УДК 004.6:004.9
DOI 10.17513/snt.40528

МОДЕЛЬ ГИБРИДНОЙ БАЗЫ ДЛЯ ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ НА ОСНОВЕ РАСПРЕДЕЛЕННОЙ КОМПЬЮТЕРНОЙ СЕТИ BLOCKCHAIN

Нажимова Н.А., Токарев С.В.

ФГБОУ ВО «Нижегородский государственный технический университет имени Р.Е. Алексеева», Дзержинский филиал, Россия, Дзержинск, e-mail: adilia@list.ru

В данной статье рассматривается разработка гибридной системы хранения и обработки персональных данных с использованием технологии блокчейн. Цель исследования заключается в разработке базы данных для безопасного и эффективного хранения персональных данных с применением технологии Blockchain. Описана гибридная модель, в которой фактические персональные данные шифруются и хранятся в автономных базах данных, в то время как в блокчейне записываются только хешированные отпечатки персональных данных и цифровые подписи. Такой подход минимизирует риски для конфиденциальности, сохраняя при этом возможность аудита и соблюдение правовых норм. 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. Предлагаемая система особенно актуальна в правовых и нормативных условиях, которые требуют подотчетности и возможности отслеживания согласия пользователя. Представленная в статье гибридная архитектура обеспечивает высокие стандарты защиты данных, обеспечивая гибкую интеграцию в существующие информационные инфраструктуры. В заключение демонстрируется, как блокчейн может быть эффективно применен в области защиты персональных данных, не как механизм хранения необработанных данных, а как поддающийся проверке реестр для криптографических доказательств и истории доступа, что представляет собой смену парадигмы в управлении данными в цифровую эпоху.

Ключевые слова: персональные данные, блокчейн, информационная безопасность, хранение данных, гибридная архитектура, криптографическая защита, хеширование, цифровая подпись, закон 152-ФЗ, аудит и контроль доступа

HYBRID DATABASE MODEL FOR STORING PERSONAL DATA BASED ON A DISTRIBUTED COMPUTER NETWORK BLOCKCHAIN

Nazhimova N.A., Tokarev S.V.

Nizhny Novgorod State Technical University named after R.E. Alekseev, Dzerzhinsk branch, Russia, Dzerzhinsk, e-mail: adilia@list.ru

This article discusses the development of a hybrid system for storing and processing personal data using blockchain technology. The purpose of the research is to develop a database for secure and efficient storage of personal data using Blockchain technology. A hybrid model is described in which the actual personal data is encrypted and stored in autonomous databases, while only hashed fingerprints of personal data and digital signatures are recorded in the blockchain. This approach minimizes privacy risks while maintaining the ability to audit and comply with legal regulations. The study highlights key blockchain mechanisms such as hashing, digital signatures, and consensus protocols, and explains how they collectively contribute to data integrity and secure access control. The proposed system is particularly relevant in legal and regulatory environments that require accountability and the ability to track user consent. The hybrid architecture presented in the article provides high standards of data protection, providing flexible integration into existing information technologies infrastructures. In conclusion, the work demonstrates how blockchain can be effectively applied in the field of personal data protection, not as a mechanism for storing raw data, but as a verifiable registry for cryptographic evidence and access history, which represents a paradigm shift in data management in the digital age.

Keywords: personal data, blockchain, information security, data storage, hybrid architecture, cryptographic protection, hashing, digital signature, law 152-FZ, audit and access control

Введение

В условиях стремительной цифровизации защита персональных данных и безопасное управление ими приобретают все большее значение. Рост числа инцидентов, связанных с несанкционированным доступом, утечкой данных и кибератаками, подчеркивает уязвимость традиционных информационных систем и растущие финансовые и репутационные риски, связанные с компрометацией личной информации. В рамках федерального закона № 152-ФЗ персональные данные определяются как любая информация, которая прямо или косвенно относится к идентифицированному или поддающемуся идентификации физическому лицу. В соответствии с этим регламентом организации, которым поручено собирать и хранить такие данные, несут юридическую ответственность за их целостность и конфиденциальность [1]. Традиционные системы хранения данных, основанные

преимущественно на централизованных реляционных базах данных, по-прежнему имеют структурные недостатки [2], которые могут быть использованы злоумышленниками [3]. Эти недостатки требуют изучения альтернативных подходов, которые могут обеспечить более надежные гарантии сохранности данных и возможности их проверки. Среди рассматриваемых технологий блокчейн стал приоритетным выбором благодаря присущим ему особенностям – децентрализации, криптографической последовательности и абсолютной неизменности, – которые в совокупности помогают предотвратить несанкционированный доступ и подделку данных. Тем не менее интеграция блокчейна в системы, обрабатывающие персональные данные, сопряжена не только с техническими трудностями, но и с юридическими и этическими соображениями. В результате разработка основанных на блокчейне систем защиты персональных данных является многообещающей и сложной задачей. Представленное исследование удовлетворяет спрос на такие инновации, предлагая гибридную модель, которая использует традиционные системы хранения данных на базе реляционных СУБД и сильные стороны блокчейна для улучшения механизмов защиты персональных данных. Ожидается, что результаты будут способствовать развитию безопасной цифровой инфраструктуры в соответствии с меняющимися нормативно-правовыми условиями и потребностями современного российского общества.

Цель исследования – разработка программного обеспечения для безопасного и эффективного хранения персональных данных с применением технологии Blockchain.

Материалы и методы исследования

В данном исследовании используется гибридный подход, основанный на блокчейне, для обеспечения безопасности обработки и хранения персональных данных (ПДн). Предлагаемая методология объединяет технологию распределенного реестра (DLT) с математическими криптографическими методами для обеспечения конфиденциальности, целостности и проверяемости операций по обработке ПДн.

Результаты исследования и их обсуждение

Применение технологии блокчейн для обеспечения безопасного хранения ПДн и управления ими представляет собой переход от традиционных подходов к модели, устойчивой к манипуляциям, вторжениям и потере данных. В представленной статье блокчейн рассматривается как распределенная система учета, основанная на криптографических подходах, которые обеспечивают безопасное, прозрачное и защищенное от несанкционированного доступа ведение записей. В отличие от традиционных систем, где безопасность рассматривается отдельно от централизованной архитектуры, блокчейн интегрирует безопасность в базовую структуру своего протокола [4].

Одним из наиболее важных атрибутов блокчейна, имеющих отношение к защите ПДн, является его неизменность [5]. Как только данные записаны в блокчейн, они не могут быть изменены задним числом без согласия участников сети. Эта функция является прямым результатом использования криптографической цепочки блоков, где каждый блок содержит хеш предыдущего блока, эффективно создавая хронологическую и не поддающуюся изменению последовательность транзакций. Это свойство особенно ценно в контексте ПДн, любая попытка изменить ранее сохраненные ПДн становится невозможной с точки зрения математических вычислений и может быть немедленно обнаружена.

Использование цифровых подписей [6] усиливает аутентификацию пользователя. Каждая транзакция в блокчейне подписывается закрытым ключом отправителя, который может быть проверен с помощью соответствующего открытого ключа. Этот механизм, гарантирует, что только уполномоченные лица могут инициировать изменения или получать доступ к ПДн.

Дополнительный уровень защиты обеспечивается прозрачной и отслеживаемой «природой» блокчейн-систем. Каждая операция: ввод данных, доступ к ним или модификация – регистрируется с помощью временной метки и уникального криптографического идентификатора. Эти записи поддаются публичной проверке и устойчивы к удалению, что обеспечивает надежный контрольный след как для пользователей, так и для регулирующих органов [7]. Прозрачность блокчейна не означает публичного раскрытия ПДн; данные хранятся вне сети в зашифрованном виде, при этом в блокчейн-сети записываются только криптографические доказательства и средства контроля доступа на основе алгоритмов консенсуса [8]. Эта гибридная модель позволяет блокчейну служить основой для верификации и авторизации без ущерба для конфиденциальности [9]. Таким образом блокчейн становится не только технологической инновацией, но и сменой парадигмы в том, как ПДн могут храниться, контролироваться и защищаться.

Рис. 1. Гибридный подход к обработке и хранению ПДн
Источник: составлено авторами

Предлагаемый в работе процесс безопасной обработки ПДн (рис. 1) с помощью блокчейна начинается с того момента, когда пользователь добровольно предоставляет ПДн сервису или платформе. Эти данные могут включать идентификационную информацию, биометрические данные, историю транзакций или другие конфиденциальные данные, защищенные в соответствии с юридическими определениями ПДн (например, № 152-ФЗ или GDPR) [10]. Вместо того чтобы хранить эти данные непосредственно в блокчейне – подход, который вызвал бы серьезные опасения по поводу конфиденциальности, – предлагается в программном продукте на базе блокчейн-системы реализовать криптографическую абстракцию.

Как только данные собраны, они подвергаются хешированию [11]. Параллельно данные подписываются цифровой подписью с использованием закрытого ключа пользователя или системы, отправляющей данные [12]. Эта цифровая подпись подтверждает подлинность источника данных и гарантирует, что данные не были изменены при передаче.

Вместо того чтобы хранить необработанные ПДн в цепочке, система записывает только хеш-значение и цифровую подпись в транзакции, которая добавляется в блокчейн. Эта запись становится частью постоянной, защищенной от несанкционированного доступа записи с отметкой времени, распространяемой по всей сети распределенных реестров. Между тем полный набор данных, включая информацию, позволяющую установить личность, хранится «вне сети», как правило, в зашифрованных базах данных или децентрализованных системах хранения файлов, таких как IPFS, Filecoin или облачные решения с жестким контролем доступа.

Когда требуется проверка (например, во время проверки соответствия требованиям, судебного спора или запроса на доступ), система не извлекает и не раскрывает ПДн. Вместо этого она повторно обрабатывает представленные данные и сравнивает полученный хеш с хешем, хранящимся в блокчейне. Если хеши совпадают, данные подтверждаются как подлинные. Кроме того, цифровая подпись, связанная с транзакцией, может быть использована для проверки личности отправителя с использованием его открытого ключа.

Чтобы снизить риск того, что исходные данные могут быть восстановлены, важно, чтобы блокчейн-системы применяли необратимые криптографические хеш-функции (такие как SHA-256 или SHA-3), гарантирующие, что, даже если хеш будет раскрыт, он не сможет быть однозначно отнесен к исходным ПДн [13]. Для формирования хеша в контексте обработки ПДн в системе выполняются следующие действия:

1. Предварительная обработка: ПДн структурированы или упорядочены в согласованном формате (в нашем случае в формате JSON).

2. хеширование: структурированные данные передаются через хеш-функцию, например SHA-256 (данные), в результате чего выводится хеш фиксированной длины.

3. Хранение: результирующее значение хеша сохраняется в транзакции блокчейна или связанной с ней записи, чтобы служить эталонным отпечатком исходных данных.

Этот хеш служит надежным средством проверки целостности данных. Если какая-либо часть исходных данных будет изменена – даже на один бит – результирующий хеш будет значительно отличаться, что указывает на подделку.

Другим важным аспектом российского законодательства о защите ПДн является требование о проверяемости и подотчетности при обработке ПДн. Российские нормативные акты требуют, чтобы любые действия по обработке данных регистрировались, и эти записи должны быть доступны для аудитов и проверок [14].

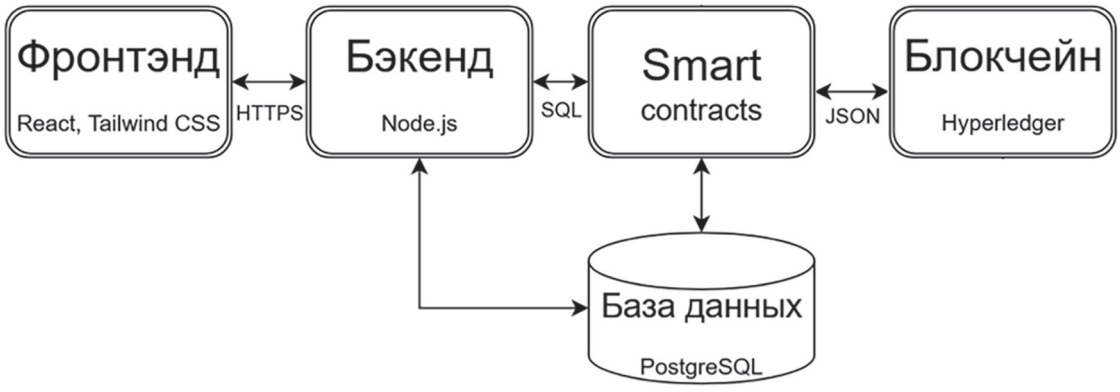

Рис. 2. Структура блокчейн системы хранения ПДн

Благодаря хранению криптографического хеша и цифровой подписи транзакций с ПДн в блокчейне создается постоянная, неизменяемая запись, которую можно проверить в любое время. Это повышает подотчетность, поскольку предоставляет поддающиеся проверке доказательства того, кто получил доступ к данным, когда и с какой целью.

Среда разработки и набор инструментов, выбранные для внедрения гибридной системы хранения ПДн, призваны обеспечить высокий уровень безопасности, производительности и простоты обслуживания. Система объединяет традиционную реляционную базу данных с инфраструктурой блокчейна, предлагая при этом адаптивный пользовательский интерфейс и безопасную внутреннюю связь (рис. 2).

Для хранения конфиденциальных ПДн в качестве основной системы управления реляционными базами данных был выбран PostgreSQL (Postgres Pro). Данное технологическое решение обеспечивает надежную поддержку целостности, масштабируемости и расширяемости данных, а также включает поддержку шифрования данных при хранении и передаче. Блокчейн-компонент построен с использованием Hyperledger Fabric, платформы распределенного реестра, специально разработанной для корпоративных приложений [15]. Hyperledger обеспечивает детальный контроль доступа, частные каналы для безопасной связи между авторизованными узлами и эффективные механизмы согласования. Смарт-контракты (smart contracts) в Hyperledger разработаны на языке программирования Go и отвечают за проверку транзакций, запись хешей зашифрованных ПДн, управление журналами аудита и обеспечение соблюдения политик доступа.

Для серверной части используется облегченный и безопасный стек с использованием Node.js и Express.js. Это обеспечивает эффективную обработку асинхронных запросов и RESTful API, интегрируя PostgreSQL и Hyperledger с помощью защищенного промежуточного программного обеспечения. Бизнес-логика, аутентификация и конечные точки API инкапсулированы на уровне серверной части. Во внешнем интерфейсе используется современный набор технологий, обеспечивающий ясность и удобство использования. React.js выбран для создания пользовательского интерфейса из-за его компонентной архитектуры и надежной экосистемы. Стилизация осуществляется с помощью фреймворка Tailwind CSS, что позволяет поддерживать чистый, адаптивный дизайн без излишней сложности.

Обмен данными между интерфейсом и серверной частью защищен по протоколу HTTPS с аутентификацией на основе JWT. Приложение размещено в контейнере с использованием Docker для обеспечения согласованной среды разработки и развертывания. Возможно использование Kubernetes для координации при развертывании в производственных масштабах. Разработка и контроль версий осуществляются с помощью Git, а конвейеры CI/CD настраиваются с помощью GitHub Actions.

Анализ результатов тестирования системы обеспечения безопасного хранения ПДн, основанной на блокчейне, показывает, что система надежно работает при моделируемых рабочих нагрузках. Все ключевые показатели, включая уровень успешности транзакций, задержку, пропускную способность и потребление ресурсов, находились в пределах допустимых и ожидаемых диапазонов. Однако, несмотря на то, что во время тестирования система поддерживала 100 %-ный показатель успешности транзакций, этот показатель соблюдался при контролируемых условиях работы сети и данных. В реальных условиях такие факторы, как непредсказуемая задержка в сети, нео-

жиданные объемы транзакций и неправильно сформированные запросы, могут повлиять на стабильность. Поэтому необходимо подготовить инфраструктуру к внезапным скачкам трафика и внедрить мониторинг ошибок в режиме реального времени.

Представленная модель гибридного программного обеспечения для хранения персональных данных на основе технологии Blockchain отделяет хранение данных от проверки данных. Это гарантирует, что даже в случае взлома автономного хранилища данных реестр на основе блокчейна по-прежнему предоставляет информацию о несанкционированном доступе, по которой целостность и подлинность данных могут быть независимо подтверждены. В результате блокчейн сам по себе становится не средством хранения ПДн, а защищенным реестром для записи доказательств целостности данных, журналов доступа и потоков разрешений, что обеспечивает как сохранение конфиденциальности, так и подотчетность данных в технологически и юридически надежной системе.

Заключение

Были рассмотрены концептуальные основы и реализация архитектуры гибридного программного обеспечения для хранения персональных данных на основе технологии Blockchain, для безопасной обработки и хранения ПДн. Было установлено, что блокчейн обеспечивает встроенную поддержку ключевых принципов безопасности, таких как конфиденциальность, целостность и прозрачность, посредством криптографических механизмов и неизменяемого ведения журнала. Гибридная модель, представленная в статье, отделяет проверку данных от их хранения, гарантируя, что конфиденциальные персональные данные не хранятся непосредственно в блокчейне, а хешируются и подписываются, в то время как исходная информация остается зашифрованной во внешних базах данных.

Продемонстрировано, как эта архитектура согласуется с российскими законами о защите данных, в частности с Федеральным законом № 152-ФЗ, обеспечивая возможность аудита и контроля доступа без ущерба для конфиденциальности. Данная работа подтверждает эффективность технологии блокчейн в удовлетворении растущего спроса на безопасные системы управления ПДн и задает направление для будущих исследований, сосредоточенных на повышении информационной безопасности в эпоху цифровых преобразований.

Список литературы

1. Добробаба М.Б. Понятие персональных данных: проблема правовой определенности // Вестник Университета имени О.Е. Кутафина. 2023. № 2 (102). С. 42–52. URL: https://vestnik.msal.ru/jour/article/view/1974 (дата обращения: 25.06.2025).

2. Хромова А.Р., Петросян Л.Э. Анализ уязвимостей в системах безопасности данных // Инженерный вестник Дона. 2023. № 6 (102). URL: http://www.ivdon.ru/ru/magazine/archive/n6y2023/8447 (дата обращения: 25.06.2025).

3. Баранова Е.М., Баранов А.Н., Борзенкова С.Ю., Васин К.И., Перезябов В.С. Современные тенденции защиты баз данных веб-приложений от SQL инъекций // Известия ТулГУ. 2023. № 12. С. 492–494. URL: https://tidings.tsu.tula.ru/tidings/pdf/web/preview_therest_ru.php?x=tsu_izv_technical_sciences_2023_12_e&year=2023 (дата обращения: 25.06.2025).

4. Носиров З.А., Фомичев В.М. Анализ блокчейн-технологии: основы архитектуры, примеры использования, перспективы развития, проблемы и недостатки // Системы управления, связи и безопасности. 2021. № 2. С. 37–75. URL: https://sccs.intelgr.com/archive/2021-02/03-Nosirov.pdf (дата обращения: 25.06.2025).

5. Рябко В.В., Васильева Т.В. Блокчейн: проблемы и перспективы развития // Вопросы развития современной науки и техники. 2021. № 4. С. 165–173. URL: https://cyberleninka.ru/article/n/blokcheyn-problemy-i-perspektivy-razvitiya (дата обращения: 25.06.2025).

6. Шандрович А.В., Демкин Д.А. Электронная цифровая подпись в контексте информационной безопасности // Вестник науки. 2024. № 7. С. 614–618. URL: https://www.вестник-науки.рф/article/16689 (дата обращения: 25.06.2025).

7. Булыга Р.П., Сафонова И.В. Технология блокчейн как инструмент повышения информационной прозрачности экосистемы бизнеса // Учет. Анализ. Аудит. 2021. № 4. С. 6–17. URL: https://accounting.fa.ru/jour/article/view/400/368 (дата обращения: 25.06.2025).

8. Аннагурбанова С., Абдурасулов А., Ахмедова М. Консенсус механизма блокчейн // Вестник науки. 2023. № 2. С. 213–217. URL: https://www.вестник-науки.рф/volume/journal-2-59-4 (дата обращения: 25.06.2025).

9. Тагансахедов Ш.Т., Гельдимаммедова М.Т., Шаларова А.Х. Конфиденциальность данных пользователей в общих сетях // Символ науки. 2024. № 9 (1–2). С. 67-69. URL: htt67–69cyberleninka.ru/article/n/konfidentsialnost-dannyh-polzovateley-v-obschih-setyah (дата обращения: 25.06.2025).

10. Терешин М.В. Правовое регулирование защиты персональных данных в РФ и ЕС в контексте вступления в силу общего регламента по защите данных (GDPR) // Образование и право. 2019. № 8. С. 89–93. URL: https://publications.hse.ru/pubs/share/direct/416404996.pdf (дата обращения: 25.06.2025).

11. Мебония М.А., Федорова О.В. Сравнительное исследование хеш-алгоритмов в криптографии // Вестник науки. 2022. № 12 (57). С. 439–443. URL: https://www.вестник-науки.рф/archiv/journal-12-57-3.pdf (дата обращения: 25.06.2025).

12. Шевченко В.А., Пантелеева Т.А. Электронная цифровая подпись (ЭЦП) в России // Вестник УМЦ. 2018. № 2 (19). С. 33–36. URL: https://cyberleninka.ru/article/n/elektronnaya-tsifrovaya-podpis-etsp-v-rossii (дата обращения: 25.06.2025).

13. Бакаева О.А., Барабошкин Д.А. Разработка протокола передачи данных на основе комбинированного алгоритма их шифрования // Программные продукты и системы. 2023. № 3. С. 493–502. URL: https://swsys.ru/files/2023-3/493-502.pdf (дата обращения: 25.06.2025).

14. Ибрагимова А. Понятие персональных данных; информационная безопасность права на неприкосновенность частной жизни согласно анализу статьи 8 Европейской конвенции по правам человека // Северо-Кавказский юридический вестник. 2021. № 4. С. 92–103. URL: https://cyberleninka.ru/article/n/ponyatie-personalnyh-dannyh-informatsionnaya-bezopasnost-prava-na-neprikosnovennost-chastnoy-zhizni-soglasno-analizu-stati-8 (дата обращения: 25.06.2025).

15. Ганкин Н.М., Михейлис Д.А. Hyperledger-инструментарий разработки отраслевых блокчейнов // Juvenis scientia. 2018. № 4. С. 17–19. URL: https://cyberleninka.ru/article/n/hyperledger-instrumentariy-razrabotki-otraslevyh-blokcheynov (дата обращения: 16.08.2025).

Конфликт интересов: Авторы заявляют об отсутствии конфликта интересов.

Conflict of interest: The authors declare that there is no conflict of interest.