

Категория	Требование	Соответствует	Реализация
1.1 Общие требования СУБД	СУБД должна быть включена в «Единый реестр российских программ для электронных вычислительных машин и баз данных» ( <a href="https://reestr.digital.gov.ru/">https://reestr.digital.gov.ru/</a> ).	да	номер реестровой записи: 18509 <a href="https://reestr.digital.gov.ru/reestr/1683980/?sphrase_id=4598709">https://reestr.digital.gov.ru/reestr/1683980/?sphrase_id=4598709</a>
1.2 Общие требования QSS	Модуль шифрования должен быть включен в «Единый реестр российских программ для электронных вычислительных машин и баз данных» ( <a href="https://reestr.digital.gov.ru/">https://reestr.digital.gov.ru/</a> ).	да	номер реестровой записи: 21868 <a href="https://reestr.digital.gov.ru/reestr/2224134/?sphrase_id=4598647">https://reestr.digital.gov.ru/reestr/2224134/?sphrase_id=4598647</a>
1.1 Общие требования СУБД	СУБД должна иметь сертификат ФСТЭК России на соответствие «Требованиям по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) – не ниже 4 уровня доверия.	да	Сертификат: 4691 от 12.07.2023
1.2 Общие требования QSS	Должен иметь сертификат соответствия ФСБ России на соответствие требованиям к средствам криптографической защиты информации класса КС2.	да	Сертификат: СФ/124-4721 от 15.01.2024
2.1 Требования к структуре и функционированию СУБД	СУБД должна функционировать на ЭВМ с характеристиками не ниже следующих: –процессор архитектур: x86-64, с тактовой частотой 1,8 ГГц; –оперативная память: не менее 4 Гбайт оперативной памяти; –жёсткий диск: не менее 400 МБ (не учитывая размер базы данных); –устройство чтения компакт-дисков; –звуковая карта; –сетевая плата Fast Ethernet 100 Мбит/с.	да	СУБД функционирует на ЭВМ с характеристиками не ниже следующих: - процессор архитектур: x86-64, с тактовой частотой 1,8 ГГц; - оперативная память: не менее 4 Гбайт оперативной памяти; - жёсткий диск: не менее 400 МБ (не учитывая размер базы данных); - устройство чтения компакт-дисков; -звуковая карта; -сетевая плата Fast Ethernet 100 Мбит/с.

2.1 Требования к структуре и функционированию СУБД	СУБД должна функционировать в среде ОС на базе Linux: - операционная система Альт 8 СП (обозначение программного изделия — ЛКНВ.11100-01) (№ сертификата 3866); - операционная система специального назначения «Astra Linux Special Edition» (в исполнении РУСБ.10015-01) x86_64, очередное обновление 1.7, (№ сертификата 2557); - операционная система «РЕД ОС» (№ сертификата 4060).	да	СУБД функционирует в среде ОС на базе Linux: - операционная система Альт 8 СП (обозначение программного изделия — ЛКНВ.11100-01) (№ сертификата 3866); - операционная система специального назначения «Astra Linux Special Edition» (в исполнении РУСБ.10015-01) x86_64, очередное обновление 1.7, (№ сертификата 2557); - операционная система «РЕД ОС» (№ сертификата 4060).
2.2 Требования к структуре и функционированию QSS	QSS должно функционировать на ЭВМ с характеристиками не ниже следующих (не считая требований самой ОС): – процессоры архитектуры (только для 64 битных CPU): x86-64 с тактовой частотой не менее 2 ГГц; – оперативная память: не менее 4 ГБ оперативной памяти; – жёсткий диск: не менее 1 ГБ.	да	QSS функционирует на ЭВМ с характеристиками не ниже следующих (не считая требований самой ОС): – процессоры архитектуры (только для 64 битных CPU): x86-64 с тактовой частотой не менее 2 ГГц; – оперативная память: не менее 4 ГБ оперативной памяти; – жёсткий диск: не менее 1 ГБ.
2.2 Требования к структуре и функционированию QSS	QSS должна функционировать в среде ОС на базе Linux: - операционная система Альт 8 СП (обозначение программного изделия — ЛКНВ.11100-01) (№ сертификата 3866); - операционная система специального назначения «Astra Linux Special Edition» (в исполнении РУСБ.10015-01) x86_64, очередное обновление 1.7, (№ сертификата 2557); - операционная система «РЕД ОС» (№ сертификата 4060).	да	QSS функционирует в среде ОС на базе Linux: – CentOS 7 и 8; – РЕД ОС; – ROSA Enterprise Linux Server (RELS); – РОСА «Кобальт»; – Альт 8 СП; – Альт Сервер 9; – Fedora 33, 34 и 35; – Debian 9 и 10; – Astra Linux Special Edition «Смоленск» 1.6, 1.7; – Ubuntu 18.04 LTS и 22.04 LTS; – openSUSE 15.4.
2.1 Требования к структуре и функционированию СУБД	Отсутствие ограничений на размер БД	да	Отсутствие ограничений на размер БД
2.1 Требования к структуре и функционированию СУБД	Поддержка не менее 4 000 000 баз данных	да	Количество баз данных: 4 294 950 911
2.1 Требования к структуре и функционированию СУБД	Поддержка таблиц не менее 30 ТБ	да	Поддержка таблиц до 32 ТБ

2.1 Требования к структуре и функционированию СУБД	Поддержка записей (строк) размером не более 500 ГБ	да	Поддержка записей (строк) размером не более 500 ГБ
2.1 Требования к структуре и функционированию СУБД	Поддержка полей (столбцов) / BLOB любых размеров до 1 ГБ	да	Поддержка полей (столбцов) / BLOB любых размеров до 1 ГБ
2.1 Требования к структуре и функционированию СУБД	Отсутствие ограничений на количество индексов	да	Отсутствие ограничений на количество индексов
2.1 Требования к структуре и функционированию СУБД	Поддержка 1500 полей (столбцов) в одной таблице	да	Поддержка до 1600 полей (столбцов) в одной таблице
2.1 Требования к структуре и функционированию СУБД	Обеспечивать журнал упреждающей записи (Write-Ahead Logging - WAL), механизм протоколирования транзакций, что позволяет восстановить систему после возможных сбоев: все изменения должны записываться на диск после того, как записи журнала, описывающие эти действия, будут гарантировано записаны на диск. Это должно позволять не сбрасывать страницы данных на диск после фиксации каждой транзакции, так как всегда есть возможность восстановления базы данных используя журнал транзакций.	да	В СУБД реализован журнал упреждающей записи (Write-Ahead Logging - WAL), механизм протоколирования транзакций, что позволяет восстановить систему после возможных сбоев. Основная идея WAL состоит в том, что все изменения должны записываться на диск после того, как записи журнала, описывающие эти действия, будут гарантировано записаны на диск. Это позволяет не сбрасывать страницы данных на диск после фиксации каждой транзакции, так как всегда есть возможность восстановления базы данных используя журнал транзакций.
2.2 Требования к структуре и функционированию QSS	Для генерации случайных последовательностей СКЗИ QSS должен использовать ФДСЧ, имеющий сертификат соответствия ФСБ России по классу не ниже 2Б.	да	Для генерации случайных последовательностей СКЗИ QSS использует ФДСЧ, имеющий сертификат соответствия ФСБ России по классу не ниже 2Б (ФДСЧ из состава механизмов доверенной загрузки, имеющих сертификаты соответствия ФСБ России по классу 2Б и выше).
2.2 Требования к структуре и функционированию QSS	Должна быть реализована возможность работы совместно с ПАК СОБОЛЬ и СЗИ НСД «Аккорд-АМДЗ» в части доверенной загрузки и получения случайных последовательностей	да	Реализована возможность работы совместно с ПАК СОБОЛЬ и СЗИ НСД «Аккорд-АМДЗ» в части доверенной загрузки и получения случайных последовательностей

3.1 Требования к стандартизации и унификации СУБД	<p>СУБД должна поддерживать следующие стандартные, унифицированные типы данных:</p> <ul style="list-style-type: none"> <li>- числовые типы (целочисленные типы: INT, SMALLINT, BIGINT; числа с произвольной точностью; типы с плавающей точкой: REAL, DOUBLE PRECISION, FLOAT; последовательные типы);</li> <li>- денежные типы;</li> <li>- символьные типы данных: VARCHAR(n), CHAR(n), TEXT;</li> <li>- двоичные типы данных;</li> <li>- типы даты и времени: DATE, TIME, TIMESTAMP, TIMESTAMP WITH TIMEZONE, INTERVAL;</li> <li>- логический тип BOOLEAN;</li> <li>- типы перечислений;</li> <li>- геометрические типы;</li> <li>- типы, описывающие сетевые адреса;</li> <li>- битовые строки;</li> <li>- типы данных, предназначенные для текстового поиска;</li> <li>- UUID;</li> <li>- XML;</li> <li>- JSON/JSONB;</li> <li>- массивы;</li> <li>- составные типы;</li> <li>- диапазонные типы;</li> <li>- типы доменов;</li> <li>- идентификаторы объектов;</li> <li>- тип pg_lsn;</li> <li>- псевдотипы.</li> </ul>	да	СУБД поддерживает стандартные, унифицированные типы данных.
3.2 Требования к стандартизации и унификации QSS	Криптографическая защита должна соответствовать требованиям ГОСТ: ГОСТ Р 34.13-2015, ГОСТ 34.13-2018, ГОСТ Р 34.12-2015, ГОСТ 34.12-2018, ГОСТ Р 34.11-2012, ГОСТ 34.11-2018 и стандартам: Р 1323565.1.026–2019, Р 50.1.111-2016, Р 50.1.113-2016	да	Криптографическая защита соответствует требованиям ГОСТ: ГОСТ Р 34.13-2015, ГОСТ 34.13-2018, ГОСТ Р 34.12-2015, ГОСТ 34.12-2018, ГОСТ Р 34.11-2012, ГОСТ 34.11-2018 и стандартам: Р 1323565.1.026–2019, Р 50.1.111-2016, Р 50.1.113-2016
4.1 Требования к функциям (задачам), выполняемым СУБД	Соответствие стандарту SQL (SQL:2016, SQL:2011, SQL:2008, SQL:2006, SQL:2003, SQL:1999 и SQL-92);	да	Соответствие стандарту SQL (SQL:2016, SQL:2011, SQL:2008, SQL:2006, SQL:2003, SQL:1999 и SQL-92);

4.2 Требования к функциям (задачам), выполняемым QSS	Аутентификация при установлении административного соединения по паролю и дополнительной случайной информации (с опциональным её хранением на внешнем носителе) с использованием алгоритма выработки ключа из пароля по алгоритму «PBKDF2» в соответствии с «Р 50.1.111-2016»	да	Аутентификация при установлении административного соединения по паролю и дополнительной случайной информации (с опциональным её хранением на внешнем носителе) с использованием алгоритма выработки ключа из пароля по алгоритму «PBKDF2» в соответствии с «Р 50.1.111-2016»
4.2 Требования к функциям (задачам), выполняемым QSS	Диверсификация ключей с использованием алгоритма KDF_GOSTR3411_2012_256 в соответствии с «Р 50.1.113-2016»	да	Диверсификация ключей с использованием алгоритма KDF_GOSTR3411_2012_256 в соответствии с «Р 50.1.113-2016»
4.2 Требования к функциям (задачам), выполняемым QSS	Аутентифицированное шифрование/расшифрование данных (с использованием разделяемой памяти/ через сокеты) в соответствии с «Р 1323565.1.026—2019» (алгоритмом «Кузнечик» в соответствии с «ГОСТ 34.12—2018»)	да	Аутентифицированное шифрование/расшифрование данных (с использованием разделяемой памяти/ через сокеты) в соответствии с «Р 1323565.1.026—2019» (алгоритмом «Кузнечик» в соответствии с «ГОСТ 34.12—2018»)
4.2 Требования к функциям (задачам), выполняемым QSS	Формирование и проверка электронной подписи в соответствии с «ГОСТ 34.10-2018» и параметрами эллиптических кривых, определёнными в «Р 1323565.1.024-2019»	да	Формирование и проверка электронной подписи в соответствии с «ГОСТ 34.10-2018» и параметрами эллиптических кривых, определёнными в «Р 1323565.1.024-2019»
4.2 Требования к функциям (задачам), выполняемым QSS	Формирование общих ключей по алгоритму «VKO» в соответствии с «Р 50.1.113-2016»	да	Формирование общих ключей по алгоритму «VKO» в соответствии с «Р 50.1.113-2016»
4.2 Требования к функциям (задачам), выполняемым QSS	Вычисление хеш-суммы от блока данных в соответствии с «ГОСТ 34.11-2018»	да	Вычисление хеш-суммы от блока данных в соответствии с «ГОСТ 34.11-2018»
4.2 Требования к функциям (задачам), выполняемым QSS	Управление ключевой информацией	да	Управление ключевой информацией
4.2 Требования к функциям (задачам), выполняемым QSS	Хранение ключей в зашифрованном и имитозащищенном виде в долговременном хранилище	да	Хранение ключей в зашифрованном и имитозащищенном виде в долговременном хранилище
4.2 Требования к функциям (задачам), выполняемым QSS	Управление администраторами QSS	да	Управление администраторами QSS
4.1 Требования к функциям (задачам), выполняемым СУБД	Поддержка представлений	да	Поддержка представлений
4.1 Требования к функциям (задачам), выполняемым СУБД	Поддержка внешних ключей	да	Поддержка внешних ключей
4.1 Требования к функциям (задачам), выполняемым СУБД	Поддержка транзакций	да	Поддержка транзакций

4.1 Требования к функциям (задачам), выполняемым СУБД	Поддержка оконных функций	да	Поддержка оконных функций
4.1 Требования к функциям (задачам), выполняемым СУБД	Поддержка наследований	да	Поддержка наследований
4.1 Требования к функциям (задачам), выполняемым СУБД	Поддержка функций и операторов	да	Поддержка функций и операторов
4.1 Требования к функциям (задачам), выполняемым СУБД	Поддержка хранимых процедур	да	Поддержка хранимых процедур
4.1 Требования к функциям (задачам), выполняемым СУБД	Поддержка различных типов индексов: B-tree, hash, GiST, SP-GiST, GIN, BRIN (B+-tree, partial sum tree, ranked B+-tree, R-tree)	да	Поддержка различных типов индексов: B-tree, hash, GiST, SP-GiST, GIN, BRIN (B+-tree, partial sum tree, ranked B+-tree, R-tree)
4.1 Требования к функциям (задачам), выполняемым СУБД	Наличие встроенной системы полнотекстового поиска	да	Наличие встроенной системы полнотекстового поиска
4.1 Требования к функциям (задачам), выполняемым СУБД	Поддержка табличных пространств	да	Поддержка табличных пространств
4.1 Требования к функциям (задачам), выполняемым СУБД	Поддержка табличных триггеров БД и триггеров событий	да	Поддержка табличных триггеров БД и триггеров событий
4.1 Требования к функциям (задачам), выполняемым СУБД	Поддержка процедурных языков, в т.ч. PL/pgSQL, PL/Perl, PL/Python, PL/Tcl	да	Поддержка процедурных языков, в т.ч. PL/pgSQL, PL/Perl, PL/Python, PL/Tcl
4.1 Требования к функциям (задачам), выполняемым СУБД	Поддержка кодировки UTF8	да	Поддержка кодировки UTF8
4.1 Требования к функциям (задачам), выполняемым СУБД	Поддержка NoSQL	да	Поддержка NoSQL
4.1 Требования к функциям (задачам), выполняемым СУБД	Наличие программных интерфейсов для работы с C/C++, Java/JDBC, ODBC, Perl, Python, Ruby	да	Наличие программных интерфейсов для работы с C/C++, Java/JDBC, ODBC, Perl, Python, Ruby
4.1 Требования к функциям (задачам), выполняемым СУБД	Наличие встроенных средств аутентификации пользователей, поддерживающих GSSAPI, SSPI, LDAP, RADIUS, PAM, BSD	да	Наличие встроенных средств аутентификации пользователей, поддерживающих GSSAPI, SSPI, LDAP, RADIUS, PAM, BSD
4.1 Требования к функциям (задачам), выполняемым СУБД	Поддержка SSL	да	Поддержка SSL
4.1 Требования к функциям (задачам), выполняемым СУБД	Возможность разграничения доступа к объектам БД	да	Возможность разграничения доступа к объектам БД
4.1 Требования к функциям (задачам), выполняемым СУБД	Возможность безопасного хранения паролей	да	Возможность безопасного хранения паролей
4.1 Требования к функциям (задачам), выполняемым СУБД	Возможность интеграции с подсистемой SE-Linux	да	Возможность интеграции с подсистемой SE-Linux

5.1 Требования к безопасности QSS	Стирание из оперативной памяти ключевой информации после окончания её использования путем перезаписи псевдослучайной последовательностью	да	Стирание из оперативной памяти ключевой информации после окончания её использования путем перезаписи псевдослучайной последовательностью
5.1 Требования к безопасности QSS	Защита ключевой информации в оперативной памяти путем ее маскирования	да	Защита ключевой информации в оперативной памяти путем ее маскирования
5.1 Требования к безопасности QSS	Контроль жизненного цикла ключа: запрет техническими средствами на использование ключа для шифрования и формирования цифровой подписи после истечения времени его жизни (не может составлять более 15 месяцев) и заблаговременное уведомление администраторов о необходимости смены ключа	да	Контроль жизненного цикла ключа: запрет техническими средствами на использование ключа для шифрования и формирования цифровой подписи после истечения времени его жизни (не может составлять более 15 месяцев) и заблаговременное уведомление администраторов о необходимости смены ключа
5.2 Специальные требования к безопасности QSS	Самотестирование криптографических функций	да	Реализованы механизмы, обеспечивающие проверку работоспособности (тестирование) криптографических функций при запуске СКЗИ, а также периодически в процессе работы
5.2 Специальные требования к безопасности QSS	Должна осуществляться регистрация входа/выхода субъектов доступа QSS, всех административных действий в СКЗИ и функций управления ключевой информацией.	да	Осуществляется регистрация входа/выхода субъектов доступа QSS, всех административных действий в СКЗИ и функций управления ключевой информацией.
5.2 Специальные требования к безопасности QSS	Должны быть реализованы механизмы (процедуры) контроля несанкционированного случайного искажения и/или разрушения компонентов, содержащих исполняемый код (не криптографическими методами): – контроль целостности до загрузки ОС; – стартовый контроль целостности; – регламентный контроль целостности.	да	Должны быть реализованы механизмы (процедуры) контроля несанкционированного случайного искажения и/или разрушения компонентов, содержащих исполняемый код (не криптографическими методами): – контроль целостности до загрузки ОС; – стартовый контроль целостности; – регламентный контроль целостности.
5.3 Общие требования к безопасности СУБД	Использование SHA2	да	Использование SHA2
5.3 Общие требования к безопасности СУБД	Использование ГОСТ Р 3412-15 / 18 "Кузнечик"	да	при совместном использовании с QSS
5.3 Общие требования к безопасности СУБД	Шифрование на уровне всех или отдельных таблиц	да	при совместном использовании с QSS
5.3 Общие требования к безопасности СУБД	Создание бэкапа зашифрованных данных	да	при совместном использовании с QSS

5.3 Общие требования к безопасности СУБД	Данные на диске и в кэше операционной системы зашифрованы	да	при совместном использовании с QSS
5.3 Общие требования к безопасности СУБД	Ролевой метод управления доступом	да	В СУБД реализован ролевой метод управления доступом
5.3 Общие требования к безопасности СУБД	Дискреционный метод управления доступом	да	<p>В СУБД реализован дискреционный метод управления доступом</p> <p>Дискреционный метод управления доступом субъектов доступа к объектам доступа СУБД (база данных, таблица, запись или столбец, поле, представление, процедура (программный код) или иные объекты доступа) осуществляется на основе настраиваемых списков управления доступом (матриц управления доступом). Списки управления доступом (матрицы управления доступом) позволяют задавать разрешение или запрет пользователям СУБД выполнять следующие операции в отношении процедур (программного кода), хранимых в базе данных:</p> <ul style="list-style-type: none"> <li>-создание;</li> <li>- модификация,</li> <li>-удаление,</li> <li>-исполнение.</li> </ul> <p>Списки управления доступом (матрицы управления доступом) позволяют задавать разрешение или запрет пользователям и процедурам (программному коду), хранимым в базе данных, выполнять следующие операции в отношении объектов доступа СУБД (база данных, таблица, запись или столбец, поле, представление или иные объекты доступа):</p> <ul style="list-style-type: none"> <li>-создание,</li> <li>-модификация,</li> <li>-удаление,</li> <li>-чтение.</li> </ul>



<p>5.3 Общие требования к безопасности СУБД</p>	<p>Первичная идентификация администраторов СУБД и администраторов баз данных (администраторов информационных систем) должна осуществляться администратором СУБД.</p> <p>Первичная идентификация пользователей базы данных должна осуществляться администратором базы данных (администратором информационной системы).</p> <p>СУБД должна осуществлять аутентификацию пользователей системы при предъявлении пароля пользователя:</p> <p>Пароль пользователя для администраторов СУБД и администраторов базы данных (администраторов информационной системы) должен устанавливаться администратором СУБД. Пароль для пользователей базы данных устанавливается администратором базы данных (администратором информационной системы).</p> <p>СУБД должна обеспечивать возможность смены установленных паролей пользователей СУБД после их первичной аутентификации.</p>	<p>да</p>	<p>Первичная идентификация администраторов СУБД и администраторов баз данных (администраторов информационных систем) должна осуществляться администратором СУБД.</p> <p>Первичная идентификация пользователей базы данных должна осуществляться администратором базы данных (администратором информационной системы).</p> <p>СУБД должна осуществлять аутентификацию пользователей системы при предъявлении пароля пользователя:</p> <p>Пароль пользователя для администраторов СУБД и администраторов базы данных (администраторов информационной системы) должен устанавливаться администратором СУБД. Пароль для пользователей базы данных устанавливается администратором базы данных (администратором информационной системы).</p> <p>СУБД должна обеспечивать возможность смены установленных паролей пользователей СУБД после их первичной аутентификации.</p>
<p>5.3 Общие требования к безопасности СУБД</p>	<p>СУБД должна обеспечивать хранение аутентификационной информации пользователя СУБД в защищенном формате или в защищенном хранилище.</p>	<p>да</p>	<p>СУБД обеспечивает хранение аутентификационной информации пользователя СУБД в защищенном формате или в защищенном хранилище.</p>
<p>5.3 Общие требования к безопасности СУБД</p>	<p>Пароль пользователя СУБД должен содержать не менее 8 символов при алфавите пароля не менее 70 символов. Максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки – 4.</p>	<p>да</p>	<p>Пароль пользователя СУБД должен содержать не менее 8 символов при алфавите пароля не менее 70 символов. Максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки – 4.</p>
<p>5.3 Общие требования к безопасности СУБД</p>	<p>Защита пароля пользователя СУБД должна обеспечиваться при его вводе за счет исключения отображения символов вводимого пароля или отображения вводимых символов условными знаками.</p>	<p>да</p>	<p>Защита пароля пользователя СУБД обеспечивается при его вводе за счет исключения отображения символов вводимого пароля или отображения вводимых символов условными знаками.</p>

5.3 Общие требования к безопасности СУБД	При попытке ввода неправильного значения идентификатора или пароля пользователя СУБД должно быть отказано в доступе. При исчерпании установленного максимального количества неуспешных попыток ввода неправильного пароля учетная запись пользователя базы данных (пользователя информационной системы) должна быть заблокирована СУБД с возможностью разблокировки администратором СУБД или администратором базы данных (администратором информационной системы) или с возможностью автоматической разблокировки по истечении временного интервала.	да	При попытке ввода неправильного значения идентификатора или пароля пользователя СУБД должно быть отказано в доступе. При исчерпании установленного максимального количества неуспешных попыток ввода неправильного пароля учетная запись пользователя базы данных (пользователя информационной системы) блокируется СУБД с возможностью разблокировки администратором СУБД или администратором базы данных (администратором информационной системы) или с возможностью автоматической разблокировки по истечении временного интервала.
5.4 Требования к целостности СУБД	Контроль целостности конфигурации системы управления базами данных, конфигураций баз данных, процедур (программного кода) системы управления базами данных, процедур (программного кода), хранимых в базах данных, в процессе запуска системы управления базами данных самостоятельно или с применением сертифицированной операционной системы	да	Контроль целостности конфигурации системы управления базами данных, конфигураций баз данных, процедур (программного кода) системы управления базами данных, процедур (программного кода), хранимых в базах данных, в процессе запуска системы управления базами данных самостоятельно или с применением сертифицированной операционной системы
5.4 Требования к целостности СУБД	Информирование администратора системы управления базами данных о нарушении целостности объектов контроля	да	Информирование администратора системы управления базами данных о нарушении целостности объектов контроля
5.4 Требования к целостности СУБД	Информирование администратора базы данных (администратора информационной системы) о нарушении целостности конфигураций баз данных, процедур (программного кода), хранимых в базах данных	да	Информирование администратора базы данных (администратора информационной системы) о нарушении целостности конфигураций баз данных, процедур (программного кода), хранимых в базах данных
5.4 Требования к целостности СУБД	Блокирование доступа пользователей системы управления базами данных (за исключением администратора системы управления базами данных) к системе управления базами данных и базам данных при выявлении нарушения целостности объектов контроля;	да	Блокирование доступа пользователей системы управления базами данных (за исключением администратора системы управления базами данных) к системе управления базами данных и базам данных при выявлении нарушения целостности объектов контроля;

5.4 Требования к целостности СУБД	Блокирование доступа пользователей базы данных (пользователей информационной системы) к базе данных при выявлении нарушения целостности конфигураций баз данных, процедур (программного кода), хранимых в базах данных.	да	Блокирование доступа пользователей базы данных (пользователей информационной системы) к базе данных при выявлении нарушения целостности конфигураций баз данных, процедур (программного кода), хранимых в базах данных.
5.4 Требования к целостности СУБД	СУБД должна контролировать целостность процедур (программного кода), процедур (программного кода), хранимых в базах данных, в процессе функционирования СУБД не реже одного раза в сутки.	да	СУБД должна контролировать целостность процедур (программного кода), процедур (программного кода), хранимых в базах данных, в процессе функционирования СУБД не реже одного раза в сутки.
5.4 Требования к целостности СУБД	СУБД должна контролировать целостность баз данных в процессе их восстановления из резервной копии.	да	СУБД должна контролировать целостность баз данных в процессе их восстановления из резервной копии.
5.5 Регистрация событий СУБД	Регистрация событий безопасности, связанных с функционированием СУБД;	да	Регистрация событий безопасности, связанных с функционированием СУБД;
5.5 Регистрация событий СУБД	Оповещение администратора СУБД, администратора базы данных (администратора информационной системы) о событиях безопасности;	да	Оповещение администратора СУБД, администратора базы данных (администратора информационной системы) о событиях безопасности;
5.5 Регистрация событий СУБД	Осуществление сбора и хранения записей в журнале событий безопасности, которые позволяют определить, когда и какие события происходили.	да	Осуществление сбора и хранения записей в журнале событий безопасности, которые позволяют определить, когда и какие события происходили.
5.5 Регистрация событий СУБД	Для каждой функции безопасности в СУБД должен быть определен перечень событий, необходимых для регистрации и учета.	да	Для каждой функции безопасности в СУБД определен перечень событий, необходимых для регистрации и учета.
5.5 Регистрация событий СУБД	Для регистрируемых событий безопасности в каждой записи журнала событий безопасности должны регистрироваться номер (уникальный идентификатор) события, дата, время, тип события безопасности.	да	Для регистрируемых событий безопасности в каждой записи журнала событий безопасности регистрируются номер (уникальный идентификатор) события, дата, время, тип события безопасности.
5.5 Регистрация событий СУБД	Записи журнала событий безопасности должны представляться в структурированном виде и содержать дату и время события безопасности, взятые из аппаратной платформы или операционной системы.	да	Записи журнала событий безопасности предоставляются в структурированном виде и содержать дату и время события безопасности, взятые из аппаратной платформы или операционной системы.

5.5 Регистрация событий СУБД	Журнал событий безопасности СУБД должен быть доступен для чтения администратору СУБД и администратору базы данных. Для пользователя базы данных (пользователя информационной системы) журнал событий безопасности должен быть недоступен. При исчерпании области памяти, отведенной под журнал событий безопасности, СУБД должна осуществлять самостоятельно или с применением механизмов сертифицированной операционной системы архивирование журнала с последующей очисткой высвобождаемой области памяти.	да	Журнал событий безопасности СУБД доступен для чтения администратору СУБД и администратору базы данных. Для пользователя базы данных (пользователя информационной системы) журнал событий безопасности недоступен. При исчерпании области памяти, отведенной под журнал событий безопасности, СУБД осуществляет самостоятельно или с применением механизмов сертифицированной операционной системы архивирование журнала с последующей очисткой высвобождаемой области памяти.
5.5 Регистрация событий СУБД	Для регистрируемых событий безопасности в каждой записи журнала событий безопасности дополнительно должны регистрироваться сведения о важности события	да	Для регистрируемых событий безопасности в каждой записи журнала событий безопасности дополнительно регистрируются сведения о важности события
5.6 Резервное копирование и восстановление СУБД	В СУБД должно обеспечиваться резервное копирование и восстановление баз данных и их конфигураций, в том числе атрибутов безопасности, самостоятельно или с применением сертифицированных операционной системы или средства резервного копирования.	да	В СУБД должно обеспечиваться резервное копирование и восстановление баз данных и их конфигураций, в том числе атрибутов безопасности, самостоятельно или с применением сертифицированных операционной системы или средства резервного копирования.
5.6 Резервное копирование и восстановление СУБД	В СУБД должно обеспечиваться резервное копирование конфигурации СУБД самостоятельно или с применением сертифицированных операционной системы или средства резервного копирования.	да	В СУБД должно обеспечиваться резервное копирование конфигурации СУБД самостоятельно или с применением сертифицированных операционной системы или средства резервного копирования.
5.7 Обеспечение доступности в СУБД	СУБД должна функционировать в отказоустойчивом кластере, обеспечивающем ее доступность за счет одновременного функционирования нескольких экземпляров системы управления базами данных;	да	В СУБД реализована возможность функционирования в отказоустойчивом кластере, обеспечивающем ее доступность за счет одновременного функционирования нескольких экземпляров системы управления базами данных;
5.7 Обеспечение доступности в СУБД	СУБД должна обеспечивать возможность синхронизации параметров конфигурации систем управления базами данных в кластере;	да	В СУБД реализована возможность синхронизации параметров конфигурации систем управления базами данных в кластере
5.7 Обеспечение доступности в СУБД	Должна обеспечиваться возможность поочередного обновления, связанного с устранением уязвимостей, каждого компонента в кластере при сохранении доступности СУБД.	да	В СУБД реализована возможность поочередного обновления, связанного с устранением уязвимостей, каждого компонента в кластере при сохранении доступности СУБД.

5.7 Обеспечение доступности в СУБД	При неуспешном обновлении СУБД в кластере должна обеспечиваться возможность возврата к её предыдущему состоянию. Данное действие не должно приводить к прерыванию работы кластера систем управления базами данных.	да	При неуспешном обновлении СУБД в кластере имеется возможность возврата к её предыдущему состоянию. Данное действие не должно приводить к прерыванию работы кластера систем управления базами данных.
5.7 Обеспечение доступности в СУБД	СУБД должна обеспечивать возможность подключения и поддержку связи с удаленными клиентами посредством асинхронного пула соединений, который должен принимать входящие подключения от удаленных клиентов и проксировать их серверу баз данных. Соединения с серверами должны устанавливаться (и завершаться) автоматически, по мере необходимости.	да	В СУБД реализована возможность подключения и поддержку связи с удаленными клиентами посредством асинхронного пула соединений, который должен принимать входящие подключения от удаленных клиентов и проксировать их серверу баз данных. Соединения с серверами должны устанавливаться (и завершаться) автоматически, по мере необходимости.
5.8 Очистка памяти СУБД	СУБД самостоятельно или с применением сертифицированной операционной системы должна обеспечивать удаление баз данных и журналов, используемых СУБД, путем многократной перезаписи уничтожаемых (стираемых) объектов файловой системы специальными битовыми последовательностями.	да	
5.8 Очистка памяти СУБД	СУБД должна удалять объекты доступа базы данных, используемые СУБД, путем перезаписи модифицированных участков объектов файловой системы при выполнении операции удаления или в отложенном режиме через промежуток времени, устанавливаемый администратором СУБД или администратором базы данных.	да	
6.1 Требования к доступности и надежности СУБД	Возможность построения отказоустойчивого кластера (ведущий-ведомый) с произвольным количеством реплик (ведомых серверов) в разных конфигурациях (теплый резерв, горячий резерв);	да	
6.1 Требования к доступности и надежности СУБД	Встроенная очередь сообщений	да	
6.1 Требования к доступности и надежности СУБД	Наличие встроенных средств репликации данных: синхронная, асинхронная, каскадная	да	
6.1 Требования к доступности и надежности СУБД	Наличие встроенных средств «горячего» резервного копирования и восстановления данных	да	
6.1 Требования к доступности и надежности СУБД	Возможность отслеживания изменений страниц БД для инкрементальных копий	да	
6.1 Требования к доступности и надежности СУБД	Возможность полного резервного копирования данных с сохранением журналов транзакций	да	

6.1 Требования к доступности и надежности СУБД	Возможность инкрементального (на уровне страниц) резервного копирования данных с сохранением журналов транзакций;	да	С помощью модуля qbackup
6.1 Требования к доступности и надежности СУБД	Возможность полного восстановления данных	да	На уровне основного функционала СУБД
6.1 Требования к доступности и надежности СУБД	Возможность инкрементального (на уровне страниц) восстановления данных;	да	С помощью модуля qbackup
6.1 Требования к доступности и надежности СУБД	Возможность контроля целостности данных и проверки резервных копий без восстановления данных	да	На уровне основного функционала СУБД
6.1 Требования к доступности и надежности СУБД	Возможность инкрементального кумулятивного (на уровне страниц) резервного копирования данных с сохранением журналов транзакций	да	С помощью модуля qbackup
6.1 Требования к доступности и надежности СУБД	Возможность выполнение операций резервного копирования и восстановления в несколько параллельных потоков	да	С помощью модуля qbackup
6.1 Требования к доступности и надежности СУБД	Возможность хранения копируемых данных в сжатом состоянии для экономии дискового пространства	да	С помощью модуля qbackup
6.1 Требования к доступности и надежности СУБД	Возможность получения списка резервных копий и соответствующей метаинформации в виде простого текста или JSON;	да	С помощью модуля qbackup
7.1 Требования к производительности и масштабируемости	Возможность асинхронного подтверждения транзакций;	да	Возможность асинхронного подтверждения транзакций;
7.1 Требования к производительности и масштабируемости	Возможность параллельного выполнения запросов;	да	Возможность параллельного выполнения запросов;
7.1 Требования к производительности и масштабируемости	Возможность параллельного создания индексов и параллельного доступа к индексам;	да	Возможность параллельного создания индексов и параллельного доступа к индексам;
7.1 Требования к производительности и масштабируемости	Возможность сканирования только индекса (покрывающие индексы);	да	Возможность сканирования только индекса (покрывающие индексы);
7.1 Требования к производительности и масштабируемости	Возможность работы с большим количеством временных объектов в рамках одной сессии;	да	Возможность работы с большим количеством временных объектов в рамках одной сессии;
7.1 Требования к производительности и масштабируемости	Быстрая Загрузка Данных + API для загрузки данных	да	Собственная разработка Quantum Direct Loader (QDL). Ускорение загрузки таблиц до 3.5 раз по сравнению с COPY.

7.1 Требования к производительности и масштабируемости	Внешнее хранение двоичных данных	да	Rbytea. Основной целью расширения является вынос двоичных данных из таблиц базы данных в нетранзакционное хранилище, тем самым разгрузив базу данных (зачастую двоичные данные имеют большой объем, который занимает значительный процент от общего размера базы, усложняя администрирование и обслуживание).
7.1 Требования к производительности и масштабируемости	Дамп и загрузка содержимого менеджера дисковых блоков + минимизация времени "разогрева кэша"	да	Модуль Universal Memory Cache Analyzer, UMCA позволяет сохранять содержимое менеджера кэша дисковых блоков в файловой системе, а затем загружать его обратно, тем самым восстанавливая прежнее состояние. За счет этого время на прогрев экземпляра не затрачивается.
7.1 Требования к производительности и масштабируемости	Расширенный функционал менеджера кэша дисковых блоков, устойчивого к вымыванию кэша	да	TARQ - собственная разработка, самобалансирующийся менеджер кэша дисковых блоков.
7.1 Требования к производительности и масштабируемости	Поддержка секционирования для больших таблиц	да	Поддержка секционирования для больших таблиц
7.1 Требования к производительности и масштабируемости	Возможность размещать данные в общей памяти используя таблицы в оперативной памяти (In-Memory)	да	Возможность размещать данные в общей памяти используя таблицы в оперативной памяти (In-Memory)
7.1 Требования к производительности и масштабируемости	Возможность параллельной выгрузки и загрузки данных	да	Возможность параллельной выгрузки и загрузки данных
7.1 Требования к производительности и масштабируемости	Наличие пула соединений.	да	с помощью модуля QCP
8. Дополнительные требования к СУБД	Возможность осуществлять журналирование выполнения транзакций независимо от результата выполнения родительской транзакции;	да	
8. Дополнительные требования к СУБД	Возможность планировать и контролировать задания, а также управлять их выполнением в базе данных (планировщик задач);	да	
8. Дополнительные требования к СУБД	Возможность изменения структуры таблицы без блокировки;	да	

8. Дополнительные требования к СУБД	Возможность перестроения индексов без блокировки таблицы;	да	
8. Дополнительные требования к СУБД	Возможность использования функций для работы с переменными различных типов в рамках текущей сессии;	да	
8. Дополнительные требования к СУБД	Расширенные возможности управления подключениями: о реализация тайм-аута для простаивающих сеансов на стороне сервера; о периодическая проверка соединения клиента с сервером во время выполнения запросов, что позволяет обнаруживать разрывы соединений раньше и освобождать ресурсы сервера при отключении клиентов.	да	
8. Дополнительные требования к СУБД	Поддержка платформонезависимой сортировки (использование ICU на всех платформах);	да	
8. Дополнительные требования к СУБД	Возможность немедленно обновлять статистику после операций INSERT, UPDATE, DELETE или SELECT INTO в целевых таблицах;	да	
8. Дополнительные требования к СУБД	Наличие встроенного агента мониторинга состояния БД;	да	
8. Дополнительные требования к СУБД	Низкоуровневые метрики	да	Работают с уровня ядра СУБД, вместо выполнения системных запросов к БД.
8. Дополнительные требования к СУБД	Встроенная агрегация / экспорт / визуализация результатов мониторинга	да	Агрегация / экспорт / визуализация на том же или соседнем хосте (без нагрузки на основной сервер)
8. Дополнительные требования к СУБД	Встроенный сервер метрик	да	Собственная разработка - сервер метрик metricsd. Быстрособираемые показатели (сбор практически не влияет на быстродействие / нагрузку сервера).
8. Дополнительные требования к СУБД	Возможность On-demand включения / выключения сбора метрик.	да	Возможность включить и выключить сбор статистики на горячую, без перезагрузки сервера.
8. Дополнительные требования к СУБД	Возможность узнавать текущее состояние выполнения запросов в работающем обслуживающем процессе.	да	