АО «Концерн ГРАНИТ»
АКЦИОНЕРНОЕ ОБЩЕСТВО

Система распределенного хранения данных

«КВАНТ-РЕЕСТР»

Пояснительная записка

2021

АННОТАЦИЯ

Настоящая Пояснительная записка определяет назначение, общие и специальные требования назначение, общие и специальные требования к системе распределенного хранения данных «КВАНТ-РЕЕСТР» (далее – комплексной информационной системе «Квант-реестр», КИС «Квант-реестр», Системе), предназначенной для использования в качестве децентрализованного и защищенного хранения файлов с поддержкой доверенных временных меток.

СОДЕРЖАНИЕ

1. ВВЕДЕНИЕ

1.1. Наименование Системы

Система распределенного хранения данных «КВАНТ-РЕЕСТР» (далее комплексная информационная система «Квант-реестр» (далее по тексту – КИС, Система).

1.2. Краткое описание Системы

Комплексная информационная система «Квант-реестр» для децентрализованного и защищенного файлового хранилища, что значительно снижает риски потери и повреждения данных. В Системе применены современные криптографические методы, в результате чего становится невозможным подмена файлов, а также появляется возможность предоставления математически подкрепленных доказательств неизменяемости хранимых файлов с течением времени.

2. НАЗНАЧЕНИЕ РАЗРАБОТКИ СИСТЕМЫ

Результатом разработки Системы является специализированный инструмент для децентрализованного хранения файлов с поддержкой доверенных временных меток, необходимый для использования нескольких независимых сторон (организаций) для решения специфических задач.

Система представляет собой цифровую платформу, применимую для широкого круга пользователей государственных информационных систем, приложений, а также для корпоративных отделов по цифровой трансформации предприятий крупного и среднего бизнеса.

3. ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

3.1. Постановка задачи и выбор методов решения

Система обеспечивает выполнение следующих функций:

1) формирование приватного элемента для пользователя с гарантированными вероятностными свойствами, т.е. пользователь должен иметь приватный идентификатор или ключ, никому не известный кроме него, выработанный при помощи датчика случайных чисел с гарантированными статистическими свойствами, или взаимодействие с функцией подписи аппаратного средства электронной подписи, соответствующего требованиям 63-ФЗ «Об электронной подписи»;

2) формирование сетевого имени (идентификатора, которым пользователь представляется в системе) на основе указанного выше приватного элемента, исключающего возможность выявления связей между сетевым именем и множеством открытых данных о физическом лице или организации, или взаимодействие с функцией предоставления открытого ключа аппаратного средства электронной подписи, соответствующего требованиям 63-ФЗ «Об электронной подписи»;

3) безопасное хранение приватного элемента у пользователя для обеспечения защищенности от несанкционированного доступа к нему или хранение приватного элемента на стороне аппаратного средства электронной подписи, соответствующего требованиям 63-ФЗ «Об электронной подписи».;

4) наличие «точки входа» для пользователя (оператора) распределенного реестра;

5) авторизация пользователя для оператора при помощи электронной подписи, использующей приватный элемент пользователя;

6) безопасный транспорт (как минимум с сохранение неизменности информации, получаемой от пользователя) для передачи информации от пользователя к оператору распределенного реестра;

7) контроль целостности и авторства каждой информационной единицы, помещаемой в распределенный реестр, с помощью электронной подписи пользователя;

8) формирование подтверждений у оператора распределенного реестра факте помещения информации в распределенный реестр (например, путем выдачи заверенных оператором квитанций пользователям);

9) наличие механизма формирования и обработки запросов по выдаче информации из распределенного реестра по запросам его участников (клиентов), обеспечивающего защищенность данного запроса (также авторизацию и контроль неизменности запроса)

10) хранение файлов в экземплярах СУБД;

11) хранение метаинформации о файлах в логе транзакций блокчейна;

12) поиск файлов по уникальному идентификатору;

13) отправка метаинформации о файлах по запросу;

14) контроль доступа пользователей к хранимым данным;

15) организация необходимой структуры базы данных;

16) получение информации об установленной версии QHB;

17) проверка состояния соединения с сервером базы данных;

18) возможность выполнения метакоманд, а таже различных функций для автоматизации широкого спектра задач;

19) создание и удаление экземпляра базы данных;

20) создание и удаление новой учетной записи;

21) запись данных в базу, обеспечение записи данных, вводимых пользователем в БД через интерактивный терминал qsql;

22) управление хранением данных;

23) чтение данных (выполнение запросов пользователя на получение интересующих данных);

24) редактирование существующих записей;

25) удаление записей;

26) реализация поддержки языка описания данных и языка запросов;

27) обеспечение восстановления БД после сбоя;

28) создание резервной копии кластера QHB;

29) непрерывное архивирование и восстановление на момент времени журнала упреждающей записи (WAL);

30) кластеризация БД;

31) переиндексация БД;

32) организация синхронного и асинхронного взаимодействия клиентских приложений с БД;

33) индексирование, позволяющее оптимизировать производительность базы данных;

34) параллелизм;

35) функция больших объектов, обеспечивающая потоковый доступ к пользовательским данным;

36) ввод запросов в интерактивном режиме, из файла, конвейера ранее запущенной программы, из аргументов командной строки на пользовательской консоли;

37) очистка БД и генерация внутренней статистики.

3.2. Описание структуры Системы и алгоритма решения задачи

Система реализована в многозвенной гибридной архитектуре, где быть предусмотрены:

1. Система управления базами данных «Квант-гибрид» (далее СУБД), включающая в себя:
   1.1. Балансировщик сетевой нагрузки предназначенный для оптимального использования серверных подключений;
   1.2. Серверный процесс, организующий фоновую запись на диск;
   1.3. Модуль для внешнего хранения больших бинарных объектов с сохранением способа их обработки в прикладных системах;
   1.4. Пользовательская консоль для выполнения команд базы данных и запросов на языке SQL;

1.5. Бинарные утилиты для управления СУБД;

1.6. Подсистема интернационализации i18n;

2. Система распределенного реестра, включающая в себя:

2.1. Модуль ЭЦП, включая аутентификацию с применением ЭЦП, а также подписание файлов посредством ЭЦП;

2.2. Модуль формирования файла для передачи оператору распределенного реестра;

2.3. Модуль проверки и экстракции файла;

2.4. Модуль записи в распределенный реестр;

2.5. Модуль извлечения информации из распределенного реестра по номеру звена;

2.6. Модуль сервера распределенного реестра.

3. Презентационный слой, обеспечивающий доступ пользователей к системе через WEB-интерфейс.

Для работы Системы предусмотрены Открытый и Закрытый сегменты, а также механизм обмена данными между этими сегментами. Клиент и сервер могут находиться как на одном, так и на разных компьютерах.

Система обеспечивает возможность обслуживания одновременно нескольких клиентских сессий, при этом пользователю гарантируется непротиворечивость и целостность возвращаемых данных. Для обслуживания нескольких конкурентных сессий, используется механизм порождения необходимого количества серверных процессов, каждый из которых в конкретный момент времени обслуживает запрос на языке SQL. Механизм организован следующим образом:

- серверные процессы порождаются диспетчером соединений, который ожидает подключения по сети или через механизм межпроцесного взаимодействия операционной системы;
- диспетчер соединений принимает входящие соединения;
- диспетчер соединений устанавливает сетевой сеанс связи;
- подключается к серверному процессу или порождает его.

3.3. Решения по составу и параметрам технических средств

Техническое обеспечение учитывает имеющиеся стандартные технические решения и оборудования Заказчика. Ниже, в таблице (Таблица 1) представлены требования к Системе и программному обеспечению.

Таблица 1 - Требования к Системе и программному обеспечению

№ п/п	Техническое средство/программное обеспечение	Характеристики	Примечание
1	Процессор	Процессоры архитектур: x86-64 ARM Эльбрус	
2	Операционная система	Семейство Linux на всех вышеуказанных архитектурах	
3	Оперативная память	Не менее 4 ГБ оперативной памяти	
4	Жесткий диск	Не менее 200 МБ (не учитывая размер базы данных)	При выборе дискового пространства для базы данных необходимо ориентироваться на конкретную задачу

3.4. Решения по информационной и программной совместимости

В Системе предусмотрены средства контроля входной информации, обновления данных в информационных массивах, контроля целостности базы данных.

Средства СУБД, а также средства используемых ОС обеспечивают документирование и протоколирование информации.

3.5. Решения по внешним интерфейсам

3.5.1. Интерфейсы пользователя

В Системе предусмотрено взаимодействие Пользователей с узлами, используя заранее определенный набор HTTP REST интерфейсов. Все возможные взаимодействия могут быть разделены на две группы:

1) Транзакции - команды, требующие от узла выполнить какое-либо действие. Набор транзакций узла определяется в его исходном коде и не может быть изменен без обновления узла. Каждая транзакция представляет собой HTTP POST запрос, содержащий сериализованное в JSON сообщение, которое должно состоять из Тела транзакции, Внутренней метаинформации и ЭЦП.
   - Тело транзакции содержит полезную нагрузку транзакции – определенные данные, позволяющие узлы выполнить определенную бизнес-логику. Например, транзакция добавления нового пользователя содержит идентификатор пользователя и его публичный ключ.
   - Внутренняя метаинформация транзакции используется узлом, чтобы различать различные типы транзакций между собой и выполнять другие внутренние действия, требуемые для обработки транзакции.
   - ЭЦП позволяет однозначно идентифицировать автора транзакции и гарантирует, что транзакция была собственноручно сформирована и отправлена именно этим пользователем.

Все части транзакции сериализовываются в формате Protobuf, чтобы упростить хранение и обработку транзакций.

2) Запросы представляют собой HTTP GET запросы, используемые для выполнения запросов определенной информацию у узла. Каждый запрос должен содержать данные, необходимые для его обработки. Например, запрос информации о пользователе должен содержать идентификатор этого

пользователя. Чтобы защититься от неавторизованного доступа, каждый запрос, как и транзакции, должен быть подписан ЭЦП отправителя.

Набор транзакций и запросов, доступных пользователю, зависит от его роли. В то время, как администраторы сети обладают наиболее богатым набором доступных транзакций и запросов, обычные пользователи имеют доступ только к ограниченному набору запросов.

Объем информации, отдаваемой в ответ на запрос, может зависеть от набора полномочий пользователя, которые регулируются администраторами сети.

3.5.2. Интерфейсы программного обеспечения

Система содержит ГОСТ-сертифицированный криптографический модуль, который поддерживает:

- Хеширование.
- Использование и проверку ЭЦП.
- Генерацию и использование публичных и приватных ключей.

3.6. Решения по идентификации и аутентификации

В Системе реализована идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю. Для аутентификации используется символьный периодически изменяющийся пароль из не менее чем 6 символов при мощности алфавита не менее 10.

3.7. Решения по регистрации и учёту действий (аудиту)

В Системе осуществляется регистрация входа/выхода субъектов доступа в систему/из системы, регистрация загрузки и инициализации операционной системы и ее программного останова. В параметрах регистрации указываются: время и дата входа/выхода субъекта доступа в систему/из системы или загрузки/останова системы.

Для результата попытки входа регистрируются: успешный или неуспешный несанкционированный, идентификатор субъекта, предъявленный при попытке доступа.

Администратором задается максимальное количество неудачных попыток аутентификации пользователя, при превышении которого производится блокировка рабочей станции.

3.8. Решения по обеспечению целостности

Реализованы механизмы (процедуры) контроля несанкционированного случайного и/или преднамеренного искажения (изменения, модификации) и/или разрушения компонентов, содержащих исполняемый код. В Системе проводится периодическое тестирование функций СЗИ, а также проверяется целостность компонент СЗИ при каждой загрузке/перезагрузке системы средствами доверенной загрузки.

3.9. Решения по защите передаваемой и хранимой информации

Реализована защита всей конфиденциальной информации, передаваемой по каналам связи. Информация, передаваемая по каналам связи, зашифрована с использованием СКЗИ. Реализована защита информации, записываемой на отчуждаемые носители.

3.10. Решения по средствам криптографической защиты информации

СКЗИ соответствует «Требованиям к средствам криптографической защиты конфиденциальной информации» по классу, достаточному для выполнения требований по соответствующему классу КС3.

3.11. Решения по информационной безопасности

Неавторизованный доступ к узлам и их компонентам ограничен использованием физических и программных методов. В Системе реализовано ограничение доступа для неавторизованных пользователей к приватным и публичным API, но администраторы сети полностью ответственны за защиту от всех видов атак и злонамеренной активности.

3.12. Решения по программному обеспечению

Анализ интегрированных СЗИ проводится на уровне исходных текстов. Предоставление исходных текстов для дополнительных модулей и интегрируемых СЗИ обеспечивается их разработчиком.

4. РЕШЕНИЯ ПО ПРОГРАММНОЙ ДОКУМЕНТАЦИИ

Документация технического проекта и эксплуатационная документация Системы разработана в соответствии с РД 50-34.698-90 «Методические указания «Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов».

Документация передана в виде подлежащих текстовому редактированию файлов в формате офисных приложений Microsoft Word или Open Office (*.doc/*.docx или *.odt), а также на бумажном носителе в количестве двух экземпляров.

ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ

Сокращение, обозначение	Расшифровка
CD/DVD	Compact Disc (компакт диск) / Digital Versatile Disc (цифровой многоцелевой диск)
CPU	Центральный процессор (с англ. «Central processing unit»)
Fiber Channel	Семейство протоколов для высокоскоростной передачи
HTTP	Протокол прикладного уровня передачи данных (с англ. «HyperText Transfer Protocol»)
IP	Маршрутизируемый протокол сетевого уровня стека TCP/IP (с англ. «Internet protocol» – межсетевой протокол)
REST	Метод взаимодействия компонентов распределённого приложения в сети Интернет, при котором вызов удаленной процедуры представляет собой обычный HTTP-запрос, а необходимые данные передаются в качестве параметров запроса (с англ. «Representational state transfer»)
АБИ	Администратор безопасности информации
АПМДЗ	Аппаратно-программный модуль доверенной загрузки
АРМ	Автоматизированное рабочее место
БД	База данных
ГОСТ	Государственный стандарт
ЕПП	Единое пространство пользователей
КСПД	Корпоративная сеть передачи данных
ЛВС	Локальная вычислительная сеть

Сокращение, обозначение	Расшифровка
НСД	Несанкционированный доступ
ОС	Операционная система
ОЭ	Опытная эксплуатация
ПО	Программное обеспечение
ПС	Программные средства
ПЭВМ	Персональная электронная вычислительная машина
РД	Руководящий документ
СЗИ	Средство защиты информации
СПО	Специальное программное обеспечение
СУБД	Система управления базами данных
ТЗ	Техническое задание
ТП	Технологический проект
УЗНИ	Учёт защищаемых носителей информации
УСЗИ	Модуль управления средствами защиты информации
ЭВМ	Электронная вычислительная машина

Термины и определения

Термин	Определение
Блокчейн	Выстроенная по определённым правилам непрерывная последовательная цепочка блоков, содержащих информацию. Связь между блоками обеспечивается не только нумерацией, но и тем, что каждый блок содержит свою собственную хеш-сумму и хеш-сумму предыдущего блока. Для изменения информации в блоке придётся редактировать и все последующие блоки. Чаще всего копии цепочек блоков хранятся на множестве разных компьютеров независимо друг от друга. Это делает крайне затруднительным внесение изменений в информацию, уже включённую в блоки. Блокчейн децентрализовано хранится на узлах распределенной компьютерной сети.
Консенсус	Механизм, используемый в распределенных системах и блокчейнах, предназначенный для достижения согласованного состояния между несколькими независимыми агентами или процессами.
Конфигурация сети	Набор параметров, определяющих поведение сети. Он включает параметры алгоритма консенсуса, например, время принятия блоков, список узлов сети, список пользователей и их прав.
Узел	Устройство, хранящее полную копию истории транзакций блокчейна и соединенное с другими узлами сети. Узлы доступны для пользователей через их приватные и публичные API.
Доверенная временная метка	Процесс надёжного отслеживания времени создания и изменения документа. Надёжность подразумевает, что никто (включая владельца) не сможет внести изменение во

Термин	Определение
	временную метку после её создания при условии, что целостность метки не будет нарушена.