS-сигналов, проблемы обеспечения непрерывности цепи хранения цифровых доказательств.

Результаты исследования обосновывают необходимость внесения изменений в УПК РФ с закреплением электронных доказательств как самостоятельного вида, разработки междисциплинарной доктрины цифровой криминалистики и формирования международных стандартов верификации цифрового алиби.

Ключевые слова: цифровое алиби, электронные доказательства, искусственный интеллект, блокчейн, deepfake, геолокация, цифровая криминалистика, GPS-спуфинг, метаданные, цепь хранения доказательств.

DIGITAL ALIBI IN THE ERA OF ARTIFICIAL INTELLIGENCE: TRANSFORMATION OF EVIDENCE IN THE CRIMINAL PROCESS OF RUSSIA AND FOREIGN COUNTRIES

A.F. Rekhovsky[1]
[1]Vladivostok State University, Vladivostok, Russian Federation

Abstract. This article presents a comprehensive study of the transformation of the concept of digital alibi in the context of the integration of artificial intelligence, blockchain, and the Internet of Things technologies into criminal procedural evidence. Digital alibi is analyzed as a dynamically developing institution that unites geolocation data from mobile devices, social media metadata, wearable device logs, and information from video surveillance systems to establish a person's location at a specific point in time. During the period 2015-2025, the concept of digital alibi has undergone a fundamental evolution, from the use of simple cellular operator data to the application of complex multi-level verification systems based on artificial intelligence and distributed ledger technologies. A comparative analysis of Russian and foreign practice reveals significant differences in the regulatory framework of electronic evidence: Western legal systems are characterized by specialized authentication standards and developed judicial practice, whereas Russian legislation lacks a separate category of evidence entitled "electronic evidence" in the Criminal Procedure Code. The study identifies critical challenges of the modern era: proliferation of deepfake technologies, GPS signal spoofing, and issues ensuring the continuity of the digital evidence chain of custody. The research substantiates the need to amend the Criminal Procedure Code of the Russian Federation by recognizing electronic evidence as an

independent type of evidence, to develop an interdisciplinary doctrine of digital forensics, and to establish international standards for the verification of digital alibi.
Keywords: digital alibi, electronic evidence, artificial intelligence, blockchain, deepfake, geolocation, digital forensics, GPS spoofing, metadata, chain of custody.

За последнее десятилетие мировое сообщество стало свидетелем беспрецедентной цифровизации общественных отношений, фундаментально трансформировавшей механизмы расследования преступлений и доказывания в уголовном процессе. Повсеместное распространение смартфонов, носимых устройств, систем Интернета вещей и социальных сетей создало новую реальность, в которой каждое действие индивида оставляет цифровые следы, потенциально значимые для установления обстоятельств совершения преступления [1, с.155]. Концепция цифрового алиби, определяемая как совокупность электронных доказательств, подтверждающих или опровергающих присутствие лица в определенном месте в конкретное время, приобрела центральное значение в расследовании преступлений и судебном разбирательстве [2, с.130-139].

Период с 2015 по 2025 годы характеризуется качественным скачком в развитии технологий, применяемых для формирования цифрового алиби. Если в начале рассматриваемого периода основными источниками геолокационных данных выступали базовые станции сотовых операторов и GPS-модули мобильных устройств, то к 2025 году арсенал инструментов расширился до носимых устройств, систем Интернета вещей, технологий распознавания лиц на базе искусственного интеллекта, блокчейн-платформ для аутентификации данных и многомодальных систем верификации [1, с.155-161]. Параллельно с технологическим прогрессом возникли новые вызовы, связанные с подделкой цифровых доказательств посредством deepfake-технологий, спуфингом GPS-сигналов и сложностями установления цепи хранения электронных данных [3, с. 76-82].

Актуальность настоящего исследования обусловлена несколькими факторами. Во-первых, отсутствием систематизированного анализа международных и российских трендов в области цифрового алиби за последнее десятилетие. Во-вторых, существенными различиями в правовых подходах к электронным доказательствам между российской и зарубежной юрисдикциями, требующими компаративного исследования [4, с.74-84]. В-третьих, стремительным развитием технологий искусственного интеллекта и блокчейн, создающих качественно новые возможности и угрозы для системы уголовного правосудия. Цель исследования заключается в комплексном анализе эволюции концепции цифрового алиби в условиях цифровой трансформации уголовного процесса, выявлении основных трендов и проблем использования электронных доказательств в российской и зарубежной практике, разработке предложений по совершенствованию правового регулирования [5, с.31-34].

Методологическую основу исследования составляет комплекс общенаучных и специально-юридических методов познания. Применялся компаративный метод для сопоставления российской и зарубежной практики использования цифрового алиби, включая анализ судебных прецедентов США, Великобритании и Европейского Союза. Историко-правовой метод использовался для выявления эволюции концепции цифрового алиби с 2015 по 2025 год, включая идентификацию пяти ключевых этапов технологической трансформации [6, с.62-66]. Системно-структурный анализ позволил выявить взаимосвязи между технологическими инновациями, правовыми институтами и криминологическими вызовами. Одним из первых определений в российской криминалистике было дано И.П. Понамаревым: «цифровое алиби следует понимать как факт непосредственного взаимодействия подозреваемого (обвиняемого) в момент совершения преступления с электронной системой, находящейся в другом месте» [7, с.437].

Эмпирическую базу исследования составили научные публикации в ведущих международных журналах по криминологии, индексируемых в базах

Scopus и Web of Science, нормативные акты РФ и зарубежных государств, регулирующие обращение с электронными доказательствами [8, с.265-270].

Начальный этап развития цифрового алиби (2015-2017) характеризовался массовым внедрением GPS-модулей в смартфоны и навигационные системы, что создало фундамент для формирования геолокационного алиби. В этот период основными источниками данных о местоположении выступали детализации соединений сотовых операторов (Call Detail Records, CDR), содержащие информацию о базовых станциях, через которые осуществлялась связь, и GPS-треки навигационных приложений [9, с.150-164]. Судебная практика зарубежных стран демонстрирует активное использование GPS-данных для установления алиби. Показательным является дело People v. Dobson (2015, США), где GPS-данные навигационной системы автомобиля использовались для установления маршрута передвижения обвиняемого и опровержения его алиби [10, с. 157-176]. В России в этот период правоприменительная практика начала систематическое использование данных сотовых операторов, хотя процессуальное оформление таких доказательств оставалось проблематичным ввиду отсутствия специального регулирования в УПК РФ [4, с. 74-84].

Критическая проблема данного периода заключалась в точности геолокации на основе CDR. Метод триангуляции по базовым станциям обеспечивал точность определения местоположения в радиусе от 100 метров до нескольких километров в зависимости от плотности размещения вышек связи, что создавало существенную погрешность для целей доказывания. GPS-модули предоставляли более высокую точность (5-10 метров), однако требовали активного использования соответствующих приложений и надежного сохранения данных [11, с. 6-16].

Второй этап развития цифрового алиби (2018-2020) ознаменовался диверсификацией источников электронных доказательств за счет массового распространения социальных сетей с функциями геотегирования и носимых устройств. Платформы Facebook, Instagram, Twitter начали сохранять метаданные о местоположении пользователей при публикации контента,

создавая дополнительные слои цифровых следов. Функция check-in в социальных сетях позволяла пользователям добровольно маркировать свое местоположение, что стало использоваться в судебной практике как для подтверждения, так и для опровержения алиби. И.Г. Смирнова справедливо отмечает что «…современные реалии расследования уголовных дел таковы, что для установления обстоятельств дела с учетом развития информационных, компьютерных технологий понятия алиби в узком смысле может оказаться недостаточно. И тогда появляются иные термины, вписывающиеся в понимание алиби в широком смысле» [12, с. 86].

Революционное значение в этот период приобрели носимые устройства - фитнес-трекеры Fitbit, Apple Watch, Garmin, которые непрерывно фиксировали геолокацию, физиологические параметры пользователя и модели физической активности. Резонансное дело Connecticut v. Richard Dabate (2015-2020) продемонстрировало потенциал носимых устройств в расследовании преступлений. Обвиняемый утверждал, что его жена была убита грабителем, однако данные с ее фитнес-трекера Fitbit показали, что в момент предполагаемого нападения она активно передвигалась по дому, что противоречило версии мужа и привело к его осуждению за убийство [13, с. 86-189]. Этот прецедент продемонстрировал, что носимые устройства могут предоставлять более надежные доказательства, чем традиционные свидетельские показания, благодаря объективной фиксации физиологических параметров [14, с.1-22].

В России в этот период правоохранительные органы начали активно использовать данные социальных сетей для установления местонахождения подозреваемых. Однако процессуальные механизмы получения таких доказательств оставались недостаточно разработанными, создавая риски признания доказательств недопустимыми [15, с. 521-540]. Статья 164.1 УПК РФ, введенная в 2016 году, регламентирует процедуру изъятия электронных носителей информации, однако не решила всех проблем, поскольку не

охватывает специфику облачных хранилищ и данных, хранящихся на серверах иностранных компаний [16, с. 109-126].

Третий этап развития цифрового алиби (2021-2023) характеризуется масштабным внедрением технологий искусственного интеллекта в анализ цифровых доказательств и формирование алиби. Системы распознавания лиц на базе нейронных сетей, интегрированные в городские системы видеонаблюдения, позволили автоматизировать процесс идентификации местонахождения лиц в публичных пространствах [17, с. 55432-442]. Платформы аналитики больших данных начали агрегировать информацию из множественных источников - GPS-данных, записей камер наблюдения, транзакций банковских карт, использования транспортных карт - для создания комплексных профилей перемещений индивидов.

Параллельно возникла критическая угроза достоверности цифровых доказательств, связанная с развитием deepfake-технологий. Генеративные нейронные сети получили способность создавать высококачественные поддельные видео- и аудиозаписи, практически неотличимые от подлинных [18, с. 100-109]. В 2021 году зафиксированы первые случаи использования deepfake для фабрикации алиби, что поставило перед судебной системой задачу разработки методов верификации аутентичности цифрового контента. В зарубежной практике начали внедряться специализированные экспертизы цифровых доказательств с применением методов форензики искусственного интеллекта, разработаны алгоритмы детекции признаков манипуляции с изображениями и видео [19, с.69-95]. В России формирование компетенций в области цифровой криминалистики происходило менее системно, хотя отдельные экспертные учреждения начали осваивать соответствующие методики [20, с.390-397]. «Использование цифровых отпечатков компьютерных устройств имеет большой идентификационный потенциал, использование которого возможно не только в рамках антифрод-систем, но и при предотвращении и расследовании компьютерных инцидентов и

киберпреступлений, деанонимизации пользователей, а также в целях защиты авторских прав и формирования целевой рекламы» [20, с.395].

Текущий этап развития цифрового алиби (2024-2025) характеризуется поиском решений проблемы аутентификации электронных доказательств через технологии распределенных реестров. Блокчейн-платформы, обеспечивающие неизменность и возможность отслеживания происхождения данных, начали применяться для создания защищенных цепей хранения цифровых доказательств [21, с. 18-33]. Принцип работы блокчейн основан на создании криптографически связанных блоков данных, каждый из которых содержит хеш предыдущего блока, временную метку и информацию о транзакции, что делает практически невозможным несанкционированное изменение записей [22, с.709-727].

Интернет вещей создал новые измерения цифрового алиби. Умные дома фиксируют присутствие жильцов через датчики движения, умные замки, системы климат-контроля. Подключенные автомобили записывают детальную телематическую информацию: геолокацию, скорость, траекторию движения, что позволяет реконструировать маршруты с высокой точностью [23, с.45-160]. Носимая медицинская электроника регистрирует физиологические параметры, позволяя верифицировать физическую активность в определенное время. Однако развитие IoT-экосистемы создает острые этические и правовые проблемы, связанные с постоянной слежкой и эрозией приватности [24, с.128-136].

Компаративный анализ российской и зарубежной практики выявляет фундаментальные различия в правовом регулировании электронных доказательств. В американской правовой системе Federal Rules of Evidence (Rule 901) содержат детализированные требования к аутентификации электронных доказательств, включая цифровое алиби. Установлен стандарт, согласно которому сторона, представляющая электронное доказательство, должна продемонстрировать, что данные являются тем, за что их выдают, через свидетельские показания, характеристики самих данных или иные обстоятельства [25, с. 1-15].

Европейский Союз в рамках регулирования электронного правосудия принял механизмы трансграничного доступа к электронным доказательствам. Общий регламент о защите данных (GDPR, 2016/679) установил строгие стандарты обработки персональных данных, включая геолокационную информацию, что создало дополнительные процессуальные гарантии при использовании цифрового алиби [26, с.105487], а также правила работы с цифровыми доказательствами[1].

Великобритания демонстрирует сбалансированный подход, сочетающий эффективность расследования с защитой прав личности. Полицейская практика использования данных мобильных телефонов для установления алиби регулируется специальными протоколами, требующими судебного санкционирования доступа к геолокационной информации.

Российская правовая система характеризуется отсутствием самостоятельного вида доказательств «электронные доказательства» в УПК РФ. Цифровые данные квалифицируются через существующие категории - вещественные доказательства (ст. 81 УПК РФ), иные документы (ст. 84 УПК РФ) или заключения эксперта (ст. 80 УПК РФ). Такая конструкция создает процессуальные сложности, поскольку не учитывает специфику электронной информации, включая возможность копирования без потери оригинала, динамический характер данных и необходимость специальных познаний для интерпретации [27, с.168-172]. Проблема усугубляется трансграничным характером цифровых данных - серверы социальных сетей расположены за пределами России, что затрудняет получение доказательств в рамках международного сотрудничества.

Центральная проблема современной концепции цифрового алиби связана с обеспечением достоверности электронных данных. Технологическое развитие

[1] 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.

создало множественные векторы угроз целостности доказательств. Спуфинг GPS-сигналов позволяет подменять реальное местоположение устройства фальсифицированными координатами. Приложения fake GPS, доступные в публичных магазинах программного обеспечения, дают возможность имитировать нахождение в любой точке мира, создавая риски фабрикации цифрового алиби. Deepfake-технологии представляют качественно новую угрозу. Генеративно-состязательные нейронные сети способны создавать синтетические видео- и аудиозаписи, воспроизводящие облик и голос реальных лиц с высокой степенью правдоподобия [28, с.569-584].

Модификация метаданных EXIF в цифровых фотографиях позволяет изменять информацию о времени, месте съемки и параметрах камеры. Экспертные исследования показывают, что значительная часть цифровых изображений, циркулирующих в социальных сетях, подвергалась той или иной форме редактирования. Проблема цепи хранения доказательств (chain of custody) в цифровой среде обостряется легкостью копирования и модификации данных. Традиционные процессуальные механизмы, разработанные для материальных объектов, не полностью адекватны специфике электронной информации. Требуется документирование каждого этапа обращения с цифровыми доказательствами, включая создание криптографических хешей, ведение журналов доступа и использование защищенных хранилищ [29, с.585-586].

Зарубежная практика выработала стандарты цифровой криминалистики, включая ISO/IEC 27037 «Guidelines for identification, collection, acquisition and preservation of digital evidence» (2012). Стандарт устанавливает процедуры обращения с электронными доказательствами, обеспечивающие их целостность и допустимость в судебном процессе[2]. В России соответствующие стандарты находятся в стадии разработки, что создает риски признания доказательств

[2] ГОСТ Р ИСО/МЭК 27037-2014. Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме.

недопустимыми и снижает эффективность их использования в расследовании преступлений.

Применение искусственного интеллекта трансформирует как формирование, так и верификацию цифрового алиби. Системы машинного обучения анализируют паттерны поведения индивидов, выявляя аномалии, которые могут указывать на фальсификацию данных [18, с.100-109]. Технологии компьютерного зрения применяются для автоматизированного анализа видеозаписей систем наблюдения. Нейронные сети распознавания лиц идентифицируют присутствие конкретных лиц в публичных пространствах, создавая временные линии их перемещений. Критическая проблема применения ИИ связана с алгоритмической предвзятостью. Исследования демонстрируют, что системы распознавания лиц обладают различной точностью для представителей разных расовых и гендерных групп, что создает риски дискриминации [30, с. 1-22].

Технологии распределенных реестров предлагают решение проблемы обеспечения целостности цифровых доказательств. Блокчейн-платформы создают неизменяемую запись всех операций с данными, что позволяет верифицировать аутентичность и отслеживать цепь хранения. Экспериментальные проекты демонстрируют практическую применимость блокчейн для управления цифровыми доказательствами. Смарт-контракты автоматизируют процессы контроля доступа, обеспечивая, что только авторизованные лица могут просматривать или модифицировать данные. Перспективным направлением является интеграция блокчейн с технологиями NFT для создания уникальных цифровых идентификаторов доказательств.

Экосистема Интернета вещей создает новые измерения цифрового алиби через непрерывный сбор данных из множественных источников. Концепция амбиентной разведки[3] предполагает создание интеллектуальных сред, которые незаметно для пользователя собирают и анализируют данные о его активности.

[3] **Суть концепции** - создание среды, в которой электронные устройства реагируют на присутствие людей, распознают его и адаптируются к потребностям пользователя.

С одной стороны, это создает беспрецедентные возможности для установления алиби и расследования преступлений. С другой стороны, возникают острые этические и правовые проблемы, связанные с постоянной слежкой и эрозией приватности. Феномен «расползания наблюдения» описывает тенденцию к расширению систем мониторинга за пределы первоначально заявленных целей. Технологии, внедренные для обеспечения безопасности, начинают использоваться для контроля поведения граждан в широком спектре контекстов.

Центральная правовая дилемма современной концепции цифрового алиби заключается в балансировании между эффективностью расследования преступлений и защитой фундаментального права на приватность [26, с.105487]. Технологии массового сбора геолокационных данных создают возможности для раскрытия преступлений, но одновременно подвергают граждан тотальной слежке. Конституционный Суд РФ в своих решениях подчеркивал необходимость соблюдения баланса между публичными и частными интересами при ограничении права на неприкосновенность частной жизни [4]. Однако конкретные критерии пропорциональности вмешательства в приватность при использовании технологий цифрового алиби остаются недостаточно разработанными.

Европейская концепция «защиты данных по дизайну» предполагает встраивание механизмов защиты приватности в архитектуру информационных систем с момента их проектирования. Применительно к системам формирования цифрового алиби это означает минимизацию сбора данных, ограничение сроков хранения, анонимизацию информации, не имеющей доказательственного значения. Концепция «цифрового свидетеля» описывает трансформацию граждан в непроизвольных источников доказательственной информации. Каждый пользователь смартфона потенциально является носителем данных, значимых для расследования преступлений, совершенных в зоне его присутствия [19, с. 69-95].

[4] См.: Постановления Конституционного Суда РФ: от 17 июня 2013 года № 13-П, от 5 марта 2013 года № 5-П, от 17 января 2019 года № 4-П, от 16 июля 2018 года № 32-П.

Совершенствование российского правового регулирования цифрового алиби требует системных изменений в уголовно-процессуальном законодательстве. Ключевым направлением является введение самостоятельного вида доказательств «электронные доказательства» в УПК РФ. Это позволит учесть специфику цифровых данных, включая их динамический характер, возможность удаленного доступа, необходимость специальных познаний для интерпретации. Требуется детализация процедур изъятия и исследования электронных доказательств, включая данные из облачных хранилищ, социальных сетей, систем Интернета вещей.

Необходимо регламентировать участие специалистов с компетенциями в области цифровой криминалистики на всех этапах обращения с доказательствами. Следует установить стандарты создания и хранения копий электронных данных, обеспечивающие их целостность через применение криптографических хеш-функций. Актуальным является внедрение концепции цифровой цепи хранения доказательств с документированием каждой операции в защищенных системах, потенциально на базе блокчейн-технологий. Необходимо законодательное закрепление стандартов оценки достоверности цифровых доказательств судом, включая презумпции и критерии, которыми суд руководствуется при оценке геолокационных данных, учитывая возможности их фальсификации.

Трансграничный характер цифровых данных требует международной гармонизации правовых стандартов обращения с электронными доказательствами. Серверы, на которых хранятся данные о геолокации пользователей, часто находятся в юрисдикциях, отличных от места совершения преступления.

Будапештская конвенция о киберпреступности [5] создала механизмы международного сотрудничества в области компьютерных преступлений, однако не охватывает в полной мере вопросы трансграничного доступа к

[5] Конвенция о преступности в сфере компьютерной информации ETS N 185 (Будапешт, 23 ноября 2001 г.).

цифровым доказательствам. США и Европейский Союз разработали Agreement on Cross-Border Access to Electronic Evidence, упрощающий процедуры получения данных от провайдеров услуг. Россия не является участником этих соглашений, что создает препятствия для международного сотрудничества.

Требуется разработка универсальных стандартов аутентификации цифровых доказательств, признаваемых в различных юрисдикциях. Модель ISO/IEC 27037 может стать основой для формирования таких стандартов, если будет дополнена специфическими требованиями к геолокационным данным и цифровому алиби. Перспективным является создание международной базы данных сертифицированных экспертов в области цифровой криминалистики, чьи заключения признавались бы в различных государствах. Необходимо создание специализированных экспертных учреждений, оснащенных современным программно-техническим инструментарием для исследования электронных доказательств, подготовка и повышение квалификации кадров в сфере цифровой криминалистики.

За последнее десятилетие концепция цифрового алиби претерпела фундаментальную трансформацию, эволюционировав от использования базовых геолокационных данных сотовых операторов до комплексных систем, интегрирующих искусственный интеллект, блокчейн, Интернет вещей и носимые устройства. Технологическое развитие создало беспрецедентные возможности для установления обстоятельств, имеющих значение для уголовного дела, но одновременно породило новые вызовы, связанные с обеспечением достоверности доказательств, защитой приватности и процессуальным оформлением электронной информации.

Компаративный анализ выявил существенные различия между российской и зарубежной практикой. Западные правовые системы характеризуются более высокой степенью нормативной разработанности статуса электронных доказательств, наличием специализированных стандартов аутентификации и формированием судебной практики по конкретным категориям дел с использованием цифрового алиби. Российское законодательство демонстрирует

отставание, проявляющееся в отсутствии самостоятельного вида доказательств «электронные доказательства», недостаточной детализации процедур изъятия и исследования цифровых данных, пробелах в регулировании трансграничного доступа к информации [4, с. 74-84].

Ключевые тренды развития концепции цифрового алиби включают технологическую диверсификацию источников геолокационных данных, интеграцию искусственного интеллекта в процессы сбора, анализа и верификации доказательств, применение блокчейн-технологий для обеспечения целостности электронной информации, обострение проблематики достоверности в контексте deepfake и спуфинга, трансформацию правовых подходов к балансу между эффективностью расследования и защитой приватности. Перспективные направления включают разработку междисциплинарной доктрины цифровой криминалистики, интегрирующей правовые, технические и криминологические аспекты, формирование универсальных международных стандартов обращения с электронными доказательствами, разработку методов детекции фальсификации цифровых данных на основе искусственного интеллекта [18, с. 100-109].

Для российской правовой системы критически важно внесение изменений в УПК РФ, закрепляющих электронные доказательства как самостоятельный вид, регламентирующих процедуры их изъятия, хранения и исследования с учетом специфики цифровой среды. Необходимо формирование компетенций в области цифровой криминалистики у правоприменителей и экспертов, включая освоение методов анализа геолокационных данных, метаданных, блокчейн-записей [20, с. 390-397]. Концепция цифрового алиби в XXI веке представляет собой динамично развивающуюся область на пересечении права, технологий и криминологии, требующую междисциплинарного подхода и постоянной адаптации правовых институтов к технологическим изменениям.

Список использованной литературы

1. Малык А.В. Цифровое алиби: понятие, сущность, проверка // Юридический вестник Дагестанского государственного университета. 2024. Т. 51. № 3. С. 155-161.

2. Александров А.С. Проблемы теории уголовно-процессуального доказывания, которые надо решать в связи с переходом в эпоху цифровых технологий // Судебная власть и уголовный процесс. 2018. № 2. С. 130-139.

3. Гирьятович Д.В. Classification of Methods of Falsification of Evidentiary Information in the Context of Digital Transformation of Crime // The digest of research works "Criminalistics: yesterday, today, tomorrow". 2023. № 4(28). P. 76-82.

4. Воронин М. Электронные доказательства в УПК: быть или не быть? // Lex russica. 2019. № 7 (152). С. 74-84.

5. Иванов Н.А. Применение специальных познаний при проверке «цифрового алиби» // Информационное Право. 2006. № 4. С. 31-34.

6. Логвин В.М. Алиби: теоретические и прикладные аспекты // Юстиция Беларуси. 2020. № 5. С. 62-66.

7. Пономарев И.П. Цифровое алиби и его проверка // Вестник Воронежского государственного университета. Серия: право. 2011. № 2. С. 437-444.

8. Мещеряков В. А. Следы преступлений в сфере высоких технологий / В. А. Мещеряков // Библиотека криминалиста. Научный журнал. – 2013. – № 5(10). – С. 265-270. – EDN RDFWJD.

9. Абдулвалиев А. Ф. Предпосылки и перспективы внедрения электронной формы уголовного дела в деятельность судебных органов / А. Ф. Абдулвалиев // Право и политика. – 2013. – № 1. – С. 58-65. – EDN PUWNHH.

10. Olson E.A., Wells G.L. What Makes a Good Alibi? A Proposed Taxonomy // Law and Human Behavior. 2004. Vol. 28. № 2. P. 157-176.

11. Meister S., Chassanoff A. Integrating Digital Forensics Techniques into Curatorial Tasks: A Case Study // International Journal of Digital Curation. 2014. Vol. 9. № 2. P. 6-16.

12. Смирнова И.Г. Значение алиби по делам о преступлениях в сфере компьютерной информации: в развитие идей В.И. Шиканова // Сибирские уголовно-процессуальные и криминалистические чтения. 2015. № 2 (8). С. 81-87.

13. Almogbil A., Alghofaili A., Deane C., Leschke T. The Accuracy of GPS-Enabled Fitbit Activities as Evidence: A Digital Forensics Study // 2020 7th IEEE International Conference on Cyber Security and Cloud Computing. 2020. P. 186-189.

14. Allison M., Caluri G., Jordoson J., Solan S. Judicial Instructions on Alibis: Impact on Mock Jury Decision-Making // Psychiatry, Psychology and Law. 2024. P. 1-22.

15. Пастухов П.С. Цифровые платформы как основа электронного документооборота в уголовном судопроизводстве // Пермский юридический альманах. 2023. № 6. С. 521-540.

16. Пастухов П.С., Абшилава Г.В. Трансформация криминалистической идентификации в структуре уголовно-процессуального доказывания // Ex jure. 2024. № 4. С. 109-126.

17. Xiao J., Li S., Xu Q. Video-Based Evidence Analysis and Extraction in Digital Forensic Investigation // IEEE Access. 2019. Vol. 7. P. 55432-442.

18. Смушкин А.Б., Менжега М.М. Некоторые вопросы цифровизации криминалистики // Lex russica. 2023. Т. 76. № 3 (196). С. 100-109.

19. Campbell E. Techno-Digital Policing and Speculative Fictions: Towards a Criminology of the Future // Crime, Media, Culture: An International Journal. 2025. Vol. 21. № 1. P. 69-95.

20. Вехов В.Б., Смушкин А.Б. Криминалистическое исследование цифровых отпечатков компьютерных устройств // Всероссийский криминологический журнал. 2024. Т. 18. № 4. С. 390-397.

21. Matijašević J., Bingulac N., Marinković D. Digital Evidence in Criminal Proceedings: Challenges and Solutions // Pravo - Teorija i Praksa. 2024. Vol. 41. № 4. P. 18-33.

22. Santamaría P., Tobarra L., Pastor-Vargas R., Robles-Gómez A. Smart contracts for managing the chain-of-custody of digital evidence: A practical case of study // Smart Cities. 2023. Vol. 6. № 2. P. 709-727.

23. Lin J., Xiao B., Zhang H., Yang X., Zhao P. A Novel Multitype-Users Welfare Equilibrium Based Real-Time Pricing in Smart Grid // Future Generation Computer Systems. 2020. Vol. 108. P. 145-160.

24. Korin A. Spatiotemporal Factors in Crime Investigation // Bulletin of the Kazan Law Institute of MIA Russia. 2024. Vol. 15. № 2. P. 128-136.

25. Lavin Perrino I. et al. An Analysis of Blockchain Solutions for Digital Evidence Chain of Custody // Universidad de Valladolid. 2025. P. 1-15.

26. Miyashita H. Human-Centric Data Protection Laws and Policies: A Lesson from Japan // Computer Law & Security Review. 2021. Vol. 40. P. 105487.

27. Попов А.П., Попов А.А. Электронные доказательства в уголовно-процессуальном доказательственном праве // Пробелы в российском законодательстве. Юридический журнал. 2020. № 1. С. 168-172.

28. Higgins E.M., Coffey B.S., Fisher B.W., Benitez I., Swartz K. School Safety or School Criminalization? The Typical Day of A School Resource Officer in the United States // The British Journal of Criminology. 2022. Vol. 62. № 3. P. 569-584.

29. Liu J., Kammar R., Sasaki R., Uehara T. Malware Behavior Ontology for Digital Evidence // 2017 IEEE International Conference on Software Quality, Reliability and Security Companion. 2017. P. 585-586.

30. O'Hagan M. Pixel Perfect Alibi: Perceptions of Fabricated Digital Alibi Evidence Created Using Generative Artificial Intelligence // OSF. 2025. P. 1-22.

References

1. Malyk A.V. Digital alibi: concept, essence, verification // Yuridichesky Vestnik Dagestanskogo Gosudarstvennogo Universiteta [Legal Bulletin of Dagestan State University]. 2024. Vol. 51, No. 3, pp. 155-161.

2. Alexandrov A.S. Problems of the theory of criminal procedural evidence that need resolution in the era of digital technologies // Sudebnaya Vlast i Ugolovny Protsess [Judicial Power and Criminal Process]. 2018. No. 2, pp. 130-139.

3. Giryatovich D.V. Classification of methods of falsification of evidentiary information in the context of digital transformation of crime // The digest of research works "Criminalistics: yesterday, today, tomorrow". 2023. No. 4(28), pp. 76-82.

4. Voronin M. Electronic evidence in the Criminal Procedure Code: to be or not to be? // Lex Russica. 2019. No. 7 (152), pp. 74-84.

5. Ivanov N.A. Application of special knowledge in verification of “digital alibi” // Informatsionnoe Pravo [Information Law]. 2006. No. 4, pp. 31-34.

6. Logvin V.M. Alibi: theoretical and applied aspects // Yustitsiya Belarusi [Justice of Belarus]. 2020. No. 5, pp. 62-66.

7. Ponomarev I.P. Digital alibi and its verification // Vestnik Voronezhskogo Gosudarstvennogo Universiteta. Seriya: Pravo [Bulletin of Voronezh State University. Series: Law]. 2011. No. 2, pp. 437-444.

8. Meshcheryakov V.A. Traces of crimes in the field of high technology / V.A. Meshcheryakov // Biblioteka Kriminalista. Nauchny Zhurnal [Library of the Criminologist. Scientific Journal]. 2013. No. 5(10), pp. 265-270. EDN RDFWJD.

9. Abdulvaliev A.F. Preconditions and prospects of introduction of electronic criminal case form in judicial bodies activity / A.F. Abdulvaliev // Pravo i Politika [Law and Policy]. 2013. No. 1, pp. 58-65. EDN PUWNHH.

10. Olson E.A., Wells G.L. What Makes a Good Alibi? A Proposed Taxonomy // Law and Human Behavior. 2004. Vol. 28, No. 2, pp. 157-176.

11. Meister S., Chassanoff A. Integrating Digital Forensics Techniques into Curatorial Tasks: A Case Study // International Journal of Digital Curation. 2014. Vol. 9, No. 2, pp. 6-16.

12. Smirnova I.G. The significance of alibi in cases related to crimes in computer information sphere: development of ideas of V.I. Shikanov // Sibirskiye Ugolovno-Protsessualnye i Kriminalisticheskie Chteniya [Siberian Criminal Procedure and Forensic Readings]. 2015. No. 2 (8), pp. 81-87.

13. Almogbil A., Alghofaili A., Deane C., Leschke T. The Accuracy of GPS-Enabled Fitbit Activities as Evidence: A Digital Forensics Study // 2020 7th IEEE International Conference on Cyber Security and Cloud Computing. 2020. pp. 186-189.

14. Allison M., Caluri G., Jordoson J., Solan S. Judicial Instructions on Alibis: Impact on Mock Jury Decision-Making // Psychiatry, Psychology and Law. 2024. pp. 1-22.

15. Pastukhov P.S. Digital platforms as the basis for electronic document flow in criminal proceedings // Permskiy Yuridicheskiy Almanakh [Perm Legal Almanac]. 2023. No. 6, pp. 521-540.

16. Pastukhov P.S., Abshilava G.V. Transformation of forensic identification in the structure of criminal procedural evidence // Ex jure. 2024. No. 4, pp. 109-126.

17. Xiao J., Li S., Xu Q. Video-Based Evidence Analysis and Extraction in Digital Forensic Investigation // IEEE Access. 2019. Vol. 7, pp. 55432-55442.

18. Smushkin A.B., Menzhega M.M. Some issues of digitalization of criminology // Lex Russica. 2023. Vol. 76, No. 3 (196), pp. 100-109.

19. Campbell E. Techno-Digital Policing and Speculative Fictions: Towards a Criminology of the Future // Crime, Media, Culture: An International Journal. 2025. Vol. 21, No. 1, pp. 69-95.

20. Vekhov V.B., Smushkin A.B. Forensic study of digital prints of computer devices // Vserossiyskiy Kriminologicheskiy Zhurnal [All-Russian Criminological Journal]. 2024. Vol. 18, No. 4, pp. 390-397.

21. Matijašević J., Bingulac N., Marinković D. Digital Evidence in Criminal Proceedings: Challenges and Solutions // Pravo - Teorija i Praksa [Law - Theory and Practice]. 2024. Vol. 41, No. 4, pp. 18-33.

22. Santamaría P., Tobarra L., Pastor-Vargas R., Robles-Gómez A. Smart contracts for managing the chain-of-custody of digital evidence: A practical case of study // Smart Cities. 2023. Vol. 6, No. 2, pp. 709-727.

23. Lin J., Xiao B., Zhang H., Yang X., Zhao P. A Novel Multitype-Users Welfare Equilibrium Based Real-Time Pricing in Smart Grid // Future Generation Computer Systems. 2020. Vol. 108, pp. 145-160.

24. Korin A. Spatiotemporal Factors in Crime Investigation // Bulletin of the Kazan Law Institute of MIA Russia. 2024. Vol. 15, No. 2, pp. 128-136.

25. Lavin Perrino I. et al. An Analysis of Blockchain Solutions for Digital Evidence Chain of Custody // Universidad de Valladolid. 2025. pp. 1-15.

26. Miyashita H. Human-Centric Data Protection Laws and Policies: A Lesson from Japan // Computer Law & Security Review. 2021. Vol. 40, Article 105487.

27. Popov A.P., Popov A.A. Electronic evidence in criminal procedural evidentiary law // Problemy v Rossiyskom Zakonodatelstve [Gaps in Russian Legislation]. Legal Journal. 2020. No. 1, pp. 168-172.

28. Higgins E.M., Coffey B.S., Fisher B.W., Benitez I., Swartz K. School Safety or School Criminalization? The Typical Day of A School Resource Officer in

the United States // The British Journal of Criminology. 2022. Vol. 62, No. 3, pp. 569-584.

29. Liu J., Kammar R., Sasaki R., Uehara T. Malware Behavior Ontology for Digital Evidence // 2017 IEEE International Conference on Software Quality, Reliability and Security Companion. 2017. pp. 585-586.

30. O'Hagan M. Pixel Perfect Alibi: Perceptions of Fabricated Digital Alibi Evidence Created Using Generative Artificial Intelligence // OSF. 2025. pp. 1-22.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Реховский Александр Федорович – доцент кафедры уголовно-правовых дисциплин Института права Владивостокского государственного университета, кандидат юридических наук, доцент, г. Владивосток, Российская Федерация; e-mail: A.Rekhovsky@vvsu.ru.

INFORMATION ABOUT THE AUTHOR

Rekhovsky Aleksandr Fedorovich – Associate Professor at the Department of Criminal Law Disciplines, Institute of Law, Vladivostok State University, Candidate of Juridical Sciences, Associate Professor, Vladivostok, Russian Federation; e-mail: A.Rekhovsky@vvsu.ru.