DOI 10.58351/2949-2041.2026.35.6.030
УДК 614.2:004.89:351.77

Техов Артур Сосланович
магистрант кафедры информационных технологий и систем,
Северо-Кавказский горно-металлургический институт
Государственный технологический университет

ПРИМЕНЕНИЕ БЛОКЧЕЙН-ТЕХНОЛОГИЙ ДЛЯ ЗАЩИТЫ МЕДИЦИНСКИХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ЗДРАВООХРАНЕНИЯ

Аннотация. В статье рассматриваются возможности применения блокчейн-технологий для обеспечения безопасности медицинских данных в современных информационных системах здравоохранения. Выполнен анализ существующих проблем хранения и обработки медицинской информации, связанных с обеспечением конфиденциальности, целостности и доступности данных. Рассмотрены преимущества использования распределенного реестра, смарт-контрактов и механизмов децентрализованного хранения информации. Показаны перспективы внедрения блокчейн-технологий для повышения уровня информационной безопасности медицинских организаций.

Ключевые слова: Блокчейн, медицинские данные, информационная безопасность, медицинская информационная система, электронная медицинская карта, смарт-контракт, управление доступом, распределенный реестр.

В настоящее время цифровизация здравоохранения сопровождается активным внедрением медицинских информационных систем, обеспечивающих хранение и обработку значительных объемов данных о пациентах. Использование электронных медицинских карт позволяет повысить эффективность медицинского обслуживания, ускорить обмен информацией между медицинскими учреждениями и улучшить качество принимаемых решений. Однако вместе с преимуществами цифровизации возникают новые угрозы информационной безопасности, связанные с несанкционированным доступом к данным пациентов, утечками конфиденциальной информации и возможностью изменения медицинских записей.

Традиционные медицинские информационные системы в большинстве случаев используют централизованные базы данных. Несмотря на широкое распространение такого подхода, он имеет ряд недостатков. Централизованное хранение информации создает единую точку отказа, а также увеличивает риск компрометации данных в случае успешной атаки на серверную инфраструктуру.

Одним из перспективных направлений решения указанных проблем является использование технологии блокчейн. Блокчейн представляет собой распределенный реестр, в котором информация хранится в виде последовательности связанных между собой блоков. Каждый новый блок содержит криптографическую ссылку на предыдущий, что обеспечивает целостность всей цепочки данных и делает невозможным скрытое изменение информации.

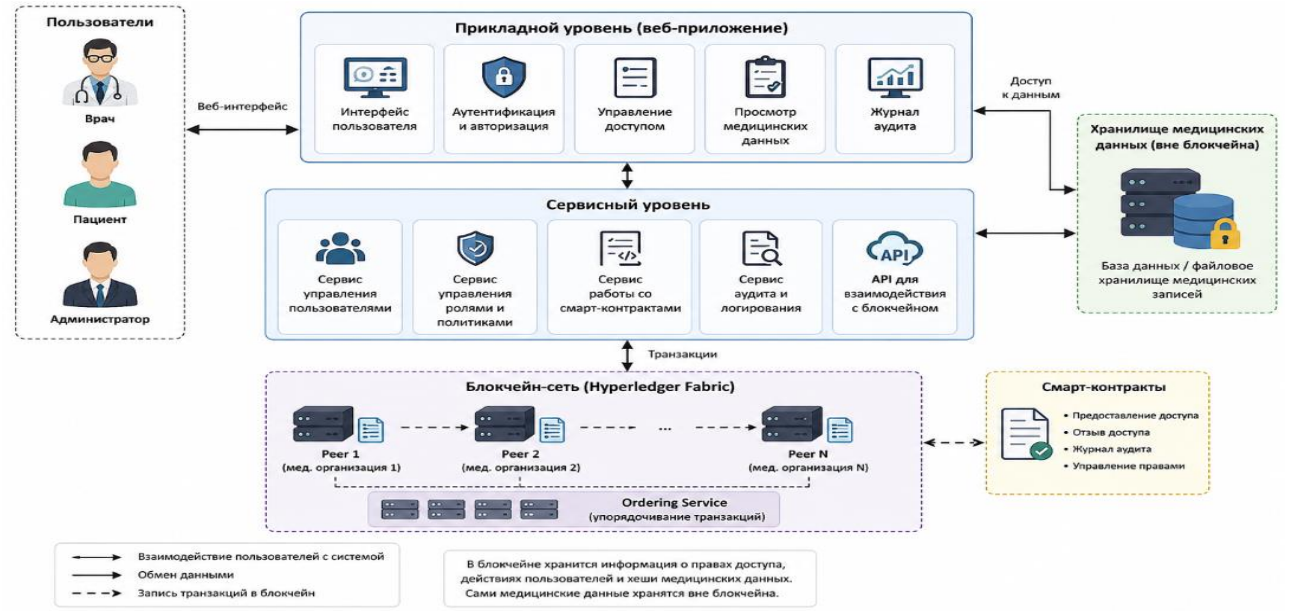


Рис. 1. Архитектура системы защиты медицинских данных
на основе блокчейн-технологий

Применение блокчейна позволяет обеспечить прозрачность операций доступа к медицинской информации. Каждое действие пользователя может регистрироваться в распределенном реестре в виде отдельной транзакции. Благодаря этому появляется возможность формирования неизменяемого журнала аудита, который может использоваться для контроля соблюдения требований информационной безопасности и расследования инцидентов.

Дополнительным преимуществом блокчейн-технологий является возможность использования смарт-контрактов. Смарт-контракт представляет собой программный код, автоматически выполняющий определенные действия при наступлении заранее установленных условий. В медицинских информационных системах смарт-контракты могут использоваться для управления доступом к электронным медицинским картам пациентов. Например, доступ к данным может предоставляться врачу только после подтверждения соответствующего запроса владельцем информации.

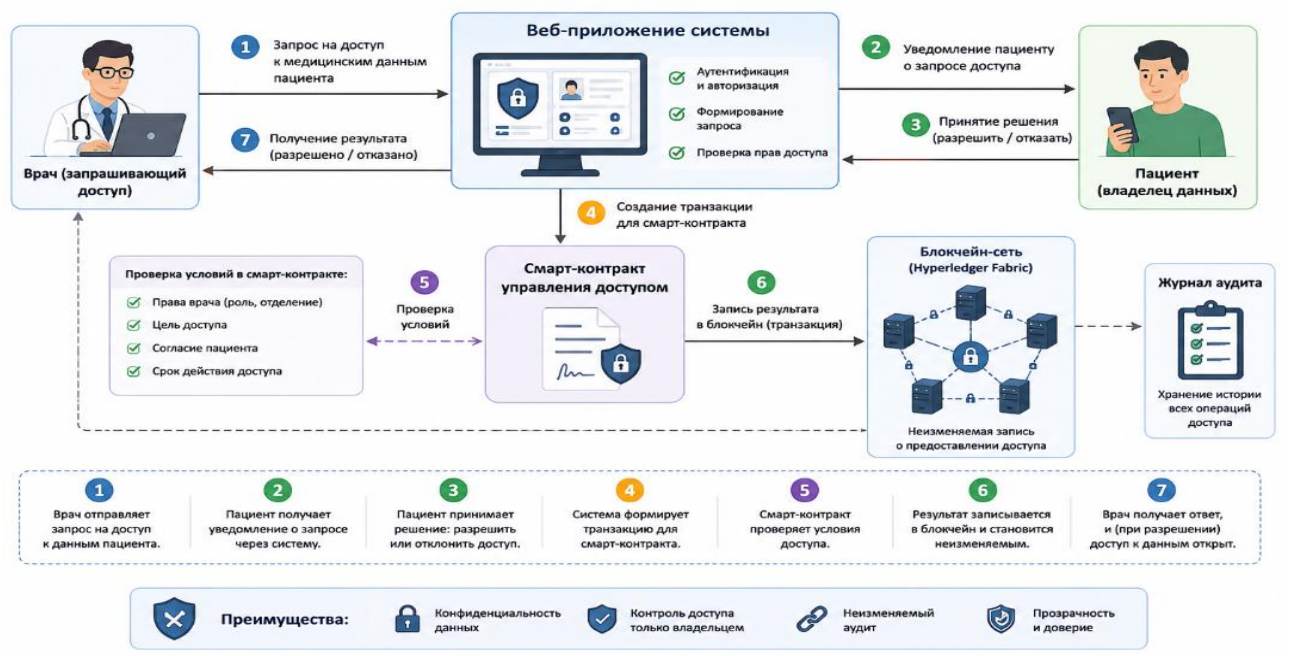
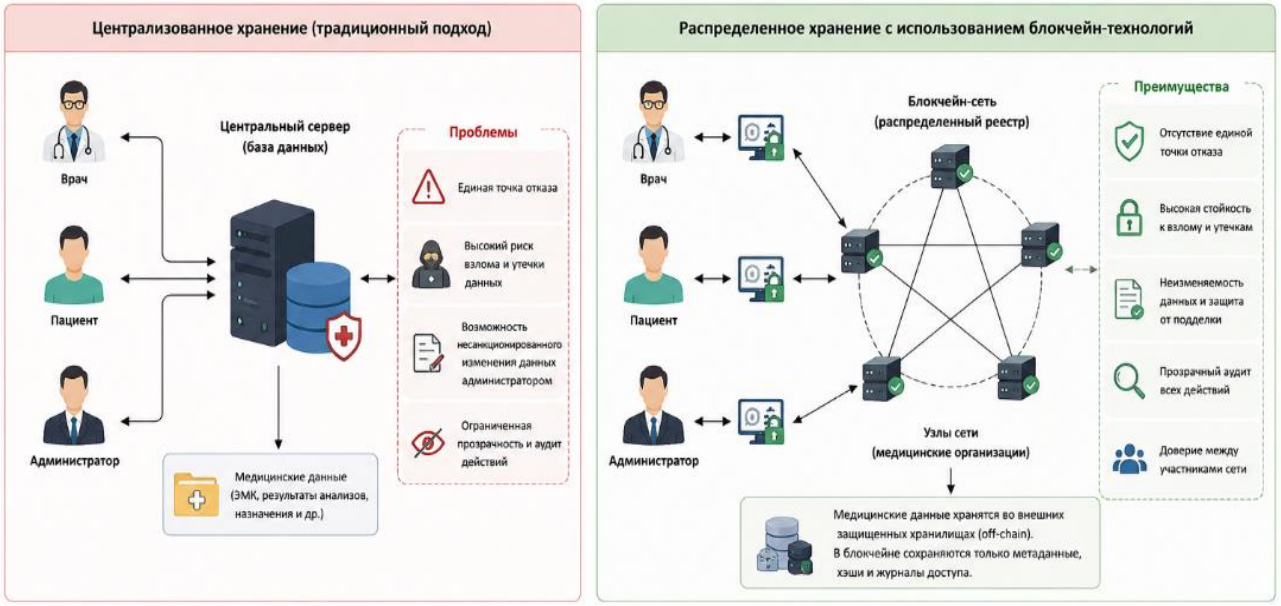


Рис. 2. Процесс предоставления доступа к медицинским данным
с использованием смарт-контракта

Важным преимуществом применения смарт-контрактов является автоматизация процессов принятия решений и исключение человеческого фактора при управлении доступом. Все правила предоставления и отзыва разрешений фиксируются в коде контракта и выполняются автоматически. Это позволяет снизить вероятность ошибок администрирования и повысить уровень доверия пользователей к системе.

Для реализации медицинских информационных систем наиболее перспективным считается использование платформы Hyperledger Fabric. Данная платформа относится к категории разрешенных блокчейн-сетей и предоставляет механизмы идентификации участников, разграничения прав доступа и поддержки конфиденциальных каналов обмена информацией. Благодаря этому обеспечивается соответствие требованиям законодательства в области защиты персональных данных и медицинской информации.

Следует отметить, что использование блокчейна не предполагает обязательного хранения всех медицинских записей непосредственно в распределенном реестре. Наиболее рациональным является гибридный подход, при котором медицинские данные размещаются в специализированной базе данных, а блокчейн используется для хранения информации о правах доступа, транзакциях и действиях пользователей. Такой подход позволяет сохранить высокую производительность системы и одновременно обеспечить надежный аудит операций.



Критерий	Централизованное хранение	Распределенное хранение (блокчейн)
Безопасность	✗ Высокие риски взлома и утечки данных	✓ Высокая безопасность и отказоустойчивость
Управление доступом	✗ Зависит от администратора системы	✓ Автоматизация через смарт-контракты
Прозрачность и аудит	✗ Ограниченный и изменяемый аудит	✓ Неизменяемый и прозрачный журнал действий
Надежность	✗ Единая точка отказа	✓ Данные распределены между узлами сети
Стоимость	~ Ниже на начальном этапе	~ Выше на этапе внедрения, ниже в долгосрочной перспективе
Соответствие требованиям	~ Зависит от качества системы	✓ Упрощает выполнение требований регуляторов

Рис. 3. Сравнение централизованного
и распределенного хранения медицинских данных

Таким образом, применение блокчейн-технологий открывает новые возможности для повышения уровня безопасности медицинских информационных систем. Использование распределенного реестра обеспечивает прозрачность и неизменяемость данных, а смарт-контракты позволяют автоматизировать процессы управления доступом к медицинской информации. Внедрение подобных решений способствует повышению доверия пользователей к цифровым сервисам здравоохранения и создает основу для дальнейшего развития современных медицинских информационных систем

Список литературы:

1. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. – 2008.
2. Androulaki E., Barger A., Bortnikov V. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains // EuroSys. – 2018.
3. Yue X., Wang H., Jin D., Li M., Jiang W. Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control // Journal of Medical Systems. – 2016.
4. Agbo C.C., Mahmoud Q.H., Eklund J.M. Blockchain Technology in Healthcare: A Systematic Review // Healthcare. – 2019.
5. Kuo T.T., Kim H.E., Ohno-Machado L. Blockchain Distributed Ledger Technologies for Biomedical and Health Care Applications // Journal of the American Medical Informatics Association. – 2017.
6. Таненбаум Э., Уэзеролл Д. Компьютерные сети. – СПб.: Питер, 2021.
7. Гаврилов А.В. Информационная безопасность медицинских информационных систем. – М.: Инфра-М, 2022