УДК 004.942:519.23/.25 Вестник УрФО № 3(53) / 2024, с. 14–25

Коренев Д. А., Захаров А. А., Ханбеков Ш. И. 10.14529/secur240302

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН ДЛЯ СОЗДАНИЯ ДОПОЛНИТЕЛЬНОГО СЕРВИСА К МИС, РАБОТАЮЩЕЙ С УСТРОЙСТВАМИ ИНТЕРНЕТА МЕДИЦИНСКИХ ВЕЩЕЙ

В статье предлагается оригинальный подход для работы врачей с медицинской информацией в домашних медицинских стационарах, позволяющий получить общую картину лечебных мероприятий, проводимых с пациентом в медицинских учреждениях города. Для доступа к медицинской информации о пациенте в больницах и поликлиниках города предлагается использовать дополнительную Блокчейн базу (блокчейн из блокчейнов) в качестве распределенного безопасного информационного хранилища актуальных медицинских данных из независимых информационных систем городских поликлиник, стационаров и домашних стационаров. Представлена архитектура хранилища, описаны структуры хранения данных и предложен псевдокод для создания блокчейна с возможностью добавления информации. Описан прототип системы, включающий сервисы для поиска, получения и обработки информации. Приводятся результаты вычислительных экспериментов, позволяющие оценить производительность прототипа системы. Описан API для работы с Блокчейн базой, использующий в том числе голосового помощника с учетом необходимых требований по защите конфиденциальной медицинской информации.

Ключевые слова: *информационная безопасность, интернет вещей, блокчейн, медицинская информационная система, телемедицина*

THE USE OF BLOCKCHAIN TECHNOLOGY TO CREATE AN ADDITIONAL SERVICE TO THE MIS WORKING WITH THE INTERNET OF MEDICAL THINGS DEVICES

The article suggests an original approach for doctors to work with medical in-formation in home medical hospitals, which allows to get an overall picture of the therapeutic measures carried out with the patient in medical institutions of the city. To access medical information about a patient in hospitals and polyclinics of the city, it is proposed to use an additional Blockchain database (blockchain from blockchains) as a distributed secure information repository of up-to-date medical data from independent information systems of urban polyclinics, hospitals and home hospitals. The architecture of the storage is presented, data storage structures are described and a pseudocode for creating a blockchain with the ability to add information is proposed. A prototype of the system is described, including services for searching, receiving and processing information. The results of computational experiments are presented to evaluate the performance of the prototype system. The API for working with the Blockchain database is described, including using a voice assistant, taking into account the necessary requirements for the protection of confidential medical information.

Keywords: *Information security, Internet of Things, Blockchain, Medical In-formation System, Telehealth*

Для понимания значения и чувствительности медицинской информации важно учитывать следующие аспекты:

1. Личная конфиденциальность. Медицинская информация содержит чувствительные данные о здоровье, медицинских диагнозах, лечении и истории болезней пациентов. Эти данные могут быть крайне частными и личными, и их неправомерное раскрытие и тем более изменение могут нанести серьезный вред личной жизни и достоинству пациента, а также физиологическому духовному здоровью. Отметим, что данные о пациенте могут находиться в различных городских медицинских организациях в МИС от различных поставщиков.

2. Доверие пациентов. Защита медицинской информации является ключевым фактором для поддержания доверия пациентов к медицинским учреждениям и профессионалам. Пациенты должны быть уверены, что их данные будут обрабатываться и храниться с соблюдением высоких стандартов конфиденциальности и безопасности.

3. Этические соображения. Медицинские данные содержат информацию, которая может быть использована для дискриминации или нанесения вреда пациентам. Защита этой информации важна для соблюдения этических принципов и защиты прав пациентов.

4. Законодательство и нормативные требования. Существующее законо-дательство, регулирующее обработку, передачу и хранение медицинской информации предусматривает штрафы и наказания за нарушение конфиденциальности данных. Понимание этих нормативных требований важно для соблюдения законодательства и минимизации рисков.

5. Безопасность и защита от угроз. Медицинская информация может быть целью злоумышленников, которые могут использовать эту информацию для вымогательства, мошенничества или других противоправных целей.

Поэтому реализация защиты медицинской информации в том числе и от киберугроз имеет важное значение.

Сама по себе идея использования блокчейна в здравоохранении не нова, например, в работе Кузнецова В.П. [1], были рассмотрены перспективы и преимущества использования блокчейна в сфере здравоохранения. В свою очередь более детально подобная проблема рассматривалась Пономарёвым К.Ю. [2], однако в работе рассматривается использование облачного хранилища данных, которое тоже может скомпрометировано. В работе Гончаренко Ю.Ю. [3] рассматривается концепт с подтверждением подлинности медицинских документов при помощи технологии блокчейн, однако упускается момент, при котором в некоторых системах необходимо иметь связь с разнородными данными: тексты, числовые значения, графические снимки, которые также должны иметь гарантию подлинности.

По данной тематике существуют коммерческие продукты от компаний BurstIQ, Guardtime и другими [4-8]. Они решают конкретно поставленную за-дачу хранения данных в медицинских информационных системах (МИС). Guardtime использует проприетарный блокчейн, BurstIQ в свою очередь придерживается использования открытых технологий и использует технологию блокчейн для МИС с открытым исходным кодом. В России для Единого депозитария результатов интеллектуальной деятельности (ЕДРИД), Федеральная антимонопольная служба (ФАС) и Сбербанк запустили проект Digital Ecosystem [6-9], где используется технология блокчейн. Проблемы, связанные с использованием МИС в России детально рассматривали Монаков Д.В. и Алтунин Д.В. [7]. Ими выделяется тот факт, что некоторые модули современных МИС зачастую не связаны между собой. Среди востребованных функций внедрение электронных медицинских карт для упрощения работы персонала ЛПУ. Аксенова Е.И. и Гобатов С.Ю. отмечают такие функции как: отслеживание приема лекарств, удаленный мониторинг здоровья, удаленный мониторинг медицинских активов. Однако на основании открытых данных можно сделать вывод, что в большинстве случаев авторы используют просто блокчейн или несколько несвязанных блокчейнов что не позволяет обеспечить хранение разнородных данных.

Прежде, чем предлагать конкретные решения касательно МИС, исполь-зующих блокчейн, надо понимать, что любые значимые данные и обязанности регулируются определенными нормативными актами начиная от конституции РФ заканчивая приказами ФСТЭК России [10-21].

На основании вышеуказанных документов можно определить требования к безопасности систем интернета вещей в сфере здравоохранения:

- Конфиденциальность: только авторизованные пользователи могут получить доступ к данным.
- Целостность: полученные пациентом медицинские данные строго идентичны выданным.
- Аутентификация: процесс, который позволяет медицинскому устройству аутентифицировать и идентифицировать одноранговый узел, с которым оно взаимодействует.
- Доступность: обеспечивает доступность медицинских услуг и устройств Интернета вещей в любое время и в любом месте для авторизованных сторон.
- Неотказуемость: гарантирует, что пользователь или медицинское устройство не сможет отрицать, что является отправителем сообщения.
- Авторизация: гарантирует, что только авторизованная сторона может иметь доступ к данным или иметь разрешение на выполнение определенных задач.

На данный момент в медицинских организациях для осуществления до-машнего стационара преимущественно используются Internet of Medical Things (IoMT) [22]. В таких системах данные о мониторинге пациента передаются в МИС при помощи специальной шины данных. Для передачи данных преимущественно используют такие протоколы, как Message Queuing Telemetry Transport (MQTT), Java Message Service (JMS), eXtensible Messaging and Presence Protocol (XMPP), Advanced Message Queuing Protocol (AMQP), Data Distribution Service (DDS), Constrained Application Protocol (CoAP) [23]. Некоторые из этих протоколов, например, DDS и CoAP, используют UDP, что не гарантирует отправку сообщения что может привести к потере данных при нестабильном соединении, при этом протоколы MQTT, AMQP, XMPP, JMS и при определенной конфигурации DDS используют TCP. Важно отметить, что отправка сообщения не гарантируется, в том случае, когда сервер, на который происходит отправка недо-

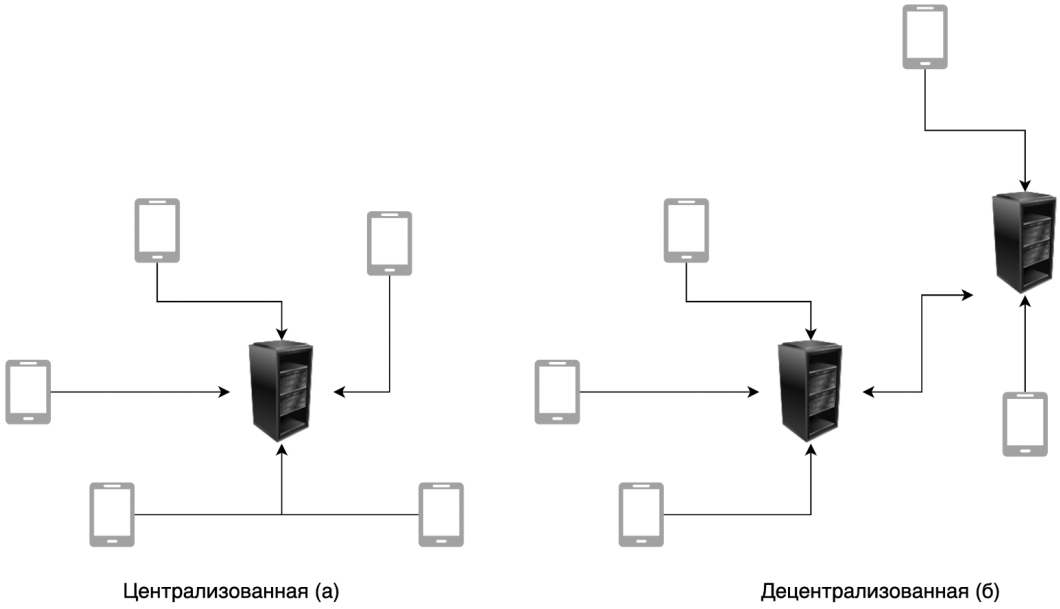

Рис. 1. Подходы к созданию систем. На рисунке (а) архитектура централизованной системы, на рисунке (б) архитектура децентрализованной системы

ступен. Для таких протоколов как CoAP можно использовать несколько серверов для отправки. В этом случае, если один сервер окажется недоступен, будет использован резервный сервер, на который можно отослать данные. Однако разработчикам таких систем необходимо учитывать каким образом сохранять данные для последующего анализа. Определение дублирующих данных также является проблемой, так как данные с IoMT могут прийти в разное время, в зависимости от задержки сети, например, с промежутком в 5 секунд, что может быть критичным.

Существует несколько подходов к созданию систем: централизованный, который применяется в большинстве случаев в МИС, и децентрализованный, они представлены на рис. 1.

Одной из проблем централизованных систем является стоимость, которая необходима для их расширения [24-27], так как в больших информационных системах необходимо тратить дополнительные ресурсы на балансировку нагрузки и синхронизацию баз данных. Распределенные системы могут использовать преимущества централизованной базы данных, особенно при совместном использовании данных. В случае сбоя распределенные системы подвержены меньшему воздействию, чем централизованные, если какой-либо узел в распределенной системе выходит из строя, система не прекратит свое функционирование, так как будут другие узлы для взаимодействия. Топология сети, коммуникационное программное обеспечение и характер распределенных данных являются основными параметрами, влияющими на работу и эффективность распределенной системы. В системе распределенных баз данных используются сложные методы управления данными для решения проблем, связанных с целостностью данных и параллелизмом. Поскольку данные расположены и репли-цируются в разных местах, то это может привести к несогласованности данных при каждом изменении данных в определенном месте.

Блокчейн – это технология, которая позволяет записывать и обмениваться общими данными по распределенной сети. Данные хранятся в неизменяемых "блоках", которые последовательно соединены друг с другом. Каждый блок содержит свой собственный хэш и хэш предыдущего блока, что обеспечивает целостность данных. Блокчейн масштабируем и обладает такой же децентрализацией, как и IoT. Существуют различные типы блокчейнов:

• Публичный – блокчейн, к которому может присоединиться любой пользователь. Он может считывать данные, обновлять и записывать новые, что позволяет публичному

блокчейну сохранять свой самоуправляемый характер. Недостатком являются высокие энергозатраты при увеличении числа участников.

• Приватный блокчейн, допускаются только верифицированные участ-ники с авторизацией или подтвержденным приглашением. Это позволяет использовать согласованный протокол и вести общий реестр.

• Блокчейн на основе разрешений – комбинация публичного и частного блокчейнов с возможностью дальнейшей настройки ролей.

Медицинские приложения требуют взаимодействия только с идентифи-цированными и прошедшими аутентификацию устройствами. Подходит как приватный блокчейн, так и блокчейн, основанный на разрешениях.

Смарт контракт является одним из ключевых инновационных элементов технологии блокчейн. Он представляет собой программный код, который выполняются автоматически при определенных условий, описанных в контракте. Смарт контракты обеспечивают автоматизацию и безопасность сделок без участия посредников. В здравоохранении смарт контракты могут повысить и эффективность, и прозрачность процессов в сфере медицинских услуг и управления медицинскими данными. Например, с помощью смарт контрактов можно автоматизировать процессы страхования здоровья, управления медицинскими досье и рецептами, а также оплаты медицинских услуг. Одним из примеров использования смарт контрактов в здравоохранении, может быть, система управления медицинскими данными пациентов. С помощью смарт контрактов можно создать защищенную и прозрачную цифровую базу данных, в которой будут храниться медицинские записи пациентов. Доступ к этим данным можно предоставлять только авторизованным лицам, что обеспечит конфиденциальность информации.

Кроме того, смарт контракты могут упростить процессы взаимодействия между различными участниками системы здравоохранения, такими как пациенты, врачи, страховые компании и административные органы. Например, с помощью смарт контрактов можно автоматизировать процесс оплаты медицинских услуг между страховыми компаниями и медицинскими учреждениями на основе предоставленных данных о выполненных процедурах и лечении. Поскольку данные поступают в режиме реального времени, смарт контракты могут автоматически обновлять отчеты и справки о состоянии здоровья. Это особенно полезно для хронически больных пациентов, которым необходимо регулярное обновление данных для корректировки лечения. Длительность разработки смарт контрактов зависит от требований, чем они сложнее, тем дольше придется разрабатывать смарт контракт, а также от того какая база блокчейна используется, является ли это уже закрепившимся решением, таким как Etherium или это что-то оригинальное.

Таким образом, смарт контракты имеют огромный потенциал для улуч-шения качества и доступности здравоохранения. Их внедрение может способствовать повышению эффективности процессов, снижению издержек и улуч-шению качества медицинского обслуживания, за счет упрощения коллаборации, с научно-исследовательскими институтами, создании персональных пла-нов лечения. В будущем использование смарт контрактов в здравоохранении может стать стандартной практикой, что приведет к созданию более эффективной и безопасной системы здравоохранения.

Стоит обратить внимание, что для обработки потоковых данных (например, данных ЭКГ) для блокчейна требуются дополнительные модификации, которые позволяют работать с цепочками одновременных данных от одного пациента. Такой подход позволяет предоставлять определенные данные в отдельных цепочках в общем потоке.

Блокчейн предлагается использовать для дублирования данных из базы данных, если такая база уже есть у МИС. Использование блокчейна позволяет хранить данные в облачном хранилище провайдера, а также обеспечить уско-рение процессов взаимодействия и принятия решений. В условиях домашнего стационара оперативное взаимодействие между пациентами, врачами и другими участниками системы крайне важно. Блокчейн может значительно ускорить обмен данными и принятие решений за счет автоматизации процессов через смартконтракты. Например, когда состояние пациента меняется, соответствующие данные могут быть автоматически переданы врачу для немедленного анализа и корректировки лечения. Кроме того, смартконтракты могут быть использованы для автоматизации процедур страхования, обеспечивая быстрое и точное возмещение затрат на медицинские услуги. Также это позволяет обеспечить поддержку интероперe-

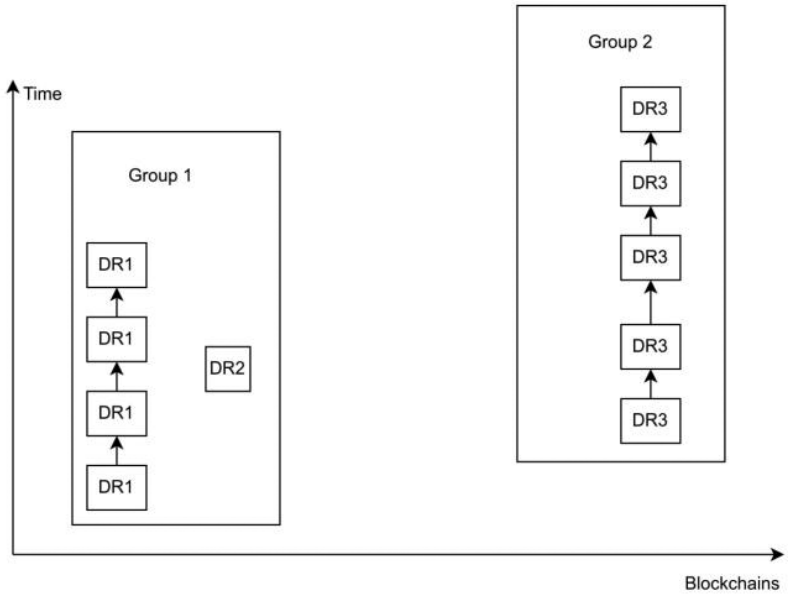

Рис. 2. Архитектура хранения данных в блокчейне

рабельности и стандартизации данных, так как медицинские данные, поступающие из различных устройств и систем, часто имеют разнородные форматы и стандарты. Это особенно актуально для домашнего стационара, где данные могут поступать от различных производителей медицинских устройств. Блокчейн позволяет унифицировать процесс сбора и обработки данных, что упрощает их интеграцию и последующий анализ. В результате врачи получают доступ к более точной и структурированной информации, что способствует повышению качества лечения.

Для хранения данных предлагается использовать блокчейн-блокчейнов, где в каждом блокчейне будут храниться данные по каждому пациенту, таким образом увеличивая консистентность данных. Схема хранения данных представлена на рис. 2.

На рис. 3 представлена архитектурная схема МИС с использованием блокчейн. На схеме, мобильные устройства отражают устройства, используемые в рамках домашнего стационара, они передают данные в блокчейн в свою медицинскую организацию. Архитектура состоит из нескольких каналов связи (Channel 1, Channel 2, Channel 3 и других), каждый из которых объединяет несколько блокчейн-менеджеров, которые привязаны к определенным медицинским учреждениям, которые объединены в единую сеть для обмена информацией между собой. Блокчейн-менеджеры представляют собой узлы, ответственные за управление блокчейнами и обеспечивающие взаимодействие с данными.

В контексте телемедицинских технологий, такая архитектура позволяет безопасно и эффективно управлять медицинскими данными пациентов. Каждый канал может быть выделен для определенного набора медицинских учреждений или групп пациентов, что позволяет обеспечить гибкость и адаптируемость системы к различным условиям.

В домашних стационарах такая архитектура обеспечивает безопасное хранение данных о состоянии здоровья пациентов, доступных в режиме реального времени для медицинских работников. Блокчейн-менеджеры, работающие в рамках своих каналов, гарантируют неизменность и подлинность данных. Совет – это группа избранных или назначенных участников, которые управляют сетью или принимают ключевые решения по развитию и функционированию блокчейна, обеспечивает координацию между всеми участниками системы.

Отметим, что одним из вариантов внедрения технологий, использующих блокчейн, может быть создание дополнительной инфраструктуры на основе блокчейн в качестве дублирующей базы МИС, например, для домашнего стационара. С одной стороны, для этого не требуется дополнительных изменений. В используемую МИС достаточно непосредственно для базы данных МИС разработать триггер, отправляющий данные в блок-

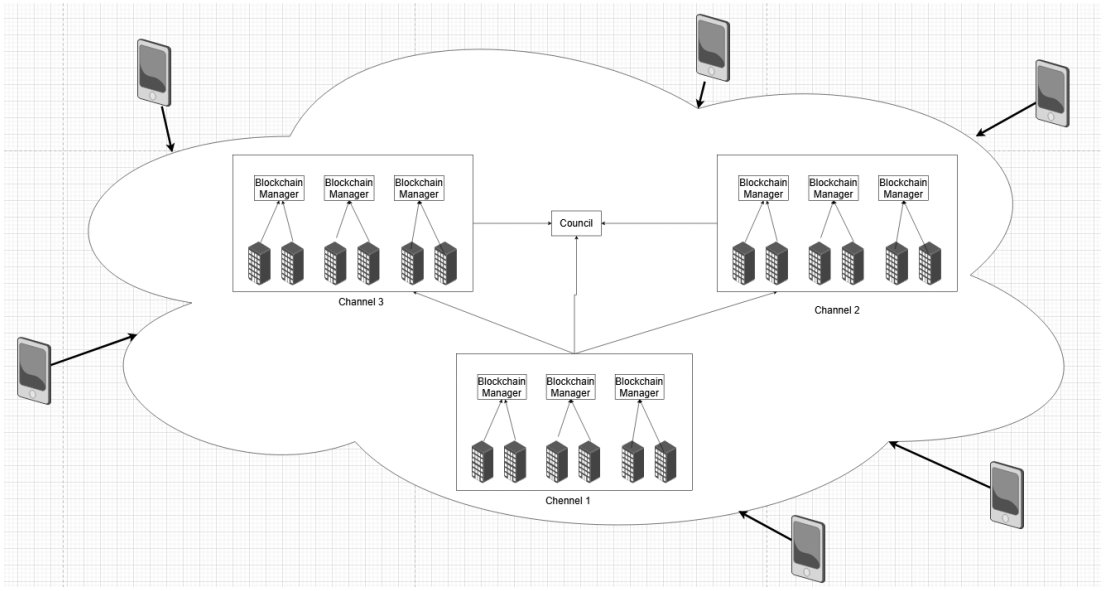

Рис. 3. Предлагаемая архитектурная схема для использования в существующих МИС

чейн, в дополнение к основной базе, или специальный шедулер, который направляет эти данные по расписанию. В условиях домашнего стационара оперативное взаимодействие между пациентами, врачами и другими участниками системы крайне важно. Блокчейн может значительно ускорить обмен данными для принятия решений за счет автоматизации процессов через смарт-контракты. Например, когда состояние пациента меняется, соответствующие данные могут быть автоматически переданы врачу для немедленного анализа и корректировки лечения. Кроме того, смарт-контракты могут быть использованы для автоматизации процедур страхования, обеспечивая быстрое и точное возмещение затрат на медицинские услуги. Также в медицинской информационной системе домашнего стационара прозрачность данных играют важную роль в обеспечении качественного медицинского обслуживания. Блокчейн позволяет каждому участнику системы (врачам, пациентам, страховым компаниям и другим заинтересованным сторонам) иметь доступ к полному журналу транзакций и изменений в данных. Это не только увеличивает доверие к системе, но и позволяет быстро и точно отслеживать любую информацию, необходимую для принятия медицинских решений. Такая прозрачность также помогает в решении спорных ситуаций, связанных и с диагнозом, и с лечением пациента.

Для получения информации, хранимой в блокчейне, необходим API, к которому были выдвинуты следующие требования:

1) поддержка основных операций блокчейна: API должен поддержи-вать основные операции, такие как создание транзакций, чтение и запись дан-ных, валидация транзакций и доступ к информации о блоках и их содержимому;

2) работа со смарт-контрактами: возможность развертывания и вызова смарт-контрактов, а также взаимодействия с ними;

3) управление учетными записями: создание и проверка статуса учетных записей (адресов) пользователей, управление пользователями;

4) доступ к истории транзакций: возможность получения полной истории транзакций для конкретной учетной записи.

Также стоит упомянуть, что в зависимости от сложности запроса, можно воспользоваться как стандартным API блокчейна, так и смарт-контрактом, так как они предлагают более гибкую выборку данных.

Для пользовательского интерфейса доступа к данным, хранящимся в блокчейне, также были определены требования, обусловленные в том числе выбором целевой аудитории пользователей технологии – медицинских работников:

1) необязательность ручного ввода;
2) низкий порог обучения для применения;
3) безопасность конфиденциальных данных.

Один из вариантов интерфейса, удовлетворяющего данным требованиям, – голосовое управление посредством виртуального ассистента [28]. Голосовой ввод команд позволяет врачу получать информацию из базы данных, не отрываясь от работы с пациентом, что, согласно [29], снижает риск случайного занесения инфекций, упрощает круг обязанностей ассистирующего врача и улучшает опыт посещения врача пациентами. Использование технологий обработки естественного языка для ввода голосовых команд упрощает процесс обучения пользователей системы, фокусируясь на функциональных возможностях виртуального ассистента без необходимости заучивать формальные команды. Безопасность использования системы голосового помощника предлагается достичь внедрением системы непрерывной аутентификации врача-пользователя [30].

Для иллюстрации взаимодействия медицинского работника с API приве-дем некоторые примеры пользовательских запросов:

• запрос на получение истории посещений клиник: GET /getHospitalVisits, с параметром идентификатора пациента;

• запрос на получение документов по пациенту из конкретной клиники: GET / getDocumentsFromHospital, с параметром идентификатора мед. учреждения, полученного из пункта 1 и идентификатора пациента;

• запрос на получение конкретного документа: GET /getDocument, с параметром идентификатора документа, полученного из пункта 2.

Ниже предоставлен пример листинга 1, в котором происходит обработка запроса на получение истории посещений клиник.

Листинг 1 – Пример кода смарт-контракта на языке Solidity по запросу на получение истории посещений клиник

```
    pragma solidity ^0.8.0;
    contract HospitalVisits {
        struct HospitalVisit {
            string hospitalName;
            string department;
            uint256 visitDate; // Unix timestamp of the visit
            string reasonForVisit;
        }
        mapping(address => HospitalVisit[]) private hospitalVisits;
        event VisitAdded(address indexed patient, string hospitalName,
uint256 visitDate);
        function addHospitalVisit(
            string memory _hospitalName,
            string memory _department,
            uint256 _visitDate,
            string memory _reasonForVisit
        ) public {
            HospitalVisit memory newVisit = HospitalVisit({
                hospitalName: _hospitalName,
                department: _department,
                visitDate: _visitDate,
                reasonForVisit: _reasonForVisit
            });
            hospitalVisits[msg.sender].push(newVisit);
            emit VisitAdded(msg.sender, _hospitalName, _visitDate);
        }
        function getHospitalVisits() public view returns (HospitalVisit[]
memory) {
            return hospitalVisits[msg.sender];
        }
        function getPatientHospitalVisits(address patient) public view
returns (HospitalVisit[] memory) {
            return hospitalVisits[patient];
        }
    }
```

Заключение

В данной статье предложен инновационный подход к интеграции техно-логии блокчейн с медицинскими информационными системами (МИС), работающими с устройствами Интернета медицинских вещей (IoMT), для улучшения качества и безопасности медицинских данных. Использование блокчейна обеспечивает создание распределенного и защищенного хранилища данных, что особенно актуально для домашних стационаров и медицинских учреждений. Это решение позволяет улучшить управление медицинскими данными, обеспечить их конфиденциальность и целостность, а также значительно ускорить процессы принятия решений.

Кроме того, предложенная архитектура позволяет использовать смарт-контракты для автоматизации различных процессов, включая страхование и корректировку лечения на основе реальных данных пациента. Это открывает новые возможности для взаимодействия медицинских учреждений, врачей и пациентов, а также улучшает прозрачность и надежность хранения данных.

Таким образом, использование технологии блокчейн в контексте МИС и IoMT является перспективным направлением для дальнейшего развития здравоохранения, которое поможет повысить эффективность и безопасность медицинских услуг.

Литература

1. Кузнецова В. П., Вардомацкая Л. П., Тропинова Е. А. Блокчейн в зда-воохранении // Экономика и управление. 2018. No 7 (153). С. 16–20.

2. Гончаренко, Ю. Ю. Использование технологии блокчейн для проверки подлинности электронных документов и файлов / Ю. Ю. Гончаренко // БЛОКЧЕЙН — 2023 г. — № 1 (47) — С. 98-101

3. Захаров, А. А. Методы разграничения доступа в сетях интернета медицинских вещей на основе атрибутивных моделей 1 / А. А. Захаров, К. Ю. Пономарёв // Телемедицина — 2020 г. — № 4 (38) — С. 44-54

4. W. A. N. A. Al-Nbhany, A. T. Zahary and A. A. Al-Shargabi, "Blockchain-IoT Healthcare Applications and Trends: A Review," // IEEE Access, vol. 12, pp. 4178-4212, 2024

5. Litvin, A. A. The Possibilities of Blockchain Technology in Medicine (Re-view) / A. A. Litvin, S. V. Korenev, E. G. Knyazeva, V. Litvin // БЛОКЧЕЙН — 2019 г. — № 4 — С. 191-199

6. Сбербанк и ФАС России запустили пилотный проект по обмену доку-ментами на основе Blockchain [Электронный ресурс] / Сбербанк крупнейший транснациональный и универсальный банк России, Центральной и Восточной Европы. — Режим доступа: https://www.sberbank.ru/ru/press_center/a11/artic1e?newsID=cb85f87f-8дc4-46df-8fdf-eab909д0277c& block-ID=1303& regionID=&1ang=ru (дата обращения: 16.05.2024).

7. Монаков, Д. М. Медицинские информационные системы: современные реалии и перспективы / Д. М. Монаков, Д. В. Алтунин // МИС — 2022 г. — № 4 — С. 46-53.

8. Аксенова Е. И., Горбатов С. Ю. Интернет медицинских вещей (IoMT): новые возможности для здравоохранения //М.: НИИОЗММ ДЗМ. – 2021.

9. Шадёркин И. А. и др. Информационные технологии в организации домашнего стационара для людей с ограниченными возможностями //Журнал телемедицины и электронного здравоохранения. – 2018. – №. 3 (8). – С. 57-63.

10. Конституция Российской Федерации: [принята всенародным голосо-ванием 12 декабря 1993 г. с изменениями, одобренными в ходе общероссийского голосования 01 июля 2020 г.]. – Текст: электронный // Официальный интернет–портал правовой информации. – URL: http://www.pravo.gov.ru (дата обращения: 22.01.2024).

11. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ // СПС Консультант Плюс URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения 22.01.2024).

12. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, ин-формационных технологиях и о защите информации» // СПС Консультант Плюс URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения 22.01.2024).

13. Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в РФ» // СПС Консультант Плюс URL: https://www.consultant.ru/document/cons_doc_LAW_121895/ (дата обращения 22.01.2024).

14. Приказ ФСТЭК от 18 февраля 2013 г. N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // ФСТЭК России URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (дата обращения 22.01.2024).

15. Приказ Минздрава России от 24.12.2018 N 911н "Об утверждении Требований к государственным информационным системам в сфере здраво-охранения субъектов Российской Федерации, медицинским информационным системам медицинских организаций и информационным системам фармацев-тических организаций" // СПС Консультант Плюс URL: https://www.consultant.ru/document/cons_doc_LAW_327147/ (дата обращения 22.01.2024).

16. Постановление Правительства РФ от 01.11.2012 N 1119 "Об утвер-ждении требований к защите персональных данных при их обработке в информационных системах персональных данных" // СПС Консультант Плюс URL: https://www.consultant.ru/document/cons_doc_LAW_137356/ (дата обращения 22.01.2024).

17. Приказ Минздрава России от 30.11.2017 N 965н "Об утверждении порядка организации и оказания медицинской помощи с применением телемедицинских технологий" // СПС Консультант Плюс URL: https://www.consultant.ru/document/cons_doc_LAW_287515/ (дата обращения 22.01.2024).

18. Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ // СПС Кон-сультант Плюс URL: https://www.consultant.ru/document/cons_doc_LAW_287515/ (дата обращения 22.01.2024).

19. Постановление Правительства РФ от 08.02.2018 N 127 (ред. от 20.12.2022) "Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений" // СПС Консультант Плюс URL: https://www.consultant.ru/document/cons_doc_LAW_290595/249cdc5b469dbd358edc05698e5b3e4be012269a/#dst100074 (дата обращения 22.01.2024).

20. Приказ ФСТЭК от 25 декабря 2017 г. N 239 "Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры российской федерации" // ФСТЭК России URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (дата обращения 22.01.2024).

21. Приказ ФСТЭК от 21 декабря 2017 г. N 235 "Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры российской федерации и обеспечению их функционирования" // ФСТЭК России URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-21-dekabrya-2017-g-n-235 (дата обраще-ния 22.01.2024).

22. Информационные технологии в организации домашнего стационара для людей с ограниченными возможностями / И. А. Шадёркин, Г. С. Лебедев, А. В. Владзимирский, А. А. Лисненко и др. // СТАЦИОНАР НА ДОМУ — 2018 г. — № 3 (8) — С. 57-63.

23. Ruzmetov A., Khudaybergenov T. Survey of IoT application layer proto-cols //Modern Science and Research. – 2024. – Т. 3. – №. 1. – С. 1-5.

24. Vidyarthi D. P. et al. Scheduling in distributed computing systems: Analysis, design and models. – Springer Science & Business Media, 2008.

25. Mesbahi M., Rahmani A. M. Load balancing in cloud computing: a state of the art survey //Int. J. Mod. Educ. Comput. Sci. – 2016. – Т. 8. – №. 3. – С. 64.

26. Patki T. et al. Economic viability of hardware overprovisioning in power-constrained high performance computing //2016 4th International Workshop on Energy Efficient Supercomputing (E2SC). – IEEE, 2016. – С. 8-15.

27. Gupta A. et al. The who, what, why, and how of high performance computing in the cloud //2013 IEEE 5th international conference on cloud computing technology and science. – IEEE, 2013. – Т. 1. – С. 306-314.

28. Применение голосового помощника в качестве виртуального консультанта для администрирования безопасности инфраструктуры локальной компьютерной сети / А. А. Захаров, А. М. Шабалин, Ш. И. Ханбеков, Д. Б. Джалилзода и др. // Виртуальный голосовой помощник — 2022 г. — № 4 (46) — С. 68-75.

29. Warren S. et al. Acceptance of voice assistant technology in dental prac-tice: A cross sectional study with dentists and validation using structural equation modeling //PLOS Digital Health. – 2024. – Т. 3. – №. 5. – С. e0000510.

30. Khanbekov S., Zakharov A. Continuous speaker authentication when using network administrator virtual assistant //2023 International Russian Smart Industry Conference (SmartIndustryCon). – IEEE, 2023. – С. 202-206.

References

1. Kuznetsova V. P., Vardomatskaya L. P., Tropinova Ye. A. Blokcheyn v zdavookhranenii // Ekonomika i upravleniye. 2018. No 7 (153). S. 16–20.

2. Goncharenko, YU. YU. Ispol'zovaniye tekhnologii blokcheyn dlya pro-verki podlinnosti elektronnykh dokumentov i faylov / YU. YU. Goncharenko // BLOKCHEYN — 2023 g. — № 1 (47) — S. 98-101

3. Zakharov, A. A. Metody razgranicheniya dostupa v setyakh interneta me-ditsinskikh veshchey na osnove atributivnykh modeley 1 / A. A. Zakharov, K. YU. Ponomarov // Telemeditsina — 2020 g. — № 4 (38) — S. 44-54.

4. U. A. N. A. Al-Nbhani, A. T. Zahari and A. A. Al-Sharghabi, "Blockchain applications and trends of the Internet of Things in healthcare: an overview" // IEEE Access, volume 12, pp. 4178-4212, 2024

5. Litvin, A. A. The possibilities of blockchain technology in medicine (Re-view) / A. A. Litvin, S. V. Korenev, E. G. Knyazeva, V. Litvin // BLOCKCHAIN — 2019 — No. 4 — pp. 191-199

6. Sberbank i FAS Rossii zapustili pilotnyy proyekt po obmenu do-kumentami na osnove Blockchain [Elektronnyy resurs] / Sberbank krupney-shiy transnatsional'nyy i universal'nyy bank Rossii, Tsentral'noy i Vo-stochnoy Yevropy. — Rezhim dostupa: https://www.sberbank.ri/gi/press_center/a11/artic1e?newsID=cb85f87f-8dc4-46df-8fdf-eab909d0277c& Yosk-ID=1303& regionID=&1ang=ru (data obrashche-niya: 16.05.2024).

7. Monakov, D. M. Meditsinskiye informatsionnyye sistemy: sovremen-nyye realii i perspektivy / D. M. Monakov, D. V. Altunin // MIS — 2022 g. — № 4 — S. 46-53.

8. Aksenova Ye. I., Gorbatov S. YU. Internet meditsinskikh veshchey (IoMT): novyye vozmozhnosti dlya zdravookhraneniya //M.: NIIOZMM DZM. – 2021.

9. Shadorkin I. A. i dr. Informatsionnyye tekhnologii v organizatsii domashnego statsionara dlya lyudey s ogranichennymi vozmozhnostyami //Zhurnal telemeditsiny i elektronnogo zdravookhraneniya. – 2018. – №. 3 (8). – S. 57-63.

10. Konstitutsiya Rossiyskoy Federatsii: [prinyata vsenarodnym golo-sovaniyem 12 dekabrya 1993 g. s izmeneniyami, odobrennymi v khode obshcheros-siyskogo golosovaniya 01 iyulya 2020 g.]. – Tekst: elektronnyy // Ofitsial'-nyy internet–portal pravovoy informatsii. – URL: http://www.pravo.gov.ru (data obrashcheniya: 22.01.2024).

11. Federal'nyy zakon "O personal'nykh dannykh" ot 27.07.2006 N 152-FZ // SPS Konsul'tant Plyus URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (data obrashcheniya 22.01.2024).

12. Federal'nyy zakon ot 27.07.2006 № 149-FZ «Ob informatsii, in-formatsionnykh tekhnologiyakh i o zashchite informatsii» // SPS Konsul'tant Plyus URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (data obrashcheniya 22.01.2024).

13. Federal'nyy zakon ot 21.11.2011 № 323-FZ «Ob osnovakh okhrany zdo-rov'ya grazhdan v RF» // SPS Konsul'tant Plyus URL: https://www.consultant.ru/document/cons_doc_LAW_121895/ (data obrashcheniya 22.01.2024).

14. Prikaz FSTEK ot 18 fevralya 2013 g. N 21 «Ob utverzhdenii so-stava i soderzhaniya organizatsionnykh i tekhnicheskikh mer po obespecheniyu bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh» // FSTEK Rossii URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (data obrashcheniya 22.01.2024).

15. Prikaz Minzdrava Rossii ot 24.12.2018 N 911n "Ob utverzhdenii Trebovaniy k gosudarstvennym informatsionnym sistemam v sfere zdravo-okhraneniya sub"yektov Rossiyskoy Federatsii, meditsinskim informatsionnym sistemam meditsinskikh organizatsiy i informatsionnym sistemam farmatsev-ticheskikh organizatsiy" // SPS Konsul'tant Plyus URL: https://www.consultant.ru/document/cons_doc_LAW_327147/ (data obrashcheniya 22.01.2024).

16. Postanovleniye Pravitel'stva RF ot 01.11.2012 N 1119 "Ob utver-zhdenii trebovaniy k zashchite personal'nykh dannykh pri ikh obrabotke v in-formatsionnykh sistemakh personal'nykh dannykh" // SPS Konsul'tant Plyus URL: https://www.consultant.ru/document/cons_doc_LAW_137356/ (data ob-rashcheniya 22.01.2024).

17. Prikaz Minzdrava Rossii ot 30.11.2017 N 965n "Ob utverzhdenii poryadka organizatsii i okazaniya meditsinskoy pomoshchi s primeneniyem tele-meditsinskikh tekhnologiy" // SPS Konsul'tant Plyus URL: https://www.consultant.ru/document/cons_doc_LAW_287515/ (data obrashcheniya 22.01.2024).

18. Federal'nyy zakon "O bezopasnosti kriticheskoy informatsionnoy infra-struktury Rossiyskoy Federatsii" ot 26.07.2017 N 187-FZ // SPS Konsul'tant Plyus URL: https://www.consultant.ru/document/cons_doc_LAW_287515/ (data obrash-cheniya 22.01.2024).

19. Postanovleniye Pravitel'stva RF ot 08.02.2018 N 127 (red. ot 20.12.2022) "Ob utverzhdenii Pravil kategorirovaniya ob"yektov kritiche-skoy informatsionnoy infrastruktury Rossiyskoy Federatsii, a takzhe pe-rechnya pokazateley kriteriyev znachimosti ob"yektov kriticheskoy informatsi-onnoy infrastruktury

Rossiyskoy Federatsii i ikh znacheniy" // SPS Kon-sul'tant Plyus URL: https://www.consultant.ru/document/cons_doc_LAW_290595/249cdc5b469dbd358edc05698e5b3e4be012269a/#dst100074 (data obrashcheniya 22.01.2024).

20. Prikaz FSTEK ot 25 dekabrya 2017 g. N 239 "Ob utverzhdenii tre-bovaniy po obespecheniyu bezopasnosti znachimykh ob"yektov kriticheskoy in-formatsionnoy infrastruktury rossiyskoy federatsii" // FSTEK Rossii URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (data obrashcheniya 22.01.2024).

21. Prikaz FSTEK ot 21 dekabrya 2017 g. N 235 "Ob utverzhdenii tre-bovaniy k sozdaniyu sistem bezopasnosti znachimykh ob"yektov kriticheskoy informatsionnoy infrastruktury rossiyskoy federatsii i obespecheniyu ikh funktsionirovaniya" // FSTEK Rossii URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-21-dekabrya-2017-g-n-235 (data ob-rashcheniya 22.01.2024).

22. Informatsionnyye tekhnologii v organizatsii domashnego statsiona-ra dlya lyudey s ogranichennymi vozmozhnostyami / I. A. Shadorkin, G. S. Le-bedev, A. V. Vladzimirskiy, A. A. Lisnenko i dr. // STATSIONAR NA DO-MU — 2018 g. — № 3 (8) — S. 57-63.

23. Ruzmetov A., Khudaybergenov T. Survey of IoT application layer pro-tocols //Modern Science and Research. – 2024. – T. 3. – №. 1. – S. 1-5.

24. Vidyarthi D. P. et al. Scheduling in distributed computing systems: Analysis, design and models. – Springer Science & Business Media, 2008.

25. Mesbahi M., Rahmani A. M. Load balancing in cloud computing: a state of the art survey //Int. J. Mod. Educ. Comput. Sci. – 2016. – T. 8. – №. 3. – S. 64.

26. Patki T. et al. Economic viability of hardware overprovisioning in power-constrained high performance computing //2016 4th International Work-shop on Energy Efficient Supercomputing (E2SC). – IEEE, 2016. – S. 8-15.

27. Gupta A. et al. The who, what, why, and how of high performance computing in the cloud //2013 IEEE 5th international conference on cloud com-puting technology and science. – IEEE, 2013. – T. 1. – S. 306-314.

28. Primeneniye golosovogo pomoshchnika v kachestve virtual'nogo kon-sul'tanta dlya administrirovaniya bezopasnosti infrastruktury lokal'noy komp'yuter-noy seti / A. A. Zakharov, A. M. Shabalin, SH. I. Khanbekov, D. B. Dzhalilzoda i dr. // Virtual'nyy golosovoy pomoshchnik — 2022 g. — № 4 (46) — S. 68-75.

29. Warren S. et al. Acceptance of voice assistant technology in dental prac-tice: A cross sectional study with dentists and validation using structural equation modeling //PLOS Digital Health. – 2024. – T. 3. – №. 5. – S. e0000510.

30. Khanbekov S., Zakharov A. Continuous speaker authentication when using network administrator virtual assistant //2023 International Russian Smart Industry Conference (SmartIndustryCon). – IEEE, 2023. – S. 202-206.

КОРЕНЕВ Дмитрий Александрович, аспирант кафедры «Информаци-онной безопасности», Тюменский государственный университет. 625003, г. Тюмень, ул. Володарского, 6. E-mail: koreneffdmitrii@gmail.com

ХАНБЕКОВ Шамиль Ирекович, аспирант кафедры «Информационной безопасности», Тюменский государственный университет. 625003, г. Тюмень, ул. Володарского, 6. E-mail: s.i.khanbekov@utmn.ru

ЗАХАРОВ Александр Анатольевич, доктор технических наук, заве-дующий базовой кафедрой «Безопасные ИТ умного города», Тюменский государственный университет. 625003, г. Тюмень, ул. Володарского, 6. E-mail: a.a.zakharov@utmn.ru

KORENEV Dmitry Alexandrovich, Postgraduate student of the Department of Information Security, Tyumen State University. 625003, Tyumen, Volodarsky st., 6. E-mail: koreneffdmitrii@gmail.com

KHANBEKOV Shamil Irekovich, Postgraduate student of the Department of Information Security, Tyumen State University. 625003, Tyumen, Volodarsky st., 6. E-mail: s.i.khanbekov@utmn.ru

ZAKHAROV Alexander Alexandrovich, Doctor of Technical Sciences, Head of the Basic Department of "Secure IT of a Smart City", Tyumen State University. 625003, Tyumen, Volodarsky st., 6. E-mail: a.a.zakharov@utmn.ru