ИНТЕГРАЦИЯ ТЕХНОЛОГИИ БЛОКЧЕЙН В МЕДИЦИНСКИЙ ДОКУМЕНТООБОРОТ НА БАЗЕ «1С: ДОКУМЕНТООБОРОТ»: ТЕХНИЧЕСКИЕ И ПРАВОВЫЕ АСПЕКТЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В КОНТЕКСТЕ СОБЛЮДЕНИЯ ПРАВОВОГО РЕГУЛИРОВАНИЯ

Д.Е. Работаев, *студент[1], руководитель контрактной службы[2]*
[1]Уральский государственный экономический университет
[2]ФГБУ «ФЦМН» ФМБА
[1](России, г. Москва)
[2](Россия, г. Екатеринбург)

DOI:10.24412/2500-1000-2025-10-2-90-96

Аннотация. *В статье рассматривается комплексный подход к внедрению технологии блокчейн в систему электронного документооборота медицинских учреждений, функционирующую на платформе «1С: Документооборот». Проанализированы ключевые технические аспекты гибридной архитектуры, при которой централизованная система 1С дополняется децентрализованным реестром для фиксации юридически значимых событий и обеспечения неизменности данных. Особое внимание уделено правовым вызовам, связанным с защитой персональных данных пациентов в соответствии с Федеральным законом № 152-ФЗ «О персональных данных», а также проблемам правового регулирования ЭДО в государственном управлении применительно к сфере здравоохранения. Предложены конкретные юридические и организационные механизмы для легализации технологии, включая разработку внутренних нормативных актов и решение коллизии между неизменностью блокчейна и «правом на забвение». Статья адресована руководителям медицинских учреждений и юристам, заинтересованным в повышении уровня защиты данных и оптимизации документооборота в условиях цифровой трансформации.*

Ключевые слова: *блокчейн, 1С: Документооборот, здравоохранение, персональные данные, ФЗ-152, электронный документооборот, информационная безопасность, электронная подпись, правовое регулирование, гибридная архитектура.*

Цифровая трансформация здравоохранения является одним из приоритетных направлений развития современной медицины. Переход к электронному документообороту (ЭДО), внедрение электронных медицинских карт (ЭМК) и телемедицинских технологий значительно повышают эффективность лечебно-диагностического процесса, однако одновременно порождают новые вызовы в области информационной безопасности. Медицинские данные, содержащие сведения о состоянии здоровья, диагнозах и назначенном лечении, относятся к специальной категории персональных данных (ПДн) и требуют высочайшего уровня защиты. Любая утечка, несанкционированное изменение или фальсификация такой информации может привести не только к серьезным финансовым и репутационным потерям для медицинского учреждения, но и нанести непоправимый вред здоровью и жизни пациента.

В Российской Федерации большинство медицинских организаций для управления документацией используют централизованные системы, среди которых широкое распространение получила платформа «1С: Предприятие» и, в частности, конфигурация «1С: Документооборот». Эти системы эффективно решают задачи регистрации, хранения и маршрутизации документов, но, как и любая централизованная архитектура, они имеют уязвимости. Основные риски связаны с возможностью компрометации данных из-за человеческого фактора (ошибки, злоумышленные действия персонала) или внешних кибератак, а также со сложностью обеспечения неоспоримого аудиторского следа, подтверждающего неизменность документа с момента его создания.

Проблемы правового регулирования ЭДО в государственном управлении, в том числе в подведомственных Минздраву России учреждениях, усугубляют эти риски. Несмотря на

наличие Федерального закона № 63-ФЗ «Об электронной подписи» и Федерального закона № 149-ФЗ «Об информации, информационных технологиях и о защите информации», сохраняется правовая неопределенность в вопросах использования современных технологий, таких как блокчейн, для обеспечения юридической значимости документов. Отсутствие прямого регулирования распределенных реестров в медицинском ЭДО создает дополнительные барьеры для их внедрения [1, с. 45].

В этом контексте технология блокчейн, или распределенного реестра, представляет собой перспективный инструмент для кардинального повышения уровня доверия и безопасности в медицинском документообороте [2]. Ее ключевые свойства – децентрализация, криптографическая защита, прозрачность и неизменность записей – позволяют создать надежный слой верификации поверх существующих информационных систем. Интеграция блокчейна с «1С: Документооборот» может обеспечить криптографически подтвержденную гарантию целостности и подлинности каждого документа, от согласия пациента на обработку ПДн до истории болезни.

Однако внедрение такой инновационной технологии сопряжено не только с техническими, но и со значительными юридическими сложностями. Необходимо обеспечить полное соответствие предлагаемого решения требованиям российского законодательства, в первую очередь Федерального закона № 152-ФЗ «О персональных данных», который накладывает строгие обязательства на операторов ПДн. Главной правовой коллизией является противоречие между фундаментальным свойством неизменности блокчейна и закрепленным в законе «правом на забвение», то есть правом субъекта требовать удаления своих данных [3].

Целью данной статьи является разработка комплексной модели внедрения технологии блокчейн в медицинских учреждениях на базе системы «1С:Документооборот», включающей как технические архитектурные решения, так и предложения по юридическому оформлению для минимизации правовых рисков и обеспечения соответствия нормативным требованиям, с учетом современных проблем регулирования ЭДО в управлении медицинским учреждением.

1. Техническая реализация: гибридная архитектура «1С + Блокчейн».

Полная замена проверенной и функциональной системы «1С: Документооборот» на децентрализованное приложение нецелесообразна ни с экономической, ни с операционной точки зрения. Наиболее эффективным подходом является создание гибридной архитектуры, в которой централизованная система и децентрализованный реестр дополняют друг друга, используя сильные стороны каждой из технологий.

1.1. Концепция и принципы работы

Основная идея гибридной модели заключается в разделении функций:

- «1С: Документооборот» остается основной системой для оперативной работы с документами: их создания, редактирования, согласования, хранения и поиска. В ней хранятся сами документы, содержащие персональные данные пациентов.

- Блокчейн-платформа выступает в роли независимого и неизменяемого «нотариуса» или регистратора событий. В блокчейн записываются не сами документы, а их метаданные и криптографические отпечатки (хэши), которые служат доказательством существования документа в определенном виде в конкретный момент времени.

Такой подход позволяет решить ключевую юридическую проблему: поскольку сами персональные данные не хранятся в блокчейне, требование «права на забвение» выполняется путем удаления соответствующей записи из базы данных 1С. При этом хэш-запись в блокчейне остается, но она не содержит ПДн и лишь подтверждает, что документ с такими атрибутами когда-то существовал, что важно для аудита и разрешения споров.

Процесс работы в такой гибридной системе выглядит следующим образом:

1. Создание документа: врач или другой сотрудник создает в «1С: Документооборот» документ (например, протокол осмотра или согласие на медицинское вмешательство).

2. Хэширование: в момент сохранения и регистрации документа система «1С» автоматически вычисляет его криптографический хэш (уникальный цифровой отпечаток файла, например, по алгоритму SHA-256). Хэш – это

уникальная строка символов фиксированной длины, которая меняется даже при незначительном изменении исходного файла.

3. Формирование транзакции: система формирует транзакцию для записи в блокчейн. Транзакция включает хэш документа, временную метку, идентификатор пользователя, создавшего запись, и тип операции (создание, подписание, изменение). Критически важным является подписание этой транзакции усиленной квалифицированной электронной подписью (УКЭП) сотрудника, которая по закону придает действию юридическую силу, равную собственноручной подписи, что придает юридическую значимость действию и связывает его с конкретным лицом. Принципы использования ЭЦП сотрудниками должны быть строго регламентированы внутренними документами ЛПУ [4].

4. Запись в блокчейн: через специализированный программный интерфейс (API) транзакция отправляется в узел блокчейн-сети, где после валидации включается в новый блок, навсегда фиксируя событие в распределенном реестре.

5. Верификация документа: в любой момент времени можно проверить подлинность и неизменность документа. Для этого достаточно заново вычислить хэш текущей версии файла в 1С и сравнить его с хэшем, записанным в блокчейне для соответствующего документа. Если хэши совпадают, документ подлинен и не подвергался изменениям. Если нет – была совершена попытка фальсификации.

2.2. Выбор блокчейн-платформы и архитектурные особенности

Для корпоративного использования в медицинских учреждениях оптимальным выбором являются частные (permissioned) блокчейн-платформы. В отличие от публичных блокчейнов (таких как Bitcoin), доступ к участию в таких сетях контролируется, что обеспечивает конфиденциальность и соответствует корпоративным стандартам. К таким платформам относятся, например, Hyperledger Fabric, Corda или Exonum. Их ключевые преимущества для данной задачи:

- Контроль доступа: участниками сети могут быть только авторизованные узлы (серверы), принадлежащие медицинскому учреждению или, в перспективе, консорциуму клиник и регуляторов. Это обеспечивает высокий уровень конфиденциальности.

- Высокая производительность: частные блокчейны способны обрабатывать значительно большее количество транзакций в секунду по сравнению с публичными, что критически важно для интенсивного документооборота крупной клиники.

- Гибкость управления: администраторы сети могут гибко настраивать правила консенсуса и управления данными.

Интеграция «1С: Документооборот» с блокчейн-платформой потребует разработки специального коннектора (шлюза) – программного модуля, который будет отвечать за:

- Перехват ключевых событий в 1С (создание, подписание документа).

- Вычисление хэшей и формирование транзакций.

- Взаимодействие с API блокчейн-узла для отправки транзакций.

- Предоставление интерфейса для верификации документов путем запроса данных из блокчейна.

Безопасность системы в целом будет зависеть от надежности управления криптографическими ключами. Каждый пользователь, имеющий право подписывать документы (врачи, руководители), должен обладать своим уником закрытым ключом, который используется для подписания транзакций, отправляемых в блокчейн. Это позволяет однозначно идентифицировать автора каждого действия. Использование УКЭП в связке с блокчейном может придать записям максимальную юридическую значимость.

2. Юридическое оформление и соответствие законодательству РФ

Внедрение блокчейн-технологии требует тщательной юридической проработки для минимизации рисков и избежания штрафов со стороны надзорных органов, в первую очередь Роскомнадзора. Медицинское учреждение, как оператор персональных данных, несет полную ответственность за их надлежащую обработку и защиту.

2.1. Соответствие Федеральному закону № 152-ФЗ «О персональных данных»

Основная задача – вписать новую технологию в существующее правовое поле. Предлагаемая гибридная архитектура с хранением

хэшей (а не самих ПДн) в блокчейне является ключевым элементом для обеспечения соответствия ФЗ-152.

- «Право на забвение» (ст. 14, 21 ФЗ-152): Как уже отмечалось, требование об удалении ПДн по запросу субъекта (так называемое «право на забвение») выполняется путем их стирания из базы данных 1С. Хэш в блокчейне не является персональными данными, так как из него невозможно восстановить исходную информацию. Он лишь служит доказательством факта, не раскрывая содержания.

- Локализация баз данных (ч. 5 ст. 18 ФЗ-152): Закон требует, чтобы базы данных, содержащие ПДн граждан РФ, находились на территории России. Это требование легко выполняется, так, как и серверы 1С, и узлы частной блокчейн-сети будут физически размещаться в дата-центрах медицинского учреждения на территории РФ.

- Согласие на обработку ПДн (ст. 9 ФЗ-152): Форму согласия на обработку ПДн необходимо будет дополнить пунктом, информирующим пациента о том, что для подтверждения целостности и подлинности его медицинской документации используются технологии распределенного реестра (блокчейн), при этом его персональные данные в самом реестре не хранятся. Получение такого информированного согласия является обязательным.

Факт получения и отзыва согласия также должен фиксироваться в блокчейне. Это создает неоспоримое доказательство волеизъявления пациента, защищая клинику от претензий, связанных с незаконной обработкой данных.

2.2. Придание юридической значимости записям в блокчейне и проблемы регулирования ЭДО.

Чтобы записи в блокчейне могли быть использованы в качестве доказательств в суде или при проверках, необходимо придать им юридическую силу. Это достигается комбинацией технических и организационных мер:

- Использование электронной подписи: В соответствии с Федеральным законом № 63-ФЗ «Об электронной подписи», документы, подписанные УКЭП, признаются равнозначными бумажным документам, подписанным собственноручно. Транзакции, отправляемые в блокчейн, должны быть подписаны УКЭП ответственного сотрудника. Это связывает запись в реестре с конкретным, идентифицированным лицом. Однако на текущий момент отсутствует прямая норма, признающая блокчейн-запись, подписанную УКЭП, самостоятельным электронным документом. Поэтому юридическая сила достигается за счет того, что запись является неотъемлемой частью аудиторского следа документа, хранящегося в 1С, который, в свою очередь, подписан УКЭП. Данный подход находит поддержку в профессиональном сообществе [5].

- Внутренние нормативные акты: Легитимность использования технологии должна быть закреплена во внутренних документах организации.

2.3. Предложения по комплекту юридических документов для внедрения

Для юридически корректного внедрения системы «1С + Блокчейн» руководителю медицинского учреждения необходимо инициировать разработку и утверждение следующего пакета документов:

1. Приказ о внедрении системы электронного документооборота с использованием технологии распределенного реестра. Этот документ официально запускает проект и назначает ответственных лиц.

2. Положение об электронном документообороте. В существующее или новое положение необходимо внести разделы, описывающие:

- архитектуру гибридной системы;
- порядок работы с документами, целостность которых подтверждается блокчейном;
- процедуру верификации подлинности документов;
- статус записей в блокчейне как неотъемлемой части аудиторского следа документа.

3. Изменения в Политику обработки персональных данных. Документ должен быть дополнен информацией о применении технологии блокчейн для фиксации хэшей документов, с явным указанием на то, что сами ПДн в реестре не хранятся.

4. Регламент управления криптографическими ключами и средствами электронной подписи. Этот документ определяет порядок выдачи, хранения, использования и отзыва ключей УКЭП сотрудниками, а также ответственность за их компрометацию. Он должен быть синхронизирован с принципами защиты

информации, изложенными в актах законодательной инициативы, касающихся безопасности критической информационной инфраструктуры (КИИ).

5. Обновленная форма согласия на обработку персональных данных. Как упоминалось выше, форма должна содержать пункт о применении технологии распределенного реестра.

6. Должностные инструкции. В инструкции сотрудников, работающих в системе, необходимо внести обязанности и ответственность, связанные с использованием новой технологии.

Разработка и внедрение этих документов не только обеспечат соответствие законодательству, но и создадут прозрачные и понятные правила работы для всего персонала, что снизит риски человеческого фактора.

3. Преимущества и риски внедрения

Внедрение гибридной системы «1С + Блокчейн» открывает для медицинского учреждения ряд стратегических преимуществ, но также сопряжено с определенными рисками, которыми необходимо управлять.

3.1. Преимущества для медицинского учреждения

- Снижение юридических рисков и предотвращение штрафов: обеспечение криптографически доказуемой целостности медицинских записей и согласий пациентов значительно укрепляет правовую позицию клиники в случае судебных споров или проверок Роскомнадзора.

- Повышение уровня информационной безопасности: неизменность блокчейна делает практически невозможной незаметную фальсификацию или удаление данных задним числом, что защищает от внутреннего и внешнего мошенничества.

- Усиление доверия со стороны пациентов: демонстрация использования передовых технологий для защиты чувствительных данных повышает репутацию учреждения и его привлекательность для пациентов, заботящихся о конфиденциальности.

- Оптимизация аудита: процесс внутреннего и внешнего аудита документооборота становится значительно проще, быстрее и прозрачнее. Проверка подлинности любого документа сводится к простой сверке хэшей.

- Создание основы для будущего взаимодействия: внедренная блокчейн-инфраструктура может в будущем использоваться для безопасного обмена данными с другими клиниками (с согласия пациента), страховыми компаниями и государственными органами, создавая единое доверенное пространство.

3.2. Потенциальные риски и пути их минимизации

- Технологические риски: сложность интеграции, возможные ошибки в коде коннектора.

- Минимизация: привлечение квалифицированных разработчиков с опытом в области блокчейн-технологий, проведение тщательного тестирования, включая нагрузочное и тестирование на проникновение.

- Операционные риски: неправильное использование системы персоналом, утеря или компрометация криптографических ключей.

- Минимизация: разработка подробных инструкций и регламентов, проведение регулярного обучения персонала, внедрение строгих процедур управления ключами УКЭП.

- Финансовые риски: высокая стоимость разработки, внедрения и поддержки системы.

- Минимизация: проведение детального технико-экономического обоснования проекта, поэтапное внедрение (начиная с пилотного проекта в одном отделении), рассмотрение возможности использования готовых платформенных решений.

- Регуляторные риски: неопределенность в законодательстве и возможное появление новых нормативных требований к технологии блокчейн.

- Минимизация: постоянный мониторинг изменений в законодательстве, консультации с профильными юристами, построение гибкой архитектуры, которую можно будет адаптировать под новые требования. Активное участие в публичных обсуждениях законопроектов на https://regulation.gov.ru/.

Заключение

Интеграция технологии блокчейн с существующей системой «1С: Документооборот» представляет собой реалистичный и эффективный путь для повышения уровня защиты персональных данных и обеспечения юридической значимости электронного документооборота в медицинских учреждениях. Предложенная гибридная модель, основанная на

хранении в блокчейне только криптографических хэшей, а не самих данных, позволяет использовать ключевые преимущества децентрализованных систем – неизменность и прозрачность аудита – при одновременном соблюдении строгих требований российского законодательства в области защиты персональных данных, включая «право на забвение».

Успешное внедрение такого проекта требует комплексного подхода, сочетающего глубокую техническую проработку и тщательное юридическое оформление с учетом существующих проблем регулирования ЭДО в госуправлении. Разработка и утверждение пакета внутренних нормативных актов, регламентирующих использование новой технологии и принципы работы с ЭЦП сотрудников, является обязательным условием для ее легитимации и минимизации правовых рисков. Несмотря на существующие вызовы, связанные со стоимостью и сложностью внедрения, стратегические выгоды от повышения безопасности, снижения юридических рисков и укрепления доверия пациентов делают инвестиции в подобные технологии оправданными и перспективными. Внедрение блокчейна в медицине способно стать фундаментом для создания более эффективных, безопасных и прозрачных систем здравоохранения будущего.

Библиографический список

1. Петров А.В., Смирнова И.К. Правовые проблемы использования технологий распределенного реестра в государственном и муниципальном управлении // Право и цифровая экономика. – 2022. – № 4. – С. 44--52.

2. Ковалев С.Н., Орлова Д.С. Блокчейн как инструмент обеспечения доверия в электронном здравоохранении // Международный журнал экспериментального образования. – 2021. – № 4. – С. 25-29.

3. Абрамова М.А. Право на забвение vs неизменяемость блокчейна: пути разрешения коллизии. Информационное право. – 2020. – № 3. – С. 12-16.

4. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи». – [Электронный ресурс]. – Режим доступа: http://pravo.gov.ru.

5. Белов А.Ю. Электронный документ и электронная подпись: новые вызовы и решения // Доклад на XI Международной конференции «Право в цифровую эпоху». – 2023.

INTEGRATION OF BLOCKCHAIN TECHNOLOGY INTO MEDICAL DOCUMENT MANAGEMENT BASED ON "1C: DOCUMENT MANAGEMENT": TECHNICAL AND LEGAL ASPECTS OF PERSONAL DATA PROTECTION IN THE CONTEXT OF LEGAL REGULATION

D.E. Rabotaev, *Student[1], Head of the Contract Service[2]*
[1]Ural State University of Economics
[2]Federal Center for Medical Nanotechnology of the FMBA of Russia
[1](Russia, Ekaterinburg)
[2](Russia, Moscow)

Abstract. *The article discusses a comprehensive approach to the implementation of blockchain technology in the electronic document management system of medical institutions operating on the "1C: Document Management" platform. The key technical aspects of a hybrid architecture are analyzed, in which the centralized 1C system is supplemented by a decentralized registry for recording legally significant events and ensuring data immutability. Particular attention is paid to the legal challenges associated with the protection of patients' personal data in accordance with Federal Law № 152-FL "On Personal Data", as well as the problems of legal regulation of EDM in public administration in relation to the healthcare sector. Specific legal and organizational mechanisms for the legalization of the technology are proposed, including the development of internal regulations and the resolution of the conflict between the immutability of the blockchain and the "right to be forgotten". The article is addressed to heads of medical institutions and lawyers interested in improving the level of data protection and optimizing document flow in the context of digital transformation.*

Keywords: *blockchain, 1C: Document Management, healthcare, personal data, Federal Law № 152-FL, electronic document management, information security, electronic signature, legal regulation, hybrid architecture.*