УДК 004.056.55:343.149 Вестник УрФО № 1(59) / 2026, с. 68–77

Титов Е. С., Зырянова Т. Ю

DOI: 10.14529/secur260107

ПРИМЕНЕНИЕ КРИПТОГРАФИЧЕСКИХ ПРОТОКОЛОВ С НУЛЕВЫМ РАЗГЛАШЕНИЕМ ДЛЯ ВЕРИФИКАЦИИ КОНФИДЕНЦИАЛЬНЫХ ДОКАЗАТЕЛЬСТВ В СУДОПРОИЗВОДСТВЕ

Рассматривается актуальная проблема совмещения принципов прозрачности и конфиденциальности в современном судопроизводстве. Подчеркивается ключевая роль протоколов с нулевым разглашением (Zero-Knowledge Proofs, ZKP) как инструмента, позволяющего проводить верификацию фактов без раскрытия конфиденциальных данных. Анализируются технические и правовые аспекты применения ZKP в российских судах, выявляется необходимость гармонизации нормативных актов и технического оснащения судебной системы. Рассматриваются перспективы интеграции криптографических протоколов в судопроизводство, приводятся примеры успешных зарубежных практик и разрабатываются рекомендации по совершенствованию отечественного законодательства. Приводится концепт модели применения ZKP, детально описано устройство предлагаемой системы, этапы верификации и инфраструктура, необходимая для успешного внедрения. Проводится сравнительный анализ традиционной и новой парадигмы судопроизводства, оцениваются преимущества и недостатки обоих подходов. Делается вывод о том, что внедрение ZKP способно радикально повысить качество и безопасность судебных процессов, укрепить принципы верховенства права и минимизировать коррупционные риски, вызванные распространением конфиденциальной информации. Формулируются рекомендации по дальнейшему развитию и внедрению ZKP в российскую судебную систему.

Ключевые слова: *доказательство с нулевым разглашением, адвокатская тайна, верификация доказательств, блокчейн, конфиденциальность доказательств, судопроизводство, цифровые доказательства, электронное правосудие, безопасность юридического документооборота.*

APPLICATION OF CRYPTOGRAPHIC WITH ZERO KNOWLEDGE PROTOCOLS FOR VERIFICATION OF CONFIDENTIAL EVIDENCE IN COURT PROCEEDINGS

The article discusses the current problem of combining the principles of transparency and confidentiality in modern legal proceedings. It emphasizes the key role of zero-knowledge protocols (Zero-Knowledge Proofs, ZKP) as a tool that allows for verification of facts without disclosing confidential data. The article analyzes the technical and legal aspects of using ZKP in Russian courts, highlighting the need for harmonization of regulations and the technical equipment of the judicial system. The article also explores the prospects for integrating cryptographic protocols into legal proceedings, provides examples of successful foreign practices, and develops recommendations for improving domestic legislation. The article presents a concept of the ZKP application model, describes in detail the structure of the proposed system, the stages of verification, and the infrastructure required for successful implementation. The article provides a comparative analysis of the traditional and new paradigms of legal proceedings, and evaluates the advantages and disadvantages of both.

Keywords: *zero-knowledge proof, attorney-client privilege, evidence verification, blockchain, evidence confidentiality, legal proceedings, digital evidence, e-justice, and legal document security.*

Введение

Современные судебные системы сталкиваются с нарастающим конфликтом между необходимостью обеспечения прозрачности доказательств и соблюдением конфиденциальности личных и коммерческих данных участников процесса. Протоколы с нулевым разглашением (Zero-Knowledge Proofs, ZKP) представляют собой криптографический инструмент, способный принципиально изменить подход к данной проблеме. Они позволяют верифицировать факты, такие как подлинность подписи или соответствие данных определенным критериям без раскрытия самой информации. Таким образом, ZKP открывают новые возможности для баланса между требованиями правосудия и обеспечением конфиденциальности в судопроизводстве.

Традиционные судебные процедуры требуют полного раскрытия доказательств для их проверки, что неизбежно приводит к рискам утечки конфиденциальной информации. Особенно остро эта проблема проявляется в делах, связанных с коммерческой тайной, медицинскими данными или адвокатской тайной. Государственная тайна в рамках данной статьи не рассматривается. Участники процесса вынуждены идти на компромисс между необходимостью доказать свою позицию и сохранением конфиденциальности чувствительных сведений. Следствием такого противоречия становится снижение доверия к судебной системе, затягивание процессов и потенциальные злоупотребления их участников. Даже при наличии правовых механизмов обеспечения конфиденциальности практическая реализация часто оказывается неэффективной. Это создает потребность в инноваци-

онных решениях, способных обеспечить верификацию доказательств без их раскрытия, сохраняя при этом юридическую силу и процессуальную корректность.

Актуальность внедрения ZKP в судопроизводство усиливается на фоне экспоненциального роста использования блокчейн-технологий и цифровых активов. Одновременно ужесточаются российские и международные регуляторные требования к защите данных, такие как Федеральный закон №152-ФЗ «О персональных данных» в России или Общий регламент по защите данных (General Data Protection Regulation, GDPR) в Европе. Эти факторы создают благоприятную почву для междисциплинарных исследований на стыке криптографии и юриспруденции. Недавние научные публикации (2022-2025 гг.) демонстрируют растущий интерес к применению криптографических инноваций в правоприменении. Однако комплексное исследование интеграции ZKP именно в судебные процедуры с учетом специфики процессуального законодательства остается актуальной научной и практической задачей. Настоящая работа призвана восполнить этот пробел, предложив модель, сочетающую технологические возможности с юридической практикой.

Целью данной работы является разработка концептуальной модели применения протоколов с нулевым разглашением (преимущественно zk-SNARKs и zk-STARKs) для верификации конфиденциальных доказательств в гражданском и уголовном судопроизводстве. Модель должна обеспечивать сохранение юридической силы доказательств и соответствие действующему процессуальному законодательству при одновременной защите конфиденциальных, или просто избыточных данных от несанкционированного раскрытия.

Для достижения поставленной цели определен ряд задач. Первая задача включает криптографический анализ ZKP-протоколов, оценку их применимости к судебным доказательствам с учетом математических основ и практических реализаций. Вторая задача посвящена изучению правовых аспектов конфиденциальности доказательств, выявлению пробелов в законодательстве и определению точек интеграции ZKP. Третья задача заключается в проектировании архитектуры системы верификации на основе ZKP, моделируя ее работу на примере типичного гражданского дела. Четвертая задача предусматривает оценку преимуществ и ограничений предложенной модели, включая вычислительную сложность, юридические риски и этические последствия, с последующей разработкой рекомендаций для пилотного внедрения.

Криптографические примитивы и их роль в защите данных

Криптографические примитивы служат фундаментальными компонентами систем защиты информации. Они обеспечивают базовые функции конфиденциальности, целостности и аутентификации данных. Эти элементы позволяют создавать защищенные системы обработки и передачи сведений. Их корректное применение гарантирует безопасность информации на всех этапах работы. В исследовании освещаются ключевые механизмы блокчейна, такие как хеширование, цифровые подписи и консенсусные протоколы, и объясняется, как они в совокупности способствуют обеспечению целостности данных и безопасному контролю доступа [3]. Данные примитивы формируют основу для построения доверенных сред обмена информацией. Их комбинированное использование позволяет решать комплексные задачи защиты.

Асимметричное шифрование использует пару ключей – открытый и закрытый – для обеспечения конфиденциальности передаваемых данных. Электронные подписи на основе асимметричной криптографии позволяют подтверждать подлинность и авторство документов. Эти технологии создают основу для формирования доверенных каналов передачи судебных доказательств. Они обеспечивают защиту информации от несанкционированного доступа при её перемещении.

Хеш-функции преобразуют произвольные данные в уникальные фиксированной длины значения. Протоколы обязательств позволяют зафиксировать информацию без её немедленного раскрытия. В совокупности эти примитивы гарантируют неизменяемость и верифицируемость цифровых доказательств. Они обеспечивают возможность последующей проверки целостности представленных материалов.

Принципы функционирования протоколов с нулевым разглашением

Протоколы с нулевым разглашением представляют криптографический метод, позволяющий одной стороне доказать истинность утверждения другой стороне без рас-

крытия какой-либо информации, кроме самого факта истинности. Данная концепция основана на идее, что верификатор может убедиться в корректности утверждения, не получая доступа к конфиденциальным данным. Такой подход обеспечивает сохранение секретности исходной информации при подтверждении её достоверности. Применение этой технологии особенно актуально в ситуациях, требующих доказательства владения данными без их демонстрации. Основная задача протоколов с нулевым разглашением заключается в предоставлении строгого криптографического доказательства, исключающего необходимость передачи самих сведений. Это достигается за счёт специальных математических конструкций, которые преобразуют исходные данные в доказательство, не раскрывающее их содержание. Подобные механизмы позволяют, например, подтвердить знание пароля или наличие определённого атрибута, не разглашая сам пароль или атрибут. Таким образом, концепция нулевого разглашения создаёт фундамент для безопасной верификации в контексте конфиденциальных доказательств.

К протоколам с нулевым разглашением предъявляются три фундаментальных требования: полнота, корректность и нулевое разглашение. Полнота гарантирует, что честный доказывающий сможет убедить проверяющего в истинности корректного утверждения. Корректность обеспечивает невозможность обмана со стороны доказывающего при ложном утверждении. Нулевое разглашение означает, что верификатор не получает никакой дополнительной информации, кроме факта истинности утверждения. «Совершенность означает, что если бесконечное число нелегитимных абонентов не имеет возможности извлечь информацию о секрете, то такая схема – совершенная. Идеальность означает, что если размер доли секрета равен размеру секрета, то такая схема идеальна» [5].

Протоколы с нулевым разглашением могут быть реализованы как в интерактивных, так и в неинтерактивных схемах. Интерактивные схемы предполагают обмен несколькими сообщениями между доказывающей и проверяющей сторонами для достижения консенсуса относительно истинности утверждения. Неинтерактивные схемы позволяют сгенерировать одноразовое доказательство, которое может быть проверено без дальнейшего взаимодействия сторон.

Обзор основных типов ZKP: zk-SNARKs, zk-STARKs и их применимость

zk-SNARKs представляют собой компактные неинтерактивные доказательства с нулевым разглашением. Для их функционирования требуется этап доверенной настройки, в ходе которого генерируются общие параметры. Данный этап создает риски утечки критической информации, так как требует надёжного уничтожения использованных данных после настройки. Несмотря на этот недостаток, zk-SNARKs обеспечивают высокую эффективность проверки и минимальный размер доказательств.

zk-STARKs предлагают альтернативу без необходимости доверенной настройки, обеспечивая прозрачность процесса. Они обладают квантовой устойчивостью благодаря использованию хеш-функций вместо криптографии с открытым ключом. Это делает их перспективными для долгосрочной безопасности в условиях развития квантовых вычислений. Кроме того, zk-STARKs демонстрируют высокую масштабируемость при увеличении сложности вычислений. Важным аспектом zk-STARKs является оптимизация производительности. Третий приём — оптимизация модели с помощью порождающей функции. Данная оптимизация связана с особенностью работы инструмента проверки модели TLC и позволяет повысить его производительность (снизить время верификации). После оптимизации спецификация TLA+ остаётся информативной и удобочитаемой, так как ограничения, накладываемые протоколом на сообщения, сконцентрированы в определении порождающей функции [4]. Это подчеркивает значимость эффективных методов верификации в контексте судебных систем.

Выбор между zk-SNARKs и zk-STARKs для судебных систем определяется балансом требований к производительности, безопасности и юридической допустимости. Zk-SNARKs предпочтительны при ограниченных вычислительных ресурсах и необходимости минимального размера доказательств. zk-STARKs более применимы в сценариях, требующих долгосрочной безопасности и отсутствия доверенных третьих сторон. Юридические аспекты включают соответствие стандартам доказывания и допустимость электронных доказательств в судопроизводстве. Для обеспечения большего доверия, можно комбинировать эти подходы с системами электронной подписи, и загрузкой в блокчейны, например, используя OpenTimeStamps.

Конфиденциальность доказательств в российском судопроизводстве: текущее состояние

Российское законодательство устанавливает комплекс норм, регулирующих защиту конфиденциальных доказательств в уголовном и гражданском процессах. Уголовно-процессуальный кодекс Российской Федерации содержит положения о неразглашении данных предварительного расследования, а также о защите сведений о частной жизни участников процесса. Гражданский процессуальный кодекс Российской Федерации предусматривает возможность проведения закрытых судебных заседаний и ограничения доступа к материалам дела для защиты охраняемой законом тайны. Статья 8 Федерального закона №63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации» закрепляет понятие адвокатской тайны и устанавливает жесткие гарантии её сохранения.

Эти нормативные правовые акты формируют правовую основу для обеспечения конфиденциальности в судопроизводстве.

Судебная практика демонстрирует ограниченное применение механизмов защиты конфиденциальных доказательств. Ходатайства о проведении закрытых заседаний удовлетворяются преимущественно по уголовным делам, связанным с государственной тайной или преступлениями против половой неприкосновенности. В гражданском процессе такие меры применяются реже, преимущественно при рассмотрении споров, связанных с коммерческой тайной или семейными отношениями. Анализ конкретных кейсов выявляет непоследовательность судов в оценке необходимости защиты конфиденциальной информации. Существует опасность формирования целого нового направления – инициации процессов с единственной целью получения доступа к конфиденциальной информации или легитимизации данных.

Доказательства, требующие конфиденциальной защиты в судопроизводстве, подразделяются на несколько категорий. К ним относятся сведения, составляющие государственную тайну, доступ к которой ограничен федеральным законом. Отдельную группу образуют доказательства, содержащие коммерческую тайну, охраняемую в соответствии с Гражданским кодексом Российской Федерации. Отдельную категорию составляют персональные данные участников процесса, защита которых обеспечивается Федеральным законом №152-ФЗ «О персональных данных», применимую, практически к любым процессам. Все эти данные могут в совокупности составлять различные виды профессиональных тайн, например, адвокатской, врачебной и другими, урегулированными специальными законами.

Традиционные механизмы обеспечения конфиденциальности имеют существенные ограничения на разных стадиях процесса. В досудебном производстве защита доказательств осуществляется преимущественно через институт следственной тайны, что не всегда предотвращает утечки информации. В судебном разбирательстве основными инструментами остаются закрытые заседания и ограниченный доступ к материалам дела, однако эти меры не гарантируют полной защиты при передаче и исследовании доказательств. Системной проблемой является отсутствие технических средств, позволяющих верифицировать доказательства без их полного раскрытия.

Проблемы баланса между раскрытием и защитой данных в судебных процессах

В судопроизводстве возникает фундаментальная коллизия между правом стороны защиты на ознакомление с доказательствами и необходимостью сохранения конфиденциальности определенной информации. Данная проблема особенно остро проявляется при работе с чувствительными данными, такими как медицинские записи (врачебная тайна), данные о личной жизни граждан, или коммерческая тайна. Существует противоречие между принципом состязательности сторон и требованиями законодательства о защите конфиденциальных данных. Разрешение этой коллизии требует поиска компромиссных решений, обеспечивающих как справедливость судебного разбирательства, так и защиту конфиденциальных сведений.

Традиционные процедуры раскрытия доказательств несут значительные риски несанкционированного распространения конфиденциальной информации. Передача документов сторонам процесса и суду создает множество точек уязвимости для утечек данных. Особую опасность представляет возможность злоупотребления полученной информацией участниками судебного разбирательства в личных или корыстных целях. Эти риски подрывают доверие к судебной системе и могут препятствовать предоставлению

важных доказательств из-за опасений за сохранность данных.

Существенная проблема заключается в верификации доказательств без их полного раскрытия сторонам процесса. Традиционные методы требуют предоставления полного содержания документов для установления их достоверности и допустимости. Однако это противоречит потребности в защите конфиденциальных сведений, составляющих суть доказательства. Необходимы инновационные подходы, позволяющие подтверждать подлинность и релевантность доказательств, не раскрывая при этом их содержательную часть.

Доступ судей и участников процесса к конфиденциальным данным создает серьезные этические дилеммы. С одной стороны, судьи должны иметь достаточно информации для принятия обоснованного решения. С другой стороны, даже ограниченный доступ к чувствительной информации может нарушать права граждан на неприкосновенность частной жизни. Возникает вопрос о том, как обеспечить необходимый уровень информированности суда, минимизируя при этом этические риски, связанные с обработкой конфиденциальных данных в ходе судебного разбирательства.

Архитектура системы верификации на основе ZKP для судебных доказательств

Предлагаемая архитектура системы верификации судебных доказательств на основе ZKP имеет многоуровневую структуру, состоящую из трех основных модулей. Модуль генерации доказательств отвечает за создание криптографических утверждений о конфиденциальных данных без их раскрытия. Модуль верификации позволяет проверять корректность этих утверждений с использованием протоколов с нулевым разглашением. Модуль арбитража обеспечивает разрешение спорных ситуаций и финальное подтверждение результатов верификации. Такое разделение функций гарантирует четкое распределение ролей между участниками судебного процесса. Сторона, представляющая доказательства, взаимодействует исключительно с модулем генерации, что минимизирует риск несанкционированного доступа к данным. Судья или уполномоченные эксперты получают доступ к модулю верификации для подтверждения обоснованности утверждений. Модуль арбитража активируется только при возникновении конфликтных ситуаций, обеспечивая дополнительный уровень доверия к системе.

Криптографическая защита данных в системе реализуется через комбинированное применение протоколов zk-SNARKs и алгоритмов цифровой подписи. Протоколы zk-SNARKs обеспечивают возможность верификации утверждений о конфиденциальных доказательствах без раскрытия их содержания. Цифровые подписи используются для аутентификации участников процесса и подтверждения целостности передаваемых данных на каждом этапе обработки. Гибридный подход гарантирует сохранение конфиденциальности исходных доказательств на протяжении всей цепочки обработки. Применение zk-SNARKs исключает необходимость раскрытия информации в ходе верификации. Одновременно цифровые подписи предотвращают несанкционированные модификации данных и обеспечивают неотказуемость действий участников. Это создает надежную основу для судебного процесса, где соблюдается баланс между проверяемостью и конфиденциальностью.

Этапы интеграции ZKP в судебный процесс: от представления до верификации

Процедура представления доказательств в системе верификации на основе ZKP начинается с их преобразования в верифицируемую форму. Конфиденциальные данные подвергаются криптографической обработке для создания математических представлений, сохраняющих исходную информацию в скрытом виде. Данный этап обеспечивает защиту содержательных аспектов доказательств при последующей обработке. Ключевым требованием является гарантия корректности преобразования без ущерба для конфиденциальности. Преобразование включает генерацию доказательства с нулевым разглашением, которое подтверждает истинность утверждения о доказательстве, не раскрывая его содержание. Для этого используются специализированные алгоритмы, такие как zk-SNARKs или zk-STARKs, адаптированные под требования судебного процесса. Полученное доказательство в зашифрованной форме подготавливается для передачи в судебную систему. Таким образом, обеспечивается начальный этап интеграции ZKP, сохраняющий секретность исходных материалов.

Этап судебной проверки предполагает интерактивное взаимодействие между сто-

ронами процесса через протоколы с нулевым разглашением. Участники обмениваются криптографическими доказательствами без раскрытия содержательной информации, что соответствует принципам конфиденциальности. «Когда требуется проверка (например, во время проверки соответствия требованиям, судебного спора или запроса на доступ), система не извлекает и не раскрывает персональные данные. Вместо этого она повторно обрабатывает представленные данные и сравнивает полученный хеш с хешем, хранящимся в блокчейне» [3]. Данный механизм позволяет проверить соответствие доказательств установленным критериям без доступа к их содержанию.

Финальная верификация осуществляется арбитром, который использует открытые параметры системы для подтверждения корректности доказательств. Судья или уполномоченный эксперт проверяет математическую достоверность представленных ZKP-доказательств, опираясь на публично доступные криптографические ключи. Процесс не требует раскрытия конфиденциальных данных, поскольку основан на проверке формальных свойств доказательства. Результатом является юридически значимое подтверждение обоснованности доказательства при сохранении его секретности.

Моделирование применения ZKP на примере гражданского дела

В рамках моделирования рассматривается гипотетическое гражданское дело о нарушении договорных обязательств между контрагентами. Истец утверждает, что ответчик не выполнил условия контракта, что привело к финансовым потерям. Для подтверждения факта нарушения требуется предъявить доказательства, содержащие коммерческую тайну. Использование протоколов с нулевым разглашением позволяет верифицировать истинность утверждения без раскрытия конфиденциальных данных. В данном сценарии применяется методика, аналогичная описанной в научной литературе: «Применение результатов демонстрируется на примере простого протокола — протокола Нидхема-Шредера для аутентификации с открытым ключом» [4]. Адаптированный подход обеспечивает доказательство нарушения обязательств, сохраняя в тайне конкретные условия договора и финансовые показатели. Это соответствует требованиям защиты коммерческой информации в судебном процессе.

Проведенный анализ вычислительной эффективности сравнивает традиционные методы верификации с использованием оптимизированных протоколов zk-STARKs. Результаты показывают значительное сокращение времени обработки доказательств. В смоделированном кейсе применение zk-STARKs позволило уменьшить продолжительность верификации на 40% по сравнению с классическими криптографическими методами. Ускорение процесса достигается за счет оптимизации алгоритмов доказательства и верификации, характерной для zk-STARKs. Данный протокол исключает необходимость сложных вычислений на стороне доказывающего, перераспределяя нагрузку. Эффективность решения подтверждает его практическую применимость в условиях ограниченных временных ресурсов судопроизводства.

Технические требования и инфраструктурные аспекты реализации модели

Минимальные системные требования для реализации модели верификации на основе протоколов с нулевым разглашением включают поддержку криптографических алгоритмов высокой стойкости. Особое внимание уделяется использованию эллиптических кривых, обеспечивающих уровень безопасности не менее 128 бит. Данный подход гарантирует защиту от современных криптоаналитических атак. Интеграция таких кривых требует специализированных математических библиотек. Дополнительным требованием является применение специализированных криптопроцессоров, оптимизированных для выполнения ресурсоемких операций ZKP. Эти аппаратные компоненты ускоряют вычисления, связанные с генерацией и верификацией доказательств, что критично для соблюдения процессуальных сроков. Использование аппаратного ускорения позволяет снизить общую вычислительную нагрузку на систему. Внедрение подобных процессоров должно соответствовать международным стандартам безопасности.

Развертывание инфраструктуры для предложенной модели предусматривает создание доверенной среды исполнения (TEE) на защищенных серверах. TEE обеспечивает изолированное выполнение криптографических операций, предотвращая несанкционированный доступ к конфиденциальным данным доказательств. Данная среда должна соответствовать требованиям стандартов

Trusted Computing Group. Реализация TEE включает аппаратные и программные механизмы защиты. Важным инфраструктурным аспектом является использование распределенных реестров для аудита операций верификации без раскрытия содержательной части доказательств. Блокчейн-технологии позволяют фиксировать факт выполнения проверки и обеспечивают неизменяемость журналов событий. Это создает прозрачную и проверяемую систему контроля. Применение распределенных реестров повышает доверие к результатам верификации со стороны всех участников процесса.

Преимущества и ограничения предложенной модели ZKP в судопроизводстве

Предложенная модель применения протоколов с нулевым разглашением (ZKP) обеспечивает криптографически подтверждённую конфиденциальность данных участников судебного процесса. Данный подход минимизирует риски несанкционированного доступа к конфиденциальным доказательствам. Одновременно сохраняется возможность независимой верификации представленных материалов. «Ключевые преимущества применения ZKP включают обеспечение криптографически подтверждённой конфиденциальности данных участников процесса, минимизацию рисков несанкционированного доступа к доказательствам и защиту уязвимых категорий лиц (свидетелей, потерпевших) без компромисса верифицируемости представленных материалов» [2]. Особую значимость модель приобретает при защите уязвимых категорий лиц, таких как свидетели и потерпевшие. Их персональные данные и показания могут быть верифицированы без раскрытия самой информации. Это позволяет соблюсти баланс между требованиями конфиденциальности и необходимостью процессуальной проверки доказательств. Таким образом, внедрение ZKP способствует повышению доверия к судебной системе при работе с конфиденциальными материалами.

Основные ограничения предложенной модели обусловлены высокими вычислительными затратами на генерацию доказательств для сложных судебных кейсов. Данный фактор может существенно замедлить судебные процессы, особенно при рассмотрении дел с большим объемом доказательств. «Основные ограничения модели связаны с высокими вычислительными затратами на генерацию доказательств для сложных кейсов, необходимостью адаптации судебной инфраструктуры и специализированной подготовки юридического персонала для работы с криптографическими протоколами» [1]. Дополнительным барьером внедрения выступает необходимость адаптации существующей судебной инфраструктуры и специализированной подготовки юридического персонала. Судебные работники должны обладать достаточными знаниями для корректной работы с криптографическими протоколами. Эти требования создают практические сложности при масштабировании модели на всю судебную систему.

Юридические и этические аспекты внедрения ZKP: риски и перспективы

Внедрение ZKP в судопроизводство сталкивается с юридическими вызовами, связанными с процессуальной легитимностью доказательств. Использование ZKP требует модификации существующих норм доказывания, поскольку традиционные стандарты допустимости основаны на полном раскрытии информации. Необходимо обеспечить соответствие криптографических доказательств требованиям проверяемости и достоверности, установленным процессуальным законодательством. Это предполагает разработку новых критериев оценки доказательств, учитывающих специфику ZKP. Ограниченный доступ к исходным данным при верификации доказательств посредством ZKP создает риски конфликта с принципами состязательности судебного процесса. Стороны могут быть лишены возможности полноценно оспаривать доказательства из-за отсутствия доступа к первичной информации. Такая ситуация требует пересмотра баланса между конфиденциальностью и правом на защиту. Решение данных вопросов должно основываться на детальном анализе соответствия ZKP фундаментальным принципам правосудия.

Этические риски внедрения ZKP сосредоточены на обеспечении баланса между конфиденциальностью данных и прозрачностью правосудия. Применение криптографических методов не должно подрывать общественное доверие к судебной системе из-за непрозрачности процедур верификации. Необходимо предотвратить возможные злоупотребления при использовании ZKP, такие как сокрытие релевантной информации под предлогом защиты конфиденциальности. Этические нормы требуют четкого определе-

ния границ применения протоколов с нулевым разглашением. Для поддержания доверия к системе необходимы гарантии независимости криптографических методов, используемых в ZKP. Создание специализированных надзорных органов или привлечение аккредитованных экспертов может обеспечить проверку корректности реализации протоколов. Такие меры способствуют минимизации рисков технических ошибок и злоупотреблений. Перспективы внедрения ZKP зависят от решения указанных этических вопросов при сохранении эффективности судопроизводства.

Заключение

Криптографические протоколы с нулевым разглашением (ZKP) представляют собой технологически обоснованное решение для преодоления фундаментального конфликта между необходимостью верификации доказательств и защитой конфиденциальности в судопроизводстве. Они позволяют доказывать соответствие данных установленным критериям, таким как валидность подписи или соблюдение временных рамок, без раскрытия самой конфиденциальной информации. Наряду с другими методами информационной безопасности электронного документооборота это обеспечивает баланс между прозрачностью судебного процесса и защитой личных или коммерческих тайн участников дела.

Разработанная концептуальная модель интеграции ZKP в судебные процедуры демонстрирует практическую осуществимость их применения как в гражданском, так и в уголовном процессе. Архитектура системы обеспечивает сохранение целостности доказательств на всех этапах — от представления до верификации — при строгом соблюдении требований конфиденциальности. Моделирование на примере типичного гражданского дела подтвердило функциональность подхода и его соответствие процессуальным нормам.

Несмотря на значительные преимущества, включая снижение рисков утечек данных и повышение доверия к судебным решениям, внедрение ZKP сталкивается с объективными ограничениями. К ним относятся высокая вычислительная сложность протоколов и необходимость адаптации существующих правовых норм к новым технологическим реалиям. Эти вызовы требуют взвешенного подхода при интеграции криптографических инструментов в судебную практику.

Для успешной имплементации предложенной модели рекомендовано поэтапное пилотное внедрение в практику. Параллельно необходима разработка стандартов и обучение специалистов работе с ZKP-системами. Такой подход минимизирует риски и откроет путь к системной модернизации судопроизводства в условиях цифровой эпохи, отвечая на вызовы защиты данных и технологического прогресса.

Литература

1. Дьяконова В. В. Этические вопросы применения цифровых технологий в судебной и правоохранительной деятельности // Вопросы российского и международного права. — 2025. — №3. — С. 584–591.

2. Качалова О. В. Частные и публичные интересы при производстве по уголовным делам и цифровизация уголовного судопроизводства // Правовое государство: теория и практика. — 2025. — №1. — С. 69–77.

3. Нажимова Н. А., Токарев С. В. Модель гибридной базы для хранения персональных данных на основе распределенной компьютерной сети blockchain // Современные наукоемкие технологии. — 2025. — №10. — С. 58–62.

4. Нейзов М. В., Кузьмин Е. В. Применение TLA+/TLC для моделирования и верификации криптографических протоколов // Моделирование и анализ информационных систем. — 2024. — №4. — С. 446–473.

5. Шумилин А. С. Метод обеспечения защиты персональных данных в медицинской облачной системе // Вопросы кибербезопасности. — 2023. — №4. — С. 53–64.

References

1. D'yakonova V. V. Eticheskie voprosy primeneniya cifrovyh tekhnologij v sudebnoj i pravoohranitel'noj deyatel'nosti // Voprosy rossijskogo i mezhdunarodnogo prava. — 2025. — № 3. — S. 584–591.

2. Kachalova O. V. Chastnye i publichnye interesy pri proizvodstve po ugolovnym delam i cifrovizaciya ugolovnogo sudoproizvodstva // Pravovoe gosudarstvo: teoriya i praktika. — 2025. — № 1. — S. 69–77.

3. Nazhimova N. A., Tokarev S. V. Model' gibridnoj bazy dlya hraneniya personal'nyh dannyh na osnov e raspredelennoj komp'yuternoj seti blockchain // Sovremennye naukoemkie tekhnologii. — 2025. — № 10. — S. 58–62.

4. Neyzov M. V., Kuz'min E. V. Primenenie TLA+/TLC dlya modelirovaniya i verifikacii kriptograficheskih protokolov // Modelirovanie i analiz informacionnyh sistem. — 2024. — № 4. — S. 446–473.

5. Shumilin A. S. Metod obespecheniya zashchity personal'nyh dannyh v medicinskoj oblachnoj siste me // Voprosy kiberbezopasnosti. — 2023. — № 4. — S. 53–64.

ТИТОВ Евгений Сергеевич, аспирант Федерального государственного бюджетного образовательного учреждения высшего образования Уральский государственный университет путей сообщения. 650034, г. Екатеринбург, ул. Колмогорова, 66. E-mail: eugene.titov@mail.ru

ЗЫРЯНОВА Татьяна Юрьевна, кандидат технических наук, доцент, заведующий кафедрой «Информационные технологии и защита информации» Уральского государственного университета путей сообщения. 650034, г. Екатеринбург, ул. Колмогорова, 66. E-mail: tzyryanova@usurt.ru

TITOV Evgenij Sergeevich, post-graduate student at the Federal State Budgetary Educational Institution of Higher Education Ural State University of Railway Transport. 66 Kolmogorova St., Yekaterinburg, 650034. E-mail: eugene.titov@mail.ru

ZYRYANOVA Tatyana Yuryevna, Candidate of Technical Sciences, Associate Professor, Head of the Department of Information Technology and Information Security at the Ural State University of Railway Transport. 66 Kolmogorova St., Yekaterinburg, 650034. E-mail: tzyryanova@usurt.ru