Доработанный вариант архитектуры с учетом блокчейна и квантозащищенности

В данном документе представлен доработанный вариант архитектуры, который включает в себя элементы блокчейна и квантозащищенности для повышения уровня безопасности обработки персональных данных. Описанные меры направлены на создание многоуровневой защиты, которая учитывает современные угрозы, связанные с квантовыми вычислениями, а также

1. Агент шифрования на стороне госоргана

- На сервере госоргана устанавливается специализированный агент, который при поступлении персональных данных выполняет первичное шифрование (формирование Хеш 1).
- Исходный ключ хранится исключительно на стороне госоргана, и доступ к нему строго ограничен.

Безопасная обработка персональных данных

Хранение ключей

Безопасное и ограниченное хранение криптографических ключей

Специализированный агент

Агент, ответственный за первичное шифрование данных

Первичное шифрование

Процесс создания первого хеша данных

2. Распределённое добавление ключевых компонентов

- Ключевые компоненты для шифрования данных передаются в центральную ETL-систему (на базе Apache Airflow), где два или три независимых сервиса добавляют свои компоненты (Второй и Третий хеш).
- Итоговый составной ключ формируется только при наличии всех компонентов, что исключает возможность восстановления данных одним

Процесс шифрования и формирования ключа

Первичное шифрование данных

Данные шифруются для обеспечения безопасности

Добавление сервиса 1

Первый сервис добавляет свой компонент

Формирование составного ключа

Создается составной ключ из всех компонентов

Передача в систему ETL

Шифрованные данные передаются в систему ETL

Добавление сервиса 2

Второй сервис добавляет свой компонент

KEY

3. Управление секретами через централизованный сервис

- Все ключевые компоненты хранятся и управляются через систему управления секретами, например, HashiCorp Vault.
- Это гарантирует, что даже администратор центральной системы не сможет самостоятельно получить полный доступ к ключам.

Управление секретами и защита ключей

Хранение ключей

Шифрование

Резервное копирование

KEY

Система управления секретами

Управление доступом

Аутентификация

Авторизация

Защита данных

Квантовая защита

Блокчейн-аудит

4. Изоляция доступа и аудит

- Центральная система ETL получает только итоговую зашифрованную таблицу (T2), а доступ к исходным данным и первичному хешу остаётся
- Все операции доступа к ключам и данным фиксируются с помощью систем аудита (например, Teleport), что обеспечивает прозрачное журналирование

Компоненты безопасной обработки данных

Мониторинг

Центральная система ETL

Аудит доступа к данным

5. Интеграция блокчейн-технологии для аудита и целостности

- Для повышения прозрачности и неизменности логов операций можно интегрировать блокчейн платформу.
- Каждая транзакция (например, операция шифрования, добавление ключевых компонентов или обращение к данным) записывается в блокчейн, что позволяет создать неизменяемую историю доступа и операций.

Раскрытие силы блокчейна в операциях

Интеграция блокчейна

1

Улучшенная прозрачность

2

Неизменяемые журналы

3

Запись транзакций

4

История доступа

6. Квантозащищённость и квантовые разрывы с запутанностями

- Для защиты от угроз квантовых вычислений можно использовать квантово-устойчивые алгоритмы шифрования, которые обеспечат безопасность даже при появлении квантовых компьютеров.
- Дополнительно можно рассмотреть применение концепций квантовой криптографии (например, квантового распределения ключей) для усиления
- Идея "квантовых разрывов" и запутанности может быть использована для проверки целостности данных и аутентификации между узлами системы, что ещё больше усложнит несанкционированное вмешательство.

Квантовая защита архитектуры

1

Алгоритмы шифрования для защиты от квантовых вычислений.

Квантово-устойчивые алгоритмы

2

Использование квантовой криптографии для безопасного обмена ключами.

Квантовая криптография

3

Проверка целостности данных с помощью запутанности.

Запутанность и разрывы

Улучшенная безопасность системы

Конкретное доработанное предложение

Развернуть на стороне госоргана специализированный агент, который при поступлении персональных данных выполняет первичное шифрование (Хеш 1) с использованием квантово-устойчивых алгоритмов. Далее данные передаются в центральную ETL-систему (например, на базе Airflow), где два-три независимых сервиса добавляют свои ключевые компоненты, формируя итоговый составной ключ. Все ключевые компоненты хранятся в HashiCorp Vault, а доступ к ним контролируется через систему аудита с использованием Teleport. Кроме того, каждая операция (от шифрования до доступа) регистрируется в блокчейне для создания неизменяемого журнала, подтверждающего целостность и прозрачность

Архитектура защиты персональных данных с квантозащитой

Аудит и прозрачность

Система аудита

Блокчейн

Квантовое распределение ключей

Агент шифрования

Центральная ETL-система

Airflow

Независимые сервисы

Хранение ключей

HashiCorp Vault

Такой комплексный подход объединяет традиционные и передовые технологии, обеспечивая не только многоуровневую защиту персональных данных, но и готовность системы к будущим угрозам, связанным с квантовыми вычислениями и