УДК 004.4
DOI

ГИБРИДНЫЙ ПОДХОД К ПОСТРОЕНИЮ АРХИТЕКТУРЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ СИСТЕМЫ ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ С ПРИМЕНЕНИЕМ ТЕХНОЛОГИИ BLOCKCHAIN

[1]Нажимова Н.А., [2]Нажимов А.В., [3]Марушин Д.Н.

[1]Федеральное государственное бюджетное образовательное учреждение высшего образования «Нижегородский технический университет им. Р.Е. Алексеева», Дзержинск, Российская Федерация, e-mail: adilia@list.ru;
[2]Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского», Дзержинск, Российская Федерация;
[3]Акционерное общество «Управляющая компания «Биохимического холдинга «Оргхим», Нижний Новгород, Российская Федерация

В данной статье описана концептуальная многослойная модель системы хранения персональных данных, основанная на технологии Blockchain. Цель исследования заключалась в разработке соответствующей архитектуры программного обеспечения и изучении вопросов интеграции разрабатываемой системы. Подробно представлен гибридный подход, который предполагает разделение персональных данных на фактические, хранящиеся вне цепочек блоков распределенной сети, и метаданные, хеши и цифровые подписи, хранящиеся внутри цепочки блоков распределенной сети блокчейн. Предполагалось, что внутренние компоненты будут отвечать за обеспечение целостности данных, аутентификацию и прозрачность доступа к ним, в то время как внешние компоненты будут обеспечивать непосредственно хранение конфиденциальных персональных данных в безопасной среде, соответствующей требованиям российского законодательства. Разработаны компоненты концептуальной модели гибридной базы данных, а также описана структура данных и распределенная система их хранения. Рассмотрен пример того, как персональные данные обрабатываются в блокчейне, а также возможности интеграции разрабатываемой системы хранения персональных данных с существующими системами. Представлены архитектурные и технологические механизмы согласования гибридной системы хранения персональных данных с основными существующими инфраструктурными решениями. В результате было показано, что гибридная архитектура представляет собой значительный шаг на пути модернизации систем защиты персональных данных, сочетая надежность и неизменность блокчейна с масштабируемостью и совместимостью традиционных решений.

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

HYBRID APPROACH TO DEVELOPING A PERSONAL DATA STORAGE SOFTWARE ARCHITECTURE USING BLOCKCHAIN TECHNOLOGY

[1]Nazhimova N.A., [2]Nazhimov A.V., [3]Marushin D.N.

[1]Federal State Budgetary Educational Institution of Higher Education "Nizhny Novgorod state technical University named after R. E. Alekseev", Dzerzhinsk, Russian Federation, e-mail: adilia@list.ru;
[2]Federal State Autonomous Educational Institution of Higher Education "National Research Lobachevsky State University of Nizhny Novgorod", Dzerzhinsk, Russian Federation;
[3]Joint Stock Company "Management company" of the Biochemical holding "Orghim", Nizhny Novgorod, Russian Federation

This article describes a conceptual multi-layered model of a personal data storage system based on Blockchain technology. The purpose of the research was to develop an appropriate software architecture and study the integration issues of the system under development. A hybrid approach is presented in detail, which involves the separation of personal data into actual data stored outside the block chains of a distributed network, and metadata, hashes and digital signatures stored inside the block chain of a distributed blockchain network. It was assumed that the internal components would be responsible for ensuring data integrity, authentication and transparency of access to them, while the external components would directly ensure the storage of confidential personal data in a secure environment that meets the requirements of Russian legislation. The components of the conceptual model of a hybrid database are developed, as well as the data structure and distributed storage system are described. An example of how personal data is processed in the blockchain is considered, as well as the possibility of integrating the personal data storage system being developed with existing systems. Architectural and technological mechanisms for matching a hybrid personal data storage system with the main existing infrastructure solutions are presented. As a result, it was shown that the hybrid architecture represents a significant step towards modernizing personal data protection systems, combining the reliability and immutability of the blockchain with the scalability and compatibility of traditional solutions.

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

Введение

В современном цифровом мире защита и доказательство отсутствия утечек персональных данных (ПДн) стали фундаментальными проблемами как для государственных, так и для корпоративных информационных систем [1]. Традиционные модели централизованного хранения часто не позволяют сбалансировать безопасность, конфиденциальность и соответствие нормативным требованиям [2; 3]. Чтобы устранить эти ограничения, технология блокчейн открывает новые возможности для создания децентрализованных и защищенных от несанкционированного доступа механизмов управления данными. Ранее авторами были рассмотрены возможности использования технологии блокчейн при разработке систем хранения и обработки ПДн [4]. В этом исследовании представлена концептуальная гибридная модель хранения ПДн, которая сочетает в себе преимущества технологии блокчейн с гибкостью традиционных систем баз данных. Предлагаемая архитектура отделяет компоненты «внутри сети», отвечающие за целостность, аутентификацию и прозрачность, от компонентов «вне сети», которые надежно хранят конфиденциальные данные в соответствии с российскими законодательными и техническими требованиями. Интеграция криптографического хеширования, цифровых подписей и смарт-контрактов в рамках этой платформы обеспечивает конфиденциальность и проверяемость данных на протяжении всего их жизненного цикла.

Цель исследования заключается в разработке архитектуры программного обеспечения, предназначенного для хранения персональных данных с применением технологии распределенной сети Blockchain.

Материалы и методы исследования

В исследовании использованы методы математического и имитационного моделирования с применением методов криптографии для обеспечения работы распределенной сети.

Результаты исследования и их обсуждение

Концептуальная модель (рис. 1) системы хранения ПДн с применением технологии blockchain предполагает разделение данных «*вне цепочки – off chain*» (фактические ПДн) и данных «*внутри цепочки – on chain*» (метаданные, хеши и цифровые подписи).

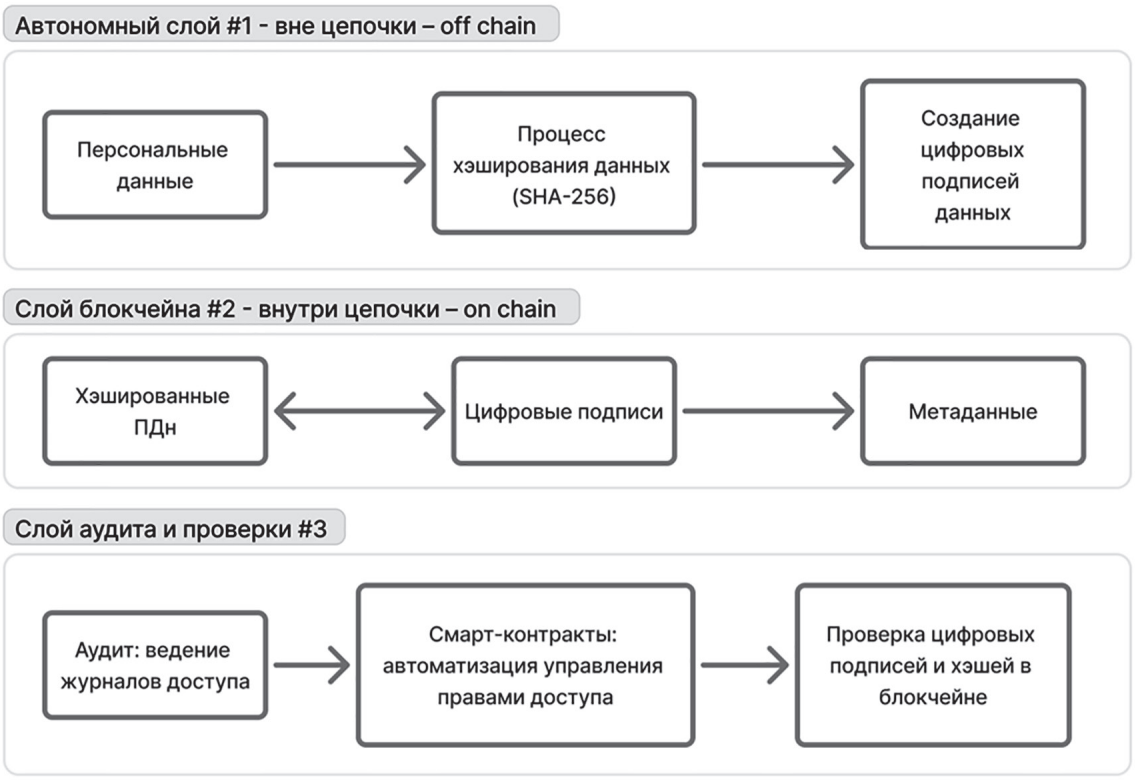

Рис. 1. Концептуальная модель системы хранения ПДн с использованием блокчейна
Источник: составлено авторами

Внутренние компоненты будут отвечать за обеспечение целостности данных, аутентификацию и прозрачность, в то время как внешние компоненты будут обеспечивать хранение конфиденциальных ПДн в безопасной, соответствующей требованиям российского законодательства среде.

Такой двойной подход позволяет использовать преимущества технологии блокчейн – неизменяемые записи, проверяемые транзакции и децентрализованный контроль – без ущерба для конфиденциальности и безопасности ПДн.

Рассмотрим основные слои концептуальной модели:

1. Автономный слой (слой 1). Фактические ПДн не хранятся непосредственно в блокчейне из-за опасений по поводу конфиденциальности данных и юридических последствий хранения конфиденциальной информации в публичном реестре [5; 6]. Вместо этого ПДн хранятся в автономном режиме в защищенных базах данных или файловых системах. Доступ к данным предоставляется только авторизованным лицам, а шифрование предотвращает несанкционированный доступ за счет использования открытых и закрытых ключей для контроля доступа к данным и возможности шифрования и дешифрования данных по мере необходимости (схематично данный уровень представлен на рис. 2).

2. Слой блокчейна (слой 2) отвечает за запись неизменяемых метаданных и криптографических доказательств, связанных с ПДн (рис. 3). Ключевые элементы, хранящиеся в блокчейне, включают:

– хешированные ПДн: сами ПДн хешируются с использованием криптографической хеш-функции (SHA-256). Это значение хеша действует как «отпечаток» данных и позволяет проверить данные, не раскрывая их фактического содержимого. Хеш хранится в блокчейне как часть записи о блоке;

- цифровые подписи – используются для проверки целостности данных и идентификации владельца или контролера данных. Цифровая подпись создается путем шифрования хеша данных с помощью закрытого ключа субъекта или контроллера данных. Подпись подтверждает, что данные не были изменены с момента их подписания;

- метаданные, такие как временная метка создания или изменения данных, идентификационные данные контроллера данных и разрешения на доступ обеспечивают прозрачную запись жизненного цикла данных, включая информацию о том, кем и когда они были обработаны.

3. Для обеспечения соблюдения правил защиты данных, включая «право на забвение» и «право на доступ к данным», в инфраструктуре блокчейна внедрена система аудита (слой аудита и проверки соответствия требованиям – слой 3). Эта система отслеживает все взаимодействия с ПДн. Концепция блокчейна гарантирует, что эти журналы не могут быть изменены [7]. Этот слой включает в себя смарт-контракты для автоматизации различных процессов, связанных с управлением ПДн. Например, смарт-контракт может автоматически предоставлять или отзывать доступ к ПДн на основе заранее определенных условий, таких как истечение срока действия согласия или изменение статуса данных.

В соответствии с технологией блокчейн данные записываются структурированным образом в виде блоков. Каждый блок служит контейнером для определенного набора записей данных, и эти записи связаны друг с другом, образуя неизменяемую цепочку.

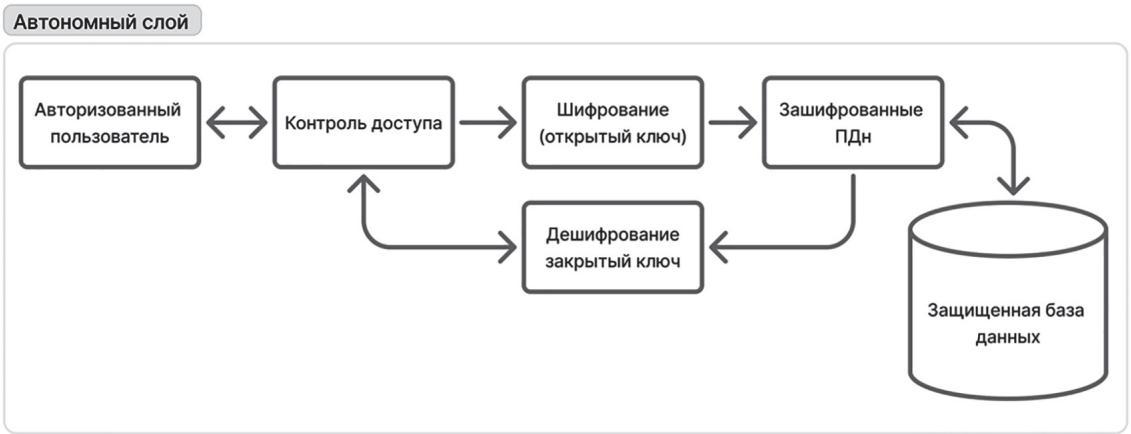

Рис. 2. Автономный слой
Источник: составлено авторами

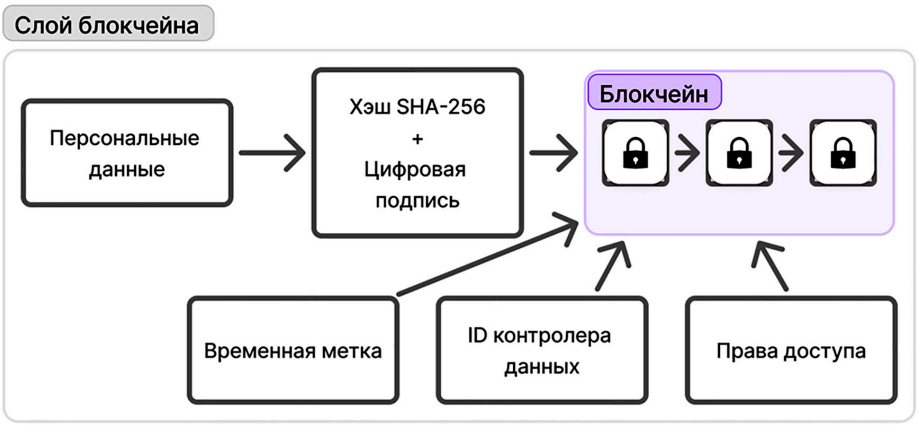

Рис. 3. Слой блокчейна
Источник: составлено авторами

Рассмотрим пример того, как ПДн обрабатываются в блокчейне на примере гипотетического гражданина.

1. Данные вводятся в систему: *Полное имя: Алексей Иванович Иванов; Дата рождения: 00.00.0000; Номер паспорта: 0000 000000; Адрес: Москва, ул. Пушкина, д. 00, кв. 00.*

2. Каждое поле или их комбинация хешируются с использованием алгоритма SHA-256.

3. Гражданин или уполномоченный регистратор подписывает хешированные данные, используя закрытый ключ. Подпись подтверждает целостность и подлинность автора:
подпись = Sign(private_key_user, hash_passport) → 7fbd...ddc

Результирующая запись в блокчейне в формате json представлена на рис. 4.

```
{
  "block": {
    "timestamp": "2025-04-29T14:00:00Z",
    "previous_block_hash": "00000000000000000abcdef1234567890abcdef1234567890abcdef1234567",
    "merkle_root": "e17f3d6dff8e9c8b9e89a320b9a244aa16d865f6bbd5c1be0e3f99ed820d3e67",
    "transactions": [
      {
        "data": {
          "hash_name": "7961d285b143d2f3cdd812c2f3fe09cc79a328c7a9888f69a0d6a5cde3a718a2",
          "hash_passport": "533e703c0414a79bb23e1b2fa93ac3a34c5fd9458915908401c0479ae89754bd"
        },
        "signature": "7fbd76e3a92c1fa5bca877d831bbd4e8d94a9f3cde07c6f0d1ef6a9171ff8ddc",
"data_reference": {
    "storage_type": "relational_db",
    "dbms": "PostgreSQL",
    "host": "secure-db.gov.ru",
    "database": "personal_data_registry",
    "table": "citizen_data",
    "record_id": "987654",
    "field_hashes": {
      "full_name_hash": "7961d285b143d2f3cdd812c2f3fe09cc79a328c7a9888f69a0d6a5cde3a718a2",
      "passport_hash": "533e703c0414a79bb23e1b2fa93ac3a34c5fd9458915908401c0479ae89754bd "
    }
      }
    ],
    "block_hash": "abcde12345ff6789011122334455667788 99aabbccddeeff0011223344556677"
  }
}
```

Рис. 4. Результирующая запись в блокчейне в формате JSON
Источник: составлено авторами

Пример записи ПДн в таблицу базы данных

Field Name	Example Value	Data Type
full_name	Алексей Иванович Иванов	VARCHAR(255)
birth_date	0000-00-00	DATE
passport_number	0000 000000	VARCHAR(20)
address	Москва, ул. Пушкина, д. 00, кв. 00	VARCHAR(255)
phone_number	+7-000-000-00-00	VARCHAR(20)
email	alexey.ivanov@example.ru	VARCHAR(100)
snils	000-000-000 00	VARCHAR(20)
inn	000000000000	VARCHAR(20)
registration_date	2025-04-29	DATE
consent_to_processing	TRUE	BOOLEAN
id	######	INTEGER

Источник: составлено авторами.

В представленной системе непосредственно ПДн хранятся в реляционных базах данных, оформленных в виде таблиц со столбцами для имени, адреса, даты рождения и других атрибутов. Эти базы данных обычно используются в централизованных системах, и доступ к ним защищен механизмами аутентификации, шифрования и регулярных проверок доступа.

В таблице представлен расширенный набор ПДн гражданина Алексея Ивановича Иванова, организованный в виде таблицы реляционной базы данных.

Интеграция представленной гибридной системы хранения ПДн может быть эффективно согласована с основными существующими системами инфраструктуры ПДн с помощью четко определенных архитектурных и технологических механизмов.

Одним из основных преимуществ этой системы является ее совместимость с традиционными государственными и корпоративными информационными системами (ERP, CRM, реестры электронного правительства и системы цифровой идентификации) [8; 9]. Интеграция в первую очередь достигается с помощью защищенных интерфейсов (API), служб промежуточного ПО и блокчейн-оракулов, которые обеспечивают поток данных между слоем блокчейна и автономным слоем [10].

Ключевым механизмом такой интеграции является использование стандартизированных схем данных и реестров метаданных, которые обеспечивают семантическую и синтаксическую совместимость между метаданными блокчейна и существующими реляционными структурами. Использование открытых протоколов обмена данными, таких как RESTful или GraphQL API [11], и защищенных транспортных протоколов, таких как туннели TLS или VPN [12], обеспечивает конфиденциальность и целостность передаваемых данных во время межсистемного взаимодействия.

Кроме того, гибридная модель может быть согласована с системами цифровой идентификации, которые используются в биометрической аутентификации и национальных системах идентификации личности. С помощью цифровых сертификатов и инфраструктуры открытых ключей (PKI) [13; 14] слой блокчейна может проверять подлинность данных, взаимодействующих с внешними системами, такими как базы данных здравоохранения, реестры образовательных учреждений и хранилища юридической документации. Эти идентификационные данные криптографически закреплены в блокчейне, гарантируя, что все связанные системы ссылаются на один и тот же проверенный источник без копирования конфиденциальных данных.

На уровне предприятия интеграция с системами внутреннего аудита и системами управления данными достигается с помощью смарт-контрактов и механизмов ведения журнала (аудита), которые автоматически регистрируют события доступа и обработки ПДн. Эти записи на основе блокчейна являются неизменяемыми и могут быть связаны с централизованными журналами аудита для обеспечения всесторонней отчетности во всех подсистемах. Например, когда больница обновляет медицинские данные гражданина в защищенной реляционной базе данных, в блокчейн может быть записано соответствующее обновление хеша и подпись доступа, что обеспечивает отслеживаемость и соответствие как ИТ-стандартам, так и юридическим требованиям.

В случае международных или трансграничных систем этот гибридный подход также поддерживает интеграцию с федеративными сетями передачи данных, позволяя различным юрисдикциям сохранять кон-

троль над зашифрованными базами данных при одновременной синхронизации отпечатков данных с помощью взаимодействующих слоев системы. Это поддерживает требования GDPR к локализации и согласию пользователей, а также обеспечивает синхронизацию данных в режиме реального времени и аудит вне институциональных границ [15].

В целом, представленная гибридная архитектура позволяет сохранить инвестиции в устаревшую инфраструктуру, одновременно внедряя инновационные технологические решения в области хранения и обработки ПДн.

Заключение

Предлагаемая гибридная модель хранения персональных данных на основе блокчейна обеспечивает эффективное и безопасное решение, которое устраняет разрыв между децентрализованной прозрачностью блокчейна и централизованной конфиденциальностью. Разделение системы на уровни автономии, блокчейна и аудита позволяет обеспечить целостность данных, их непрерывный мониторинг и соответствие нормативным требованиям, таким как «право на забвение» и управление согласием пользователей.

Кроме того, модель демонстрирует высокую степень взаимодействия с существующими ИТ-инфраструктурами, включая правительственные и корпоративные базы данных, благодаря стандартизированным интерфейсам, сервисам промежуточного ПО и системам цифровой идентификации. Эта интеграция обеспечивает совместимость с устаревшими платформами при одновременном внедрении передовых криптографических средств контроля и неизменяемых контрольных журналов.

В целом, гибридная архитектура представляет собой значительный шаг на пути модернизации систем защиты данных, сочетая надежность и неизменность блокчейна с масштабируемостью и совместимостью традиционных решений для хранения данных.

Список литературы

1. Прокопенко А.Н. Борьба с утечками персональных данных – поможет ли ужесточение ответственности? // Вестник Казанского юридического института МВД России. 2024. №2 (56). С. 48-56. [Электронный ресурс]. URL: https://vestnikkui.ru/ru/nauka/article/81374/view (дата обращения: 09.10.2025). DOI: 10.37973/VESTNIKKUI-2024-56-7.

2. Ирзаев М.Г. Корпоративная база персональных данных сотрудников с доступом для мобильных клиентов // Перспективы развития информационных технологий. 2016. № 30. С. 74-79. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/korporativnaya-baza-personalnyh-dannyh-sotrudnikov-s-dostupom-dlya-mobilnyh-klientov (дата обращения: 09.10.2025).

3. Воробьев К.С. Проблемы правовой охраны баз данных в условиях цифровой экономики: между частным и публичным // Вопросы российской юстиции. 2022. № 22. С. 121-134; [Электронный ресурс]. URL: https://injust-journal.ru/?page_id=3108 (дата обращения: 09.10.2025).

4. Нажимова Н.А., Токарев С.В. Модель гибридной базы для хранения персональных данных на основе распределенной компьютерной сети blockchain // Современные наукоемкие технологии. 2025. № 10. С. 58–62. [Электронный ресурс]. URL: https://top-technologies.ru/ru/article/view?id=40528 (дата обращения: 09.10.2025). DOI: 10.17513/snt.40528.

5. Рязанова Е.Н. Ответственность за распространение персональных данных как способ противодействия правонарушениям в сфере информационно-коммуникационных технологий // Вестник Санкт-Петербургского университета МВД России. 2022. № 3 (95). С. 118-123. [Электронный ресурс]. URL: https://vestnikspbmvd.ru/ru/nauka/article/48998/view (дата обращения: 09.10.2025). DOI: 10.35750/2071-8284-2022-3-118-123.

6. Бродская Э.Г. Понятие и сущность защиты персональных данных // Экономика и социум. 2019. № 4 (59). С. 773-778. [Электронный ресурс]. URL: https://www.iupr.ru/_files/ugd/b06fdc_0d8e3a360c514eab84f18bb092e3a7fb.pdf (дата обращения: 09.10.2025).

7. 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. [Электронный ресурс]. URL: https://sccs.intelgr.com/archive/2021-02/03-Nosirov.pdf (дата обращения: 25.10.2025).

8. Сулимова Е.А. Цифровой инструментарий управления предприятиями: CRM, ERP, ECM, BI // Инновации и инвестиции. 2023. № 5. С. 158-160. [Электронный ресурс]. URL: https://innovazia.ru/upload/iblock/ea5/w04bvybk3aha5zchmam32c140143zo3p/%E2%84%965%202023%20%D0%98%D0%B8%D0%98.pdf (дата обращения: 09.10.2025).

9. Максимов А.А., Голубева О.Л., Волович Г.И., Некрасов С.Г. Миграция данных в контексте ERP-систем // Вестник ЮУрГУ. Серия: Компьютерные технологии, управление, радиоэлектроника. 2023. № 3. С. 118-129. [Электронный ресурс]. URL: https://vestnik.susu.ru/ctcr/article/download/13498/10166 (дата обращения: 09.10.2025). DOI: 10.14529/ctcr230310

10. Федосеев С.В. Информационные и программные аспекты разработки и применения смарт-контрактов // Правовая информатика. 2021. № 3. С. 25-33. [Электронный ресурс]. URL: http://uzulo.su/prav-inf/pdf-jpg/pi-2021-3-st3-s25-33.pdf (дата обращения: 09.10.2025).

11. Галигузова Е.В., Илларионова Ю.Е. Язык запросов GRAPHQL как замена REST API. Сравнение GRAPHQL и REST API // Символ науки. 2023. № 1-2. С. 9-11. [Электронный ресурс]. URL: https://os-russia.com/SBORNIKI/SN-2023-01-2.pdf (дата обращения: 09.10.2025).

12. Муратов Г.А. Особенности работы протокола TLS/SSL // Молодой исследователь Дона. 2021. № 3 (30). С. 67-70. [Электронный ресурс]. URL: https://mid-journal.ru/upload/mid/iblock/bf4/16_1327-Muratov_67_70.pdf (дата обращения: 09.10.2025).

13. Кобылат А.О., Рудская Е.Н. Биометрические инструменты управления банковскими рисками // Вестник магистратуры. 2014. № 7-2 (34). С. 65-75. [Электронный ресурс]. URL: https://www.magisterjournal.ru/docs/VM34_2.pdf (дата обращения: 09.10.2025).

14. Хорев П.Б., Лосев Д.А. Безопасный обмен файлами на основе сетей доверия и сертификатов открытых ключей с помощью разработанного приложения // Программные продукты и системы. 2024. № 2. С. 230-237. [Электронный ресурс]. URL: https://www.swsys.ru/download_full.php?journal=146 (дата обращения: 09.10.2025).

15. Чурилов А.Ю. Принципы общего Регламента Европейского союза о защите персональных данных (GDPR): проблемы и перспективы имплементации // Сибирское юридическое обозрение. 2019. № 1. С. 29-35. [Электронный ресурс]. URL: https://www.siberianlawreview.ru/jour/article/view/187/187 (дата обращения: 09.10.2025).

Конфликт интересов: Авторы заявляют об отсутствии конфликта интересов.

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