УТВЕРЖДЕНО

643.72410666.00067-05 31 01

ЗАЩИЩЕННАЯ СИСТЕМА УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ «JATOBA»

Описание применения

643.72410666.00067-05 31 01

Листов 28

Подп. и дата	
Инв. №	
Взам. инв.	
Подп. и дата	
Инв. № подл.	

2023

Литера O_1

АННОТАЦИЯ

В документе приведены сведения о защищенной системе управления базами данных «Jatoba» (далее − СУБД «Jatoba»). Настоящий документ содержит описание назначения СУБД «Jatoba», описание функциональных возможностей, условий применения и решаемых СУБД «Jatoba» задач, а также входные и выходные данные СУБД.

СОДЕРЖАНИЕ

1. Назначение программы 4
1.1. Назначение СУБД «Jatoba» 4
1.2. Основные характеристики 4
1.3. Производительность СУБД 8
2. Условия применения 9
3. Описание задачи 14
3.1. Классы решаемых задач 14
3.2. Методы решения задач 15
3.2.1. Задачи управления базами данных, решаемые ядром СУБД 15
3.2.2. Задачи расширения функциональных возможностей ядра СУБД 18
3.2.3. Задачи расширения защиты данных и обеспечения отказоустойчивости 19
4. Входные и выходные данные 26
4.1. Входные данные 26
4.2. Выходные данные 26
Перечень сокращений 27
Лист регистрации изменений 28

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1. Назначение СУБД «Jatoba»

СУБД «Jatoba» предназначена для управления базами данных (далее – БД) в значимых объектах критической информационной инфраструктуры 1 категории, в государственных информационных системах 1 класса защищенности, в автоматизированных системах управления производственными и технологическими процессами 1 класса защищенности, в информационных системах персональных данных при необходимости обеспечения 1 уровня защищенности персональных данных, в информационных системах общего пользования II класса на базе электронно-вычислительных машин (далее – ЭВМ) под управлением операционных систем (далее – ОС) приведенных в таблице 2.1.

1.2. Основные характеристики

СУБД «Jatoba» реализована в архитектуре клиент-сервер. Рабочий сеанс включает следующие взаимодействующие процессы (программы):

- главный серверный процесс, управляющий файлами баз данных, принимающий подключения клиентских приложений и выполняющий различные запросы клиентов к базам данных;
- клиентское приложение пользователя, выполняющее операции в БД;
- CLI-консоль на АРМ управления.

Клиентская и серверная часть СУБД «Jatoba» могут располагаться на разных ЭВМ. Взаимодействие организовано по протоколу TCP/IP. Сервер СУБД «Jatoba» может обслуживать одновременно несколько подключений клиентов.

В состав СУБД «Jatoba» входят компоненты, приведенные в таблице 1.1.

Таблица 1.1 – Состав компонент

№	Наименование	Описание	J4		J5	
			Дист.	Обр.к.	Дист.	Обр.к.
1	ядро СУБД		X	X	X	X
2	jaDog	компонент управления режимом работы узлов кластера	X	—	X	—
3	jaPooler	компонент балансировки подключений пользователей к СУБД	X	—	X	—
4	fasttrun	компонент совместимости с 1С	X	X	X	X
5	fulleq	компонент	X	X	X	X

№	Наименование	Описание	J4		J5	
			Дист.	Обр.к.	Дист.	Обр.к.
		совместимости с 1С				
6	mchar	компонент совместимости с 1С	X	X	X	X
7	online_analyze	компонент совместимости с 1С	X	X	X	X
8	plantuner	компонент совместимости с 1С	X	X	X	X
9	Oracle_FDW (Foreign data wrapper for oracle)	компонент доступа к данным СУБД Oracle	X	—	X	—
10	OraFCE (Oracle function compatibility extension)	компонент совместимости с СУБД Oracle	X	X	X	X
11	pg_Variables	компонент совместимости с системой глобальных переменных СУБД Oracle	X	X	X	X
12	JDV (Jatoba data vault)	компонент контроля субъектов доступа	X	X	X	X
13	pgSQL-HTTP	компонент формирования HTTP/HTTPS запросов из СУБД	X	X	X	X
14	PlsPgSQL	компонент обфускации кода PL/pgSQL	X	—	X	—
15	PostGIS	компонент работы с географическими данными	X	X	X	X
16	JCS (Jatoba crypto access storage)	компонент сокрытия информации в файлах данных СУБД	X	X	X	X
17	SQL_Firewall	компонент выявления и предотвращения исполнения нетипичных SQL-запросов	X	X	X	X
18	pg_Cryogen	компонент компрессии данных СУБД	X	X	X	X
19	pg_Task	компонент планирования заданий СУБД	X	X	X	X

№	Наименование	Описание	J4		J5	
			Дист.	Обр.к.	Дист.	Обр.к.
20	pgAudit	компонент расширенного журналирования событий СУБД	X	X	X	X
21	ja_Log	компонент централизованного сбора записей событий СУБД	X	—	X	—
22	pgBadger	компонент формирования отчетов по журналам СУБД	X	X	X	X
23	SecurityProfile	компонент управления парольными политиками пользователей СУБД	X	X	X	X
24	pg_ProBackup	компонент расширенного резервного копирования	X	—	X	—
25	PTrack	компонент расширенного резервного копирования	X	X	X	X
26	ja_CSum	компонент контроля целостности	X	X	X	X
27	ja_Sync_Ldap	компонент синхронизации учетных записей со службами каталогов	X	X	X	X
28	pg_Profile	компонент формирования отчетов производительности СУБД	X	X	X	X
29	JDS (Jatoba data safe)	компонент пользовательского веб-интерфейса для администраторов	X	—	X	—
30	ja_Plan_Manager	компонент создания планов запросов в базах данных (БД), их оптимизации и экспорта в БД	—	—	X	X
31	ja_Hipe_Cluster	компонент высокопроизводительн	—	—	X	X

№	Наименование	Описание	J4		J5	
			Дист.	Обр.к.	Дист.	Обр.к.
		ого кластера				
32	TDS_FDW	компонент поддержки платформы Microsoft SQL Server	—	—	X	X

СУБД «Jatoba» реализует следующие функциональные возможности:

а) управление данными во внешней памяти;

б) управление данными в оперативной памяти;

в) выполнение запросов (DDL/DML);

г) управление транзакциями;

д) журнализация изменений, резервное копирование и восстановление базы данных после сбоев, репликация.

СУБД «Jatoba» в дополнение к стандартным возможностям управления базами данных, реализует функции:

а) хранение пространственных, географических и геометрических данных, поддержка запросов к ним и управление ими;

б) синтаксическая совместимость с распространенными PL/SQL Oracle;

в) расширенные возможности секционирования больших таблиц;

г) протоколирование, анализ и запрет выполнения команд манипулирования данными (DDL/DML);

д) сбор журналов аудита всех операций и загрузка конфигураций в СУБД;

е) работа в составе отказоустойчивого кластера с механизмом переключения нагрузки на основной узел кластера;

ж) защита от несанкционированного изменения конфигурационных файлов;

з) единый пользовательский интерфейс для управления конфигурациями компонентов СУБД и просмотра их состояния.

и) поддержка предустановленных профилей парольных политик:

- FSTEC_1_class – профиль для ИС первого класса защищенности;
- FSTEC_2_class – профиль для ИС второго класса защищенности;
- CIS – профиль, основанный на рекомендациях Center for Internet Security;
- Corporate_1 – корпоративный профиль первого уровня для учетных записей пользователей;

- Corporate_2 – корпоративный профиль второго уровня, для учетных записей администраторов программных (программно-аппаратных средств);
- Corporate_3 – корпоративный профиль третьего уровня для, технических (сервисных, служебных) учетных записей, используемых в технологических процессах ИС или встроенных производителями программных (программно-аппаратных) средств в такие средства.

1.3. Производительность СУБД

СУБД должна обеспечивать требования по производительности указанные в таблице 1.2.

Таблица 1.2 – Требования к производительности СУБД

№	Параметр производительности	J4		J5	
		Серверная часть, исполнение		Серверная часть, исполнение	
		Дист.	Обр.к.	Дист.	Обр.к.
1	Количество пользовательских сессий, поддерживаемых параллельно	800	750	800	750
2	Количество обрабатываемых стандартных запросов в единицу времени (сек)	3650	3475	3520	3305
		(256 сессий)	(128 сессий)	(256 сессий)	(128 сессий)
3	Количество транзакций в единицу времени (ед/сек)	730	695	704	661
		(256 сессий)	(128 сессий)	(256 сессий)	(128 сессий)
4	Задержка в выполнении стандартного запроса (сек)	мин. 13,5 (1 сессия)	мин. 14,4 (1 сессия)	мин. 13,9 (1 сессия)	мин. 15,9 (1 сессия)
		макс. 5558 (800 сессий)	макс. 5724 (750 сессий)	макс. 5222 (800 сессий)	макс. 7475 (700 сессий)
		348 (256 сессий)	210 (128 сессий)	441 (256 сессий)	191 (128 сессий)
5	Количество экземпляров системы управления базами данных, которые могут совместно работать в режиме балансировки нагрузки	2 – 64	—	2 – 64	—

2. УСЛОВИЯ ПРИМЕНЕНИЯ

Установка СУБД «Jatoba» должна выполняться на ЭВМ защищаемой локальной вычислительной сети, расположенные в контролируемой зоне.

Допускается установка СУБД «Jatoba» на ЭВМ, функционирующие под управлением ОС, указанных в таблице 2.1.

Таблица 2.1 – Поддерживаемые операционные системы

№	Наименование ОС	Серверная часть	Клиентская часть	Docker (ver.)	Сертификат ФСТЭК	
					№ серт.	Дата выдачи
1	Windows 10	X	X	—	—	—
2	Windows 11	X	X	—	—	—
3	Windows Server 2016	X	X	—	—	—
4	Windows Server 2019	X	X	—	—	—
5	Windows Server 2022	X	X	—		
6	Astra Linux 1.6 Special Edition Смоленск (x86-64)	X	X	—	2557	30.01.2012
7	Astra Linux 1.7 Special Edition Смоленск (x86-64)	X	X	20.10.2	2557	30.01.2012
8	Astra Linux 2.12 Common Edition Орел (x86-64)	X	X	—	—	—
9	Debian 10	X	X	24.0.2	—	—
10	Debian 11	X	X	24.0.2	—	—
11	Альт 8 СП	X	X	20.10.11	3866	10.08.2018
12	Альт 9.1 Server	X	X	—		
13	Альт 10 Server	X	X	23.0.1	—	—
14	Ubuntu 18.04	X	X	24.0.2	—	—
15	Ubuntu 20.04	X	X	24.0.2	—	—
16	Ubuntu 22.04	X	X	24.0.2	—	—
17	РЕД ОС 7.2 Муром	X	X	—	—	—
18	РЕД ОС 7.3 Муром	X	X	20.10.1	4060	12.01.2019
19	РОСА 7.3 Кобальт для серверных систем	X	X	—	4039	07.12.2018

20	CentOS 7	X	X	24.0.2	—	—
21	RedHat Enterprise Linux 7.8	X	X	—	—	—
22	RedHat Enterprise Linux 8.2	X	X	—	—	—
23	Oracle Linux 8	X	X	—	—	—

СУБД «Jatoba» устанавливается на ЭВМ с процессорами, имеющими архитектуру x86-64 и AMD64, удовлетворяющие следующим аппаратным требованиям, указанным в таблице 2.2.

Таблица 2.2 – Аппаратные требования к средствам вычислительной техники, на которых функционируют клиентская и серверная части СУБД

Параметр	Характеристика
Требования к аппаратному обеспечению сервера СУБД	
ОЗУ	Не менее 2 Гб
Свободный объем жесткого диска	Минимальный объем от 40 Гб Рекомендуемый объем от 100 Гб
Устройства видео вывода	Монитор и видеоадаптер с поддержкой VGA и разрешением 800x600 или выше
Тип процессора и минимальная тактовая частота процессора	64-разрядный процессор Intel или AMD 3 ГГц или больше
Минимальное количество ядер	4
Максимальное количество ядер	256
Устройства ввода-вывода	Стандартные 105-клавишная клавиатура и манипулятор «мышь» с USB, либо PS/2-интерфейсами
Адаптер Ethernet	100 Мбит/с
Требования к аппаратному обеспечению АРМ управления	
ОЗУ	Не менее 4 Гб
Свободный объем жесткого диска	От 3 Гб
Устройства видео вывода	Монитор и видеоадаптер с поддержкой VGA и разрешением 800x600 или выше
Тип процессора и минимальная тактовая частота процессора	64-разрядный процессор Intel или AMD Рекомендуемая частота: 2.4 ГГц или больше
Устройства ввода-вывода	Стандартные 105-клавишная клавиатура и манипулятор «мышь» с USB-интерфейсами, либо PS/2 интерфейсами
Адаптер Ethernet	100 Мбит/с
Требования к программному обеспечению сервера	
Операционная система	Требования приведены в таблице 2.1
Требования к программному обеспечению АРМ управления	
Операционная система	Требования приведены в таблице 2.1
Требования к аппаратному обеспечению сервера Jatoba data safe	

Параметр	Характеристика
ОЗУ	Не менее 2 Гб
Свободный объем жесткого диска	Минимальный объем от 40 Гб Рекомендуемый объем от 100 Гб
Устройства видео вывода	Монитор и видеоадаптер с поддержкой VGA и разрешением 800x600 или выше
Тип процессора и минимальная тактовая частота процессора	64-разрядный процессор Intel или AMD 3 ГГц или больше
Минимальное количество ядер	4
Устройства ввода-вывода	Стандартные 105-клавишная клавиатура и манипулятор «мышь» с USB-интерфейсами, либо PS/2 интерфейсами
Адаптер Ethernet	100 Мбит/с
Требования к программному обеспечению сервера Jatoba data safe	
Поддерживаемые платформы	• linux-x64 • linux-arm
СУБД	Защищенная система управления базами данных «Jatoba»
Веб-сервер	nginx
Internet браузер	• Google Chrome; • Яндекс.Браузер; • Chromium; • Opera; • Mozilla Firefox

СУБД «Jatoba» может использоваться для обеспечения базовых и адаптированных мер защиты информации:

а) при создании защищенных автоматизированных систем, не обрабатывающих сведения составляющие государственную тайну, до класса защищенности 1Г включительно (руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (Гостехкомиссия России, 1992);

б) для обеспечения 1 уровня защищенности персональных данных (п. 12 Приказа ФСТЭК России № 21 от 18 февраля 2013 г. (ред. от 14.05.2020) «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»);

в) в государственных информационных системах 1 класса защищенности (п. 26 Приказа ФСТЭК России № 17 от 11 февраля 2013 г. (ред. от 28.05.2019) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»);

г) при создании защищенных информационных систем управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды до 1 класса защищенности включительно (п. 26 Приказа ФСТЭК России № 31 от 14 марта 2014 г. (ред. от 15.03.2021) «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»);

д) при создании информационных систем 1 категории значимости (п. 27 Приказа ФСТЭК России № 239 от 25.12.2017 (ред. от 20.02.2020) «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»);

е) в информационных системах общего пользования II класса в соответствии с приказом ФСБ России и ФСТЭК России от 31.08.2010 г. №416/489,

и обеспечивать базовые и адаптированные меры защиты информации, приведенные ниже.

В таблице 2.3 приведены выполняемые меры защиты информации в соответствии с Приказами ФСТЭК России № 17 от 11.02.2013 (ред. от 28.05.2019), № 21 от 18.02.2013 (ред. от 14.05.2020), № 31 от 14.03.2014 (ред. от 15.03.2021) и № 239 от 25.12.2017 (ред. от 20.02.2020).

Таблица 2.3 – Реализуемые меры защиты информации

Наименование	**J4**		**J5**		**Приказы ФСТЭК**		
					ГИС	**ИСПДн**	**КИИ и КВО**
	Дист.	**Обр.к.**	**Дист.**	**Обр.к.**	**№17**	**№21**	**№239, №31**
Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)	X	X	X	X	ИАФ.1	ИАФ.1	ИАФ.1
	X	X	X	X	ИАФ.4 ИАФ.4(1г)	ИАФ.4	ИАФ.4
	X	X	X	X	ИАФ.5	ИАФ.5	—
Управление доступом субъектов доступа к объектам доступа (УПД)	X	X	X	X	УПД.1	УПД.1	УПД.1
	X	X	X	X	УПД.1(1)	—	—
	X	X	X	X	УПД.1(2)	—	—
	—	—	X	—	УПД.1 (5)	—	—
	X	X	X	X	УПД.2	УПД.2	УПД.2
	X	X	X	X	УПД.2(1)	—	—
	X	—	X	—	УПД.4	УПД.4	УПД.4
	X	X	X	X	УПД.5	УПД.5	УПД.5

Наименование	J4		J5		Приказы ФСТЭК		
					ГИС	ИСПДн	КИИ и КВО
	Дист.	Обр.к.	Дист.	Обр.к.	№17	№21	№239, №31
	X	X	X	X	УПД.6 УПД.6(1)	—	—
	X	X	X	X	УПД.9	УПД.9	УПД.9
	X	X	X	X	УПД.9(3)	—	—
	—	—	X	—	УПД.9(4)	—	—
Регистрация событий безопасности (РСБ)	X	X	X	X	РСБ.2(1а)	—	—
	X	X	X	X	РСБ.3	РСБ.3	АУД.4
	X	—	X	—	РСБ.3(1)	—	—
	X	X	X	X	РСБ.6	РСБ.6	АУД.3
	X	X	X	X	РСБ.7	РСБ.7	АУД.6
	X	X	X	X	РСБ.8	—	АУД.9
					РСБ.8(1)	—	—
Обеспечение целостности информационной системы и информации ОЦЛ)	X	X	X	X	ОЦЛ.1	ОЦЛ.1	ОЦЛ.1
	X	X	X	X	ОЦЛ.2	ОЦЛ.2	ОЦЛ.2
	X	X	X	X	ОЦЛ.7	ОЦЛ.7	ОЦЛ.4
Обеспечение доступности информации (ОДТ)	X	—	X	—	ОДТ.4	ОДТ.4	ОДТ.4
	X	—	X	—	ОДТ.5	ОДТ.5	ОДТ.5
	X	—	X	—	ОДТ.6 (2)	—	ОДТ.7

СУБД «Jatoba» выполняет требования по безопасности информации, установленные приказом ФСТЭК России от 14.04.2023 № 64 «Требования по безопасности информации к системам управления базами данных».

3. ОПИСАНИЕ ЗАДАЧИ

Основная задача, решаемая СУБД «Jatoba» в процессе своего функционирования – управление реляционными базами данных, обеспечивающими многопользовательский доступ к данным при необходимых уровнях отказоустойчивости и защищенности в соответствии с нормативными документами, указанными в «Условиях применения» данного документа.

3.1. Классы решаемых задач

Для решения основной задачи функционирования СУБД «Jatoba» задача создания и управления реляционными базами данных разбивается на следующие классы задач:

а) задачи управления базами данных, решаемые ядром СУБД:

- управление данными во внешней памяти;
- управление данными в оперативной памяти;
- выполнение запросов;
- управление транзакциями;
- журнализация изменений, резервное копирование и восстановление базы данных после сбоев, репликация;
- поддержка языков определения и манипулирования данными;

б) задачи расширения функциональных возможностей ядра СУБД:

- хранение пространственных, географических и геометрических данных, поддержка запросов к ним и управление ими;
- совместимость с функциями процедурных языков СУБД «Oracle»;
- расширение возможностей секционирования больших таблиц;

в) задачи защиты данных и обеспечения отказоустойчивости:

- протоколирование, анализ и запрет выполнения команд манипулирования данными (DDL/DML);
- ролевое разграничение доступа
- дискреционное разграничение доступа;
- идентификация и аутентификация;
- очистка памяти;
- регистрация событий;
- контроль целостности;
- управление подключениями к системе управления базами данных;
- обеспечение отказоустойчивости СУБД «Jatoba»;

- управление конфигурациями компонентов СУБД «Jatoba» и просмотр их состояния с использованием единого пользовательского интерфейса;
- передача значимых событий в системы информационно-технологического мониторинга и системы учета событий информационной безопасности.

3.2. Методы решения задач

3.2.1. Задачи управления базами данных, решаемые ядром СУБД

3.2.1.1. Управление данными во внешней памяти

В СУБД «Jatoba» на уровне ядра реализован программный интерфейс управления данными во внешней памяти. Через данный интерфейс другим компонентам и подсистемам СУБД предоставляется набор функций поблочного чтения и записи из файлов данных, составляющих конкретную базу данных. Внутренние функции интерфейса реализуют управление структурой и расположением файлов баз данных, находящихся под управлением ядра СУБД.

3.2.1.2. Управление данными в оперативной памяти

В СУБД «Jatoba» управление данными в оперативной памяти организуется с помощью встроенных менеджеров памяти нескольких видов. Внутренняя структура памяти представляет собой массивы и хеш-таблицы связанных сегментов, блоков и страниц для высокопроизводительного выполнения процедур обработки данных.

3.2.1.3. Выполнение запросов

В СУБД «Jatoba» реализован конвейер из нескольких исполнительных блоков, отвечающий за выполнение запросов пользователей. Каждый запрос проходит блок разбора и анализа синтаксической корректности SQL-запроса, блок построения дерева планов выполнения запросов, блок оптимизации и нахождения оптимального плана выполнения запроса в дереве и блок непосредственного выполнения выбранного плана, приводящий к результату запроса (внесение, получение или изменение данных).

В СУБД «Jatoba» реализован механизм для создания, оптимизации, экспорта/импорта и подмены планов запросов в БД.

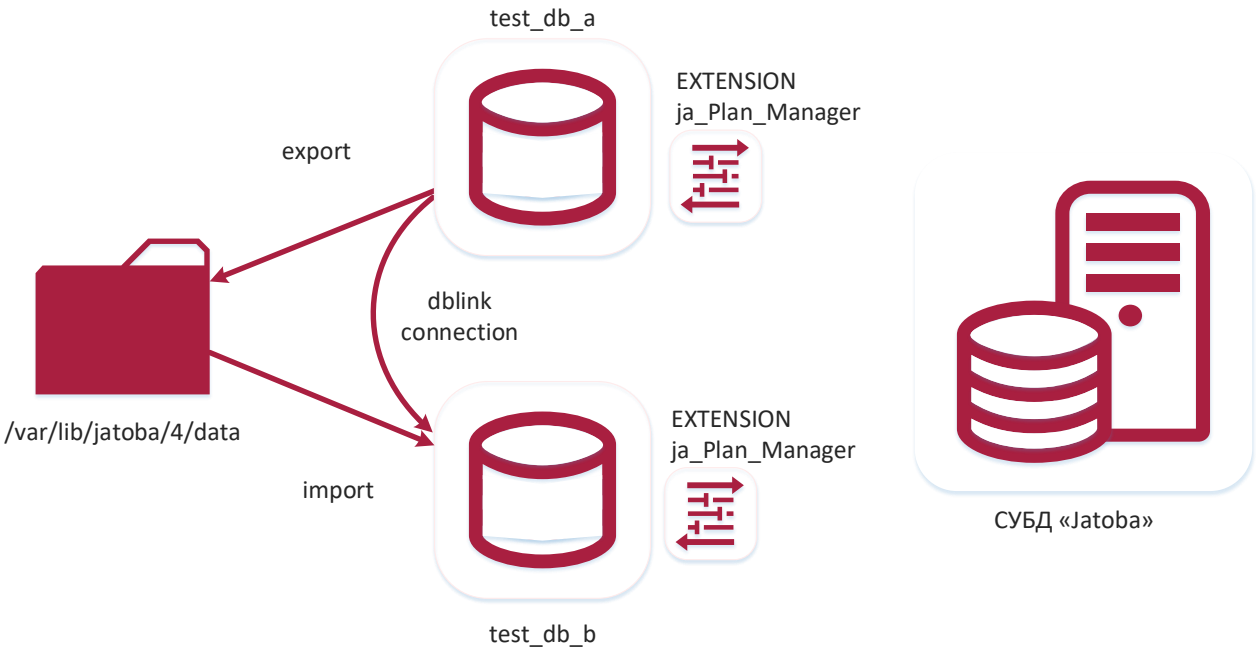

Рисунок 3.1 – Схема работы экспорт/импорта планов запросов

Помимо базовых механизмов СУБД для балансировки и оптимизации запросов пользователей к СУБД используется компонент «jaPooler»

Компонент имеет функциональную возможность оптимизировать запросы от пользователя (ей) к серверу при их подключении к серверу СУБД на указанный порт, как представлено на рисунке 3.2.

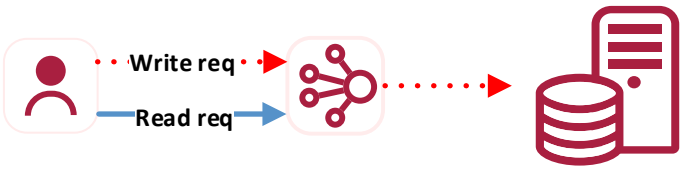

Рисунок 3.2 – Балансировка запросов пользователя

Также компонент обладает функциональной возможностью балансировки подключений множества пользователей к серверам СУБД, как представлено на рисунке 3.3.

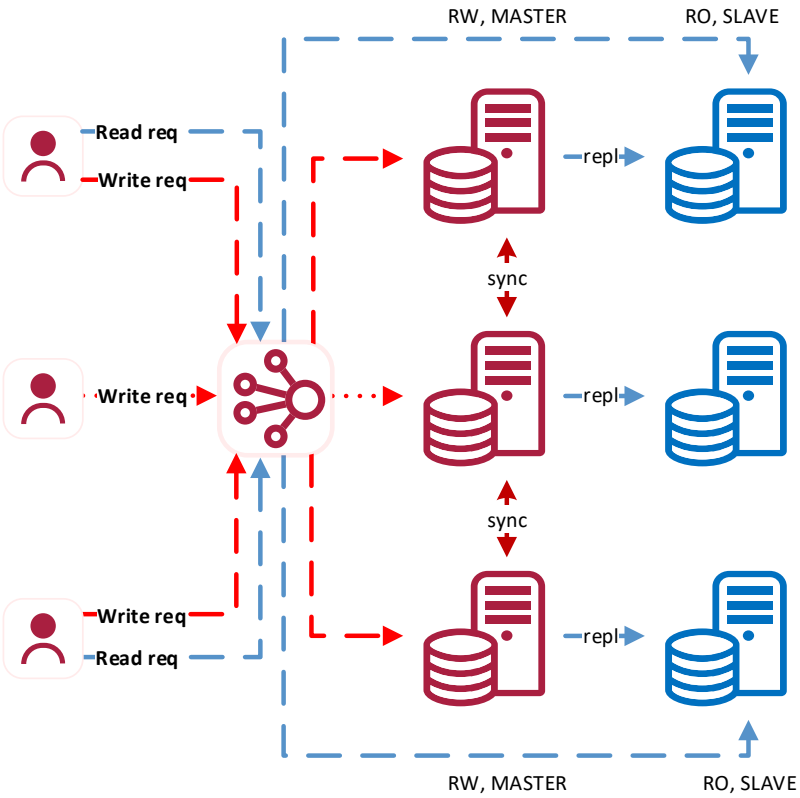

Рисунок 3.3 – Балансировка запросов пользователей к серверам СУБД

Подключения формируются, как от пользователей, так и от пользовательских приложений.

Для выявления и предотвращение исполнения нетипичных SQL-запросов используется компонент «SQL_Firewall». Компонент предназначен для защиты базы данных от SQL-инъекций или неожиданных запросов.

Компонент SQL_Firewall функционирует в режимах:

- "learning" – режим обучения;
- "enforcing" – режим применения;
- "permissive" – режим разрешающий любые SQL запросы;
- "disabled" – режим отключенного модуля.

3.2.1.4. Управление транзакциями

В СУБД «Jatoba» реализован на уровне ядра механизм управлениями транзакциями. Данный механизм тесно связан с механизмом многоверсионности данных, что позволяет реализовать безблокировочный механизм одновременного изменения данных множеством параллельных транзакций. В результате каждая транзакция пользователя либо успешно завершается и данные надежно фиксируются во внешней памяти, либо отвергается с отбрасыванием сделанных изменений.

3.2.1.5. Журнализация изменений, резервное копирование и восстановление базы данных после сбоев, репликация

В СУБД «Jatoba» реализован ряд механизмов, значительно повышающих надежность ее работы в условиях возникновения аварийной ситуации (физический выход из строя оборудования сервера). Список механизмов включает: журнал транзакций (журнал опережающей записи), который в момент исполнения транзакции фиксирует все сделанные ею изменения в отдельное хранилище внешней памяти; процедуры резервного копирования и восстановления, в том числе с использованием журнала транзакций, чтобы восстановить работу с момента последней зафиксированной транзакции до сбоя; процедуры репликации данных для передачи всех зафиксированных транзакций на резервные сервера с возможностью включения в оперативную работу резервного сервера в случае выхода главного сервера из строя.

3.2.1.6. Поддержка языков определения и манипулирования данными

В СУБД «Jatoba» реализована полная поддержка современных стандартов языка SQL, включая выражения определения (CREATE/DROP/ALTER) необходимых объектов баз данных для хранения и управления данными пользователей и выражения манипулирования данными (SELECT/INSERT/UPDATE/DELETE), отвечающими за преобразования данных пользователя.

3.2.2. Задачи расширения функциональных возможностей ядра СУБД

3.2.2.1. Хранение пространственных, географических и геометрических данных, поддержка запросов к ним и управление ими

В СУБД «Jatoba» реализован набор расширений, обеспечивающий управление пространственными данными для построения на базу СУБД геоинформационных систем. Набор расширений включает дополнительные типы данных и процедуры обработки данных этих типов.

3.2.2.2. Совместимость с функциями процедурных языков СУБД «Oracle»

В СУБД «Jatoba» реализован набор расширений, обеспечивающий интеграцию СУБД «Jatoba» с СУБД «Oracle». Расширения предоставляют дополнительные функции, повышающие синтаксическую совместимость и упрощающие перенос хранимых процедур, и предоставляют дополнительные методы прозрачного доступа к данными из одной СУБД в другую.

3.2.2.3. Расширение возможностей секционирования больших таблиц

В СУБД «Jatoba» реализована функциональная возможность, позволяющая обычным серверам баз данных (называемым узлами) координировать свои действия друг с другом в архитектуре «ничего общего» («shared nothing»). Узлы образуют кластер, который позволяет СУБД хранить больше данных и использовать больше ядер центрального процессора, чем это было бы возможно на одном компьютере. Эта

архитектура также позволяет масштабировать базу данных, просто добавляя дополнительные узлы в кластер. Данное расширение позволяет выполнять распределение таблиц и запросов по рабочим узлам, входящим в кластер.

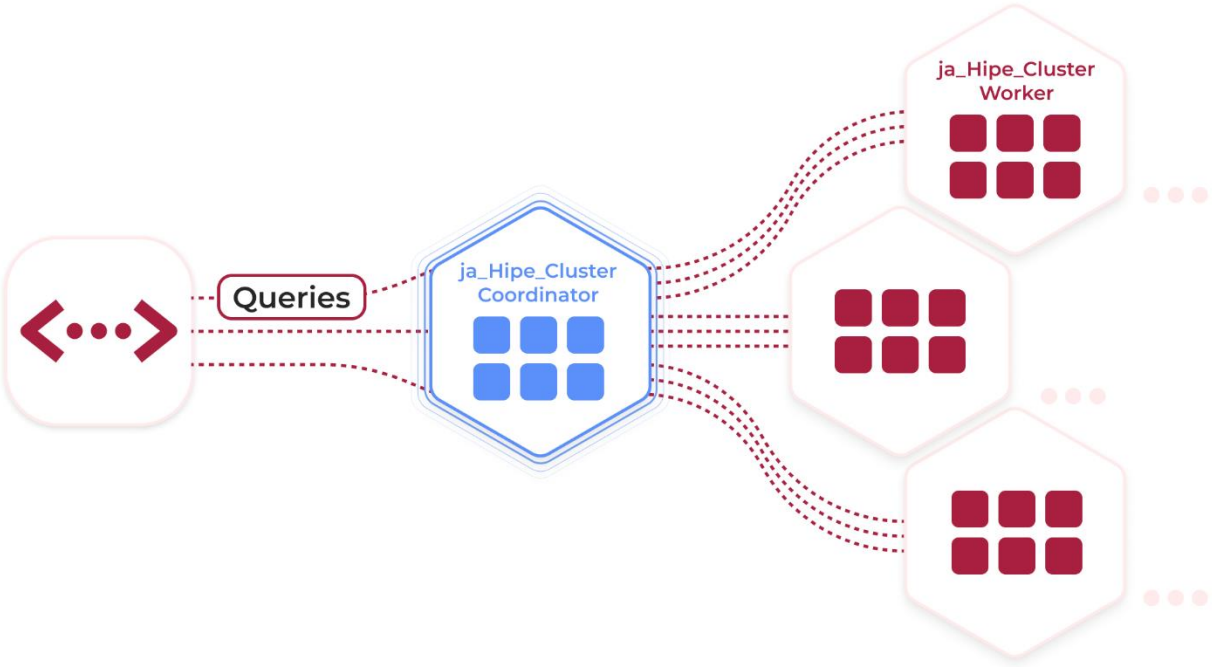

Рисунок 3.4 – Отправка запросов на рабочие узлы

3.2.3. Задачи расширения защиты данных и обеспечения отказоустойчивости

3.2.3.1. Протоколирование, анализ и запрет выполнения команд манипулирования данными (DDL/DML)

В СУБД «Jatoba» реализован механизм детального протоколирования запросов пользователей. Реализация данного механизма использует возможности блоков управления запросов для формирования детальной информации о статусе выполнения запроса. Статусная информация включает описание об объекте и субъекте доступа.

3.2.3.2. Ролевое разграничение доступа

В СУБД «Jatoba» реализован механизм ролевого разграничения доступа. Механизм контроля доступа при обращении к объекту доступа в процессе выполнения запроса проверяет необходимые привилегии. В случае отсутствия достаточных привилегий доступ к объекту запрещается, выполнение запроса пользователя прекращается по ошибке.

Дополнительно в пользовательском веб-интерфейсе для администраторов компонента «Jatoba data safe» реализована двухкомпонентная ролевая модель.

Первым компонентом выступает предопределенная ролевая модель JDS, в которую включена доступность разделов.

Вторым компонентом ролевой модели является набор групповых ролей в целевой СУБД, которым предоставлены необходимые права и привилегии при инициализации компонент и расширений СУБД.

Механизм разграничения доступа реализован таким образом при котором пользователю JDS присваивается предустановленная роль в компоненте, определяющая доступность разделов и в соответствии с данной ролью, пользователь ассоциируется с учетной записью в целевой СУБД.

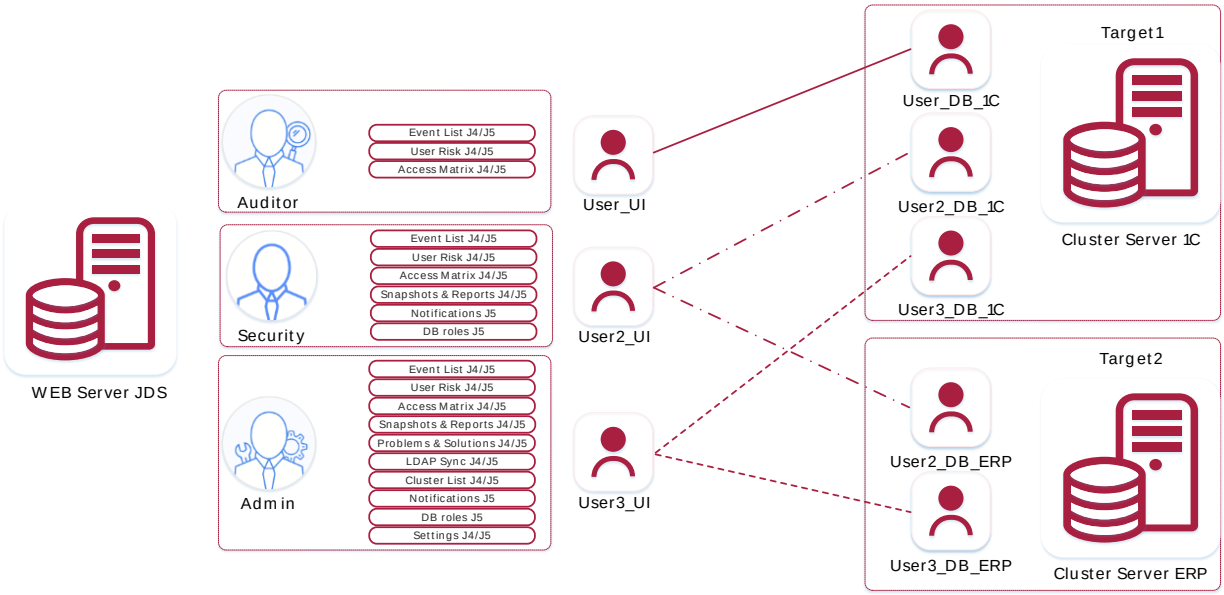

Рисунок 3.5 – Двухкомпонентная ролевая модель

3.2.3.3. Дискреционное разграничение доступа

В СУБД «Jatoba» реализован дискреционный механизм разграничения доступа. Механизм контроля доступа при обращении к объекту доступа в процессе выполнения запроса проверяет необходимые привилегии на вложенные объекты уровня БД. В случае отсутствия достаточных привилегий доступ к объекту запрещается, выполнение запроса пользователя прекращается по ошибке.

3.2.3.4. Идентификация и аутентификация

В СУБД «Jatoba» каждое подключение пользователя предварительно проходит процедуру аутентификации. Аутентификация включает проверку данных сетевого подключения, имени базы данных, имени пользователя и согласования метода аутентификации. Если запрошенные данные подтверждаются, то проводится процедура установления идентичности пользователя в соответствии с заданным методом аутентификации. Основным методом аутентификации пользователей является метод «Password».

Поддерживается функциональная возможность применения методов аутентификации:

- GSSAPI;
- LDAP(LDAPS);
- PAM;
- RADIUS;
- SSL;
- SSPI.

3.2.3.5. Очистка памяти

В СУБД «Jatoba» поддерживаются внутренние процедуры очистки блоков памяти, в которых располагаются данные пользователя в процессе его работы с некоторой базой данных. В случае фиксации этих данных ядром СУБД и отсутствия текущего использования этих данных другими запросами пользователей, данные принудительно удаляются во избежание утечек конфиденциальной информации. При завершении сессии пользователя вся память, где хранились данные пользователя, также принудительно отчищается.

3.2.3.6. Регистрация событий

В ядро СУБД «Jatoba» встроен механизм регистрации различных событий, связанных как с работой самого ядра СУБД, так и с выполнение запросов пользователей на доступ и изменение данных. Реализовано несколько уровней детализации событий, которые администратор может выбрать и настроить на основании имеющихся требований, предъявляемых к СУБД.

Помимо встроенного механизма СУБД, применение компонента «Jatoba data safe» пользовательского веб-интерфейс для администраторов и в совокупности с компонентом централизованного сбора записей событий в СУБД «ja_Log» позволяют обеспечить централизованный сбор, хранение, обработку и просмотр событий безопасности с СУБД.

3.2.3.7. Контроль целостности

СУБД «Jatoba» на уровне ядра поддерживает несколько механизмов обеспечения целостности данных.

Первый встроенный механизм СУБД позволяет проводить проверки корректности данных, которые пользователь вносит в базу данных. Реализована программная возможность включения этих проверок для отдельных полей таблиц по выбору пользователя. Также реализована система ограничений, накладываемая на данные, помещаемые в таблицы. Данные ограничения позволяют обеспечивать ссылочную целостность данных в разных таблицах.

Вторым механизмом контроля целостности является компонент «ja_CSum» предназначенный для выполнения периодических фоновых проверок фалов, расположенных в ключевых директориях СУБД, а также:

- конфигурации системы управления базами данных;
- конфигураций баз данных;
- процедур (программного кода) системы управления базами данных;
- процедур (программного кода), хранимых в базах данных.

3.2.3.8. Механизм управления подключениями к системе управления базами данных

Защита подключений реализуется сторонними по отношению к ядру СУБД средствами, что подтверждается соответствующими описанными требованиями к среде функционирования.

3.2.3.9. Обеспечение отказоустойчивости СУБД «Jatoba»

Отказоустойчивость в СУБД «Jatoba» реализуется средствами репликации данных. Экземпляр СУБД может выступать в роли ведущего или ведомого сервера. Роль сервера определяется соответствующими конфигурационными параметрами, заданными администратором СУБД. Ведомый сервер всегда зависит от ведущего и получает от него все изменения данных, которые накапливаются в журнале транзакций. В случае выхода из строя ведущего сервера, ведомый сервер может автоматически или по команде администратора принять на себя роль ведущего. После восстановления функционирования сервера ему снова может быть возвращена роль ведущего.

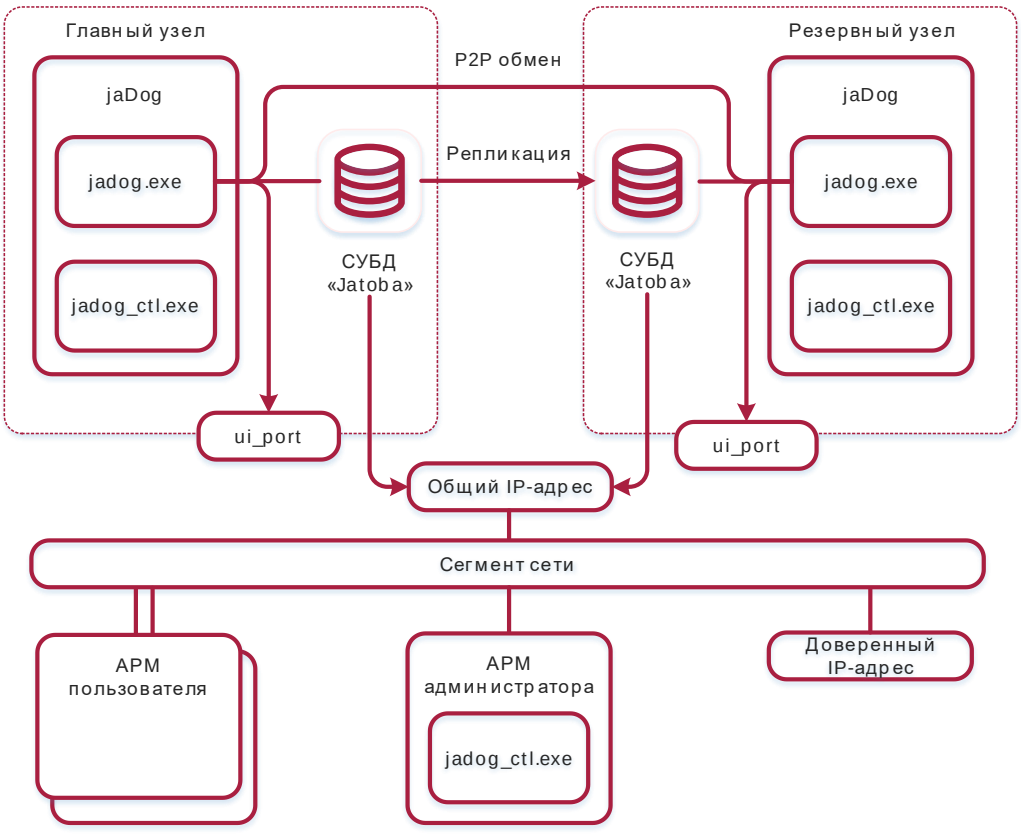

Рисунок 3.6 – Физическая структура узлов кластера

Базовые функциональные возможности кластера расширены до полнофункционального инженерного решения катастрофоустойчивого и георасределенного кластера.

Дополнительно отказоустойчивость СУБД «Jatoba» реализуется применением полного или инкрементального резервного копирования.

Полные резервные копии содержат все файлы данных, необходимые для восстановления сервера баз данных с нулевой точки;

Инкрементальные копии создаются на уровне страниц данных и включают только ту информацию, которая изменилась со времени последнего резервного копирования.

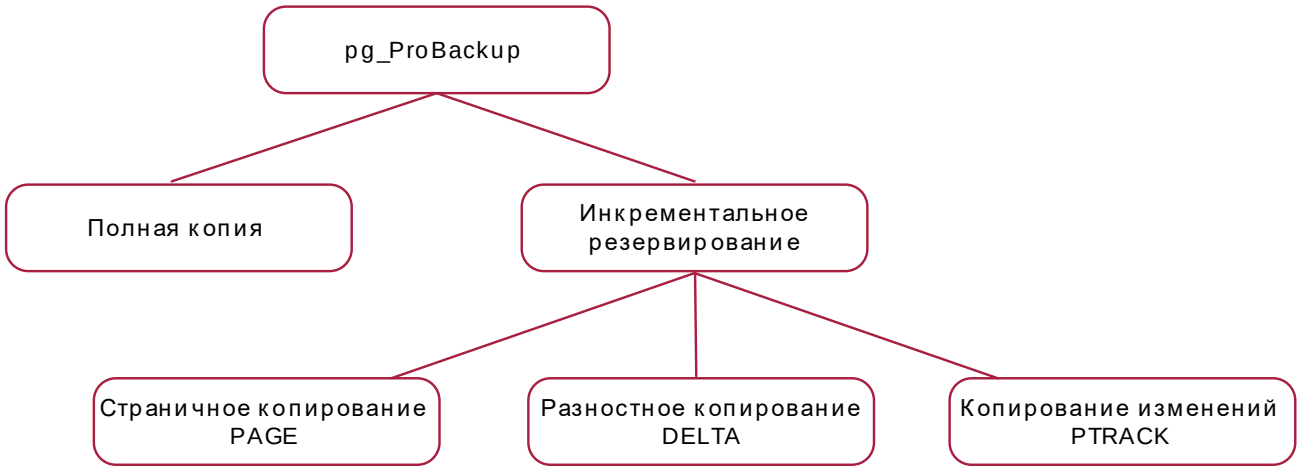

Рисунок 3.7 – Реализуемые способы резервного копирования

3.2.3.10. Ограничение программной среды

СУБД на уровне ядра и используя компонент «ja_CSum» выявляет и блокирует загрузку в адресное пространство СУБД:

- ПО не включенного в перечень разрешенного;
- ПО целостность которого нарушена.

3.2.3.11. Управление компонентами СУБД «Jatoba» и просмотр их состояния с использованием единого пользовательского интерфейса

Для обслуживания и управления СУБД «Jatoba» используется единый пользовательский интерфейс в виде командной строки (CLI).

Дополнительно реализован пользовательский веб-интерфейс для администраторов в компоненте «Jatoba data safe», содержащий следующие разделы:

- Разделы «Анализ рисков» (UserRisk) и «Матрица доступа» (Access matrix) используются для контроля имеющихся привилегий в СУБД и привилегий на вложенные объекты уровня БД.

– Раздел «Список кластеров» (Cluster list) позволяет управлять преднастроенным кластером серверов СУБД. Раздел представляет собой графическое отображение управления компонентом «Jadog».

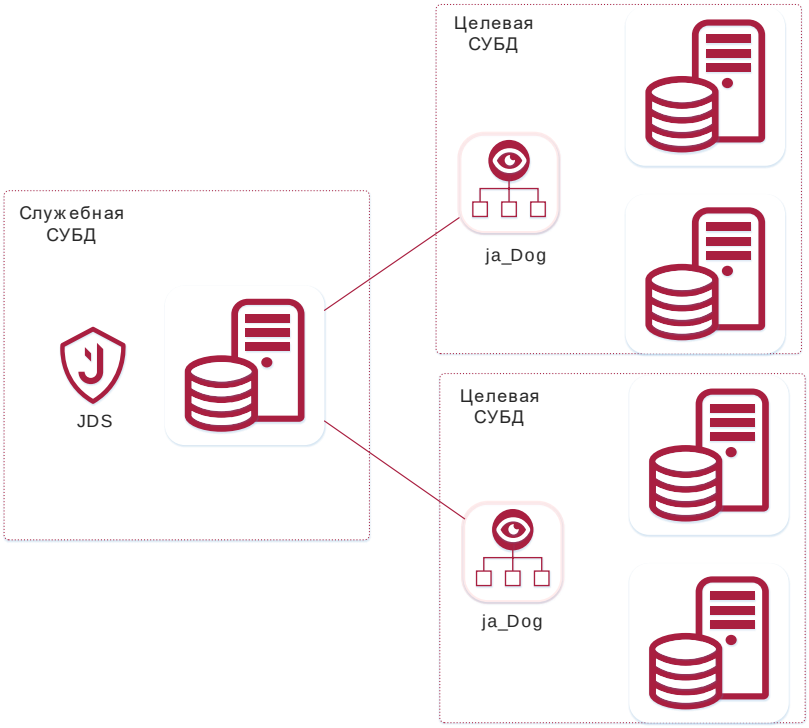

Рисунок 3.8 – Схема работы компонента при клиент-серверном варианте

– Раздел «Список событий» (Event List) предназначен для просмотра событий безопасности в выбранной инсталляции (Target).

Для функционирования раздела требуется, чтобы на целевой СУБД был установлен компонент «ja_Log», обеспечивающий передачу событий безопасности в служебную СУБД. Компонент «pgAudit» при этом обеспечивает расширенную регистрацию событий безопасности.

– Подраздел «Снимки и отчеты» (Snapshots & Reports) предназначен для создания снимков состояния БД (Snapshots) и получения отчетов. Формирование статической информации выполняется компонентом «pg_Profile».

– Подраздел «Проблемы и решения» (Problems & Solutions) представляет собой интеллектуальный инструмент, который позволяет определять ряд проблем, существующих в целевой СУБД.

– Раздел «LDAP синхронизация» (LDAP Sync) предназначен для графического отображения операций по синхронизации учетных записей со службой каталогов и учетных записей целевой СУБД. Для выполнения синхронизации требуется, чтобы расширение было установлено на целевой СУБД.

– Раздел «Уведомления» предназначен для оповещения администраторов о событиях целевой СУБД и компонента «JDS» по классам событий, кодам событий, ключевым фразам и словам.

– Раздел «Роли БД» предназначен для:

- создания ролей;
- редактирования ролей;
- назначения атрибутов и привилегий ролей.

Сопоставление разделов JDS и, обеспечивающих их функционирование, компонентов целевой СУБД представлено на рисунке 3.9.

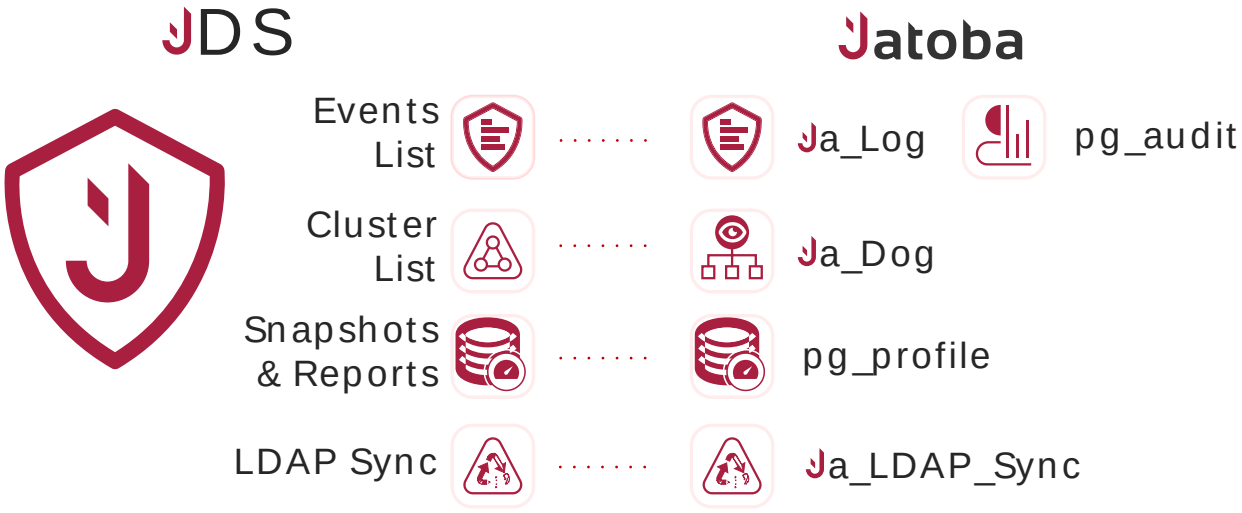

Рисунок 3.9 – Разделы JDS и компоненты СУБД, требуемые для работы разделов JDS

3.2.3.12. Передача событий безопасности в системы информационно-технологического мониторинга и системы учета событий информационной безопасности

В СУБД «Jatoba» через систему регистрации событий административными мерами реализуется передача событий в сторонние системы информационно-технологического мониторинга и учета событий безопасности. Данная функция включается соответствующими конфигурационными параметрами администратором СУБД на основании соответствующих требований безопасности.

4. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

4.1. Входные данные

Входными данными являются:

а) загружаемые табличные стройки;

б) атрибуты ролей, определяющие их полномочия и взаимодействие с системой аутентификации клиентов;

в) привилегии ролей, определяющие ролевые правила разграничения доступа к объектам баз данных;

г) настройка обращений ролей пользователей к защищенным данным;

д) политики защиты строк, определяющие правила доступа к строкам таблиц.

4.2. Выходные данные

Выходными данными является результат использования субъектом доступа защищаемых объектов, предоставленных ему в соответствии с установленными правилами разграничение доступа.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

DDL	–	Data Definition Language, язык описания данных
DML	–	Data Manipulation Language, язык манипулирования данными
SQL	–	Structured Query Language, язык структурированных запросов
БД	–	База данных
ГИС	–	Государственные информационные системы
Дист.	–	Дистрибутив
ИСПДн	–	Информационная система персональных данных
КВО	–	Критически важный объект
КИИ	–	Критическая информационная инфраструктура
Обр.к	–	Образ контейнера
ОС	–	Операционная система
СУБД	–	Система управления базами данных
ФСТЭК России	–	Федеральная служба по техническому и экспортному контролю России
ЭВМ	–	Электронно-вычислительная машина

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Изм	Номера листов (страниц)				Всего листов (страниц) в докум.	№ докум.	Входящий № сопроводитель ного докум. и дата	Подпись	Дата
	изменен ных	заменен ных	новых	аннули рован ных					

№ изменения:____________	Подпись отв. лица:___________	Дата внесения изм.:__________