

УТВЕРЖДЕН
643.72410666.00067-05 95 01-ЛУ

**ЗАЩИЩЕННАЯ СИСТЕМА УПРАВЛЕНИЯ
БАЗАМИ ДАННЫХ «ЈАТОВА»**

Руководство администратора

643.72410666.00067-05 95 01

Листов 139

| | | | | |
|--------------|--------------|--------------|--------------|--------------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | Инв. № дубл. | Подп. и дата |
| | | | | |

2023

Литера О₁

АННОТАЦИЯ

Документ представляет собой руководство администратора системы управления базами данных «Jatoba» (далее по тексту – СУБД, СУБД «Jatoba»).

Руководство администратора содержит следующие разделы:

- Раздел 1, в котором приведены назначение и функции СУБД «Jatoba» и требования к среде функционирования СУБД.
- Раздел 2, в котором приведен состав СУБД «Jatoba».
- Раздел 3, в котором подготовка к установке СУБД «Jatoba».
- Раздел 4, в котором описана настройка параметров СУБД «Jatoba».
- Раздел 5, в котором описаны основные операции в СУБД «Jatoba».
- Раздел 6, в котором приведены настройки безопасности СУБД «Jatoba».
- Раздел 7, в котором приведена инструкция по резервному копированию и восстановлению баз данных.
- Раздел 8, в котором приведена инструкция по созданию отказоустойчивого кластера СУБД «Jatoba».
- Раздел 9, в котором приведены сообщения об ошибках.
- Раздел 10, в котором приведена информация о действиях после сбоев и возникших ошибках при эксплуатации СУБД «Jatoba».
- Приложение 1, в котором приведены значения полей из файла pg_hba.conf.
- Приложение 2, которое содержит перечень событий СУБД с распределением по категориям безопасности.



Все примеры в данном документе приведены для СУБД «Jatoba» версии ядра 4.x, для других версий все шаги выполняются аналогично, разница состоит в именах директорий.

Например, СУБД «Jatoba» версии 5.x по умолчанию устанавливается в директорию:

- ОС Windows – «C:\Program Files\GIS\Jatoba\5\bin»;
- ОС Linux – «/usr/jatoba-5/bin».



Важная информация

Для сертифицированной версии СУБД «Jatoba» поддерживается работа только на ОС, указанных в формуляре на поставку!

Степени важности примечаний, применяемые в документе:



Важная информация – указания, требующие особого внимания



Дополнительная информация – указания, позволяющие упростить работу с изделием

СОДЕРЖАНИЕ

| | |
|---|----|
| 1. Общие сведения о СУБД «Jatoba» | 6 |
| 1.1. Назначение СУБД «Jatoba» | 6 |
| 1.2. Функции СУБД «Jatoba» | 7 |
| 1.3. Требования к среде функционирования СУБД «Jatoba» | 7 |
| 2. Состав СУБД «Jatoba» | 10 |
| 2.1. Функциональные возможности и функциональные возможности по защите информации | 12 |
| 2.1.1. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ) | 12 |
| 2.1.2. Управление доступом субъектов доступа к объектам доступа (УПД) | 12 |
| 2.1.3. Регистрация событий безопасности (РСБ) | 12 |
| 2.1.4. Обеспечение целостности информационной системы и информации (ОЦЛ) | 13 |
| 2.1.5. Обеспечение доступности информации (ОДТ) | 13 |
| 2.1.6. Компоненты, расширяющие функции управления данными | 14 |
| 3. Подготовка к установке СУБД «Jatoba» | 16 |
| 4. Настройка параметров СУБД «Jatoba» | 17 |
| 4.1. Использование памяти | 17 |
| 4.2. Использование дискового пространства | 21 |
| 4.3. Использование ресурсов ядра | 22 |
| 4.4. Настройка режима вакуумизации на основе стоимостных оценок | 22 |
| 4.5. Настройка режима фоновой записи | 24 |
| 4.6. Настройка режима асинхронного поведения | 26 |
| 4.7. Параметры межсетевое взаимодействия | 29 |
| 4.7.1. Основные параметры, связанные с настройкой сети | 31 |
| 4.8. Настройка производительности СУБД «Jatoba» | 33 |
| 5. Основные операции в СУБД «Jatoba» | 34 |
| 5.1. Создание ролей в БД | 34 |
| 5.2. Удаление ролей в БД | 34 |
| 5.3. Создание БД | 35 |
| 5.4. Удаление БД | 36 |
| 6. Настройка безопасности СУБД «Jatoba» | 38 |
| 6.1. Идентификация и аутентификация субъектов доступа | 38 |
| 6.1.1. Настройка конфигурационного файла pg_hba.conf | 38 |
| 6.1.2. Настройка парольной политики | 39 |
| 6.2. Управление доступом субъектов доступа к объектам доступа | 70 |
| 6.2.1. Блокирование и разблокирование учетных записей | 70 |
| 6.2.2. Создание новых ролей, присвоение атрибутов и системных привилегий | 70 |
| 6.2.3. Создание ролей при активированной парольной политике | 75 |
| 6.3. Регистрация событий безопасности СУБД «Jatoba» | 76 |

| | |
|---|-----|
| 6.3.1. Настройки регистраций событий безопасности СУБД «Jatoba» под управлением ОС Windows Server..... | 76 |
| 6.3.2. Настройки регистрации событий безопасности СУБД «Jatoba» под управлением ОС семейства GNU/Linux..... | 77 |
| 6.3.3. Настройка расширенной регистрации событий безопасности..... | 78 |
| 7. Резервное копирование и восстановление баз данных | 89 |
| 7.1. Выгрузка кластера баз данных СУБД «Jatoba» в формате скрипта..... | 89 |
| 7.2. Выгрузка определенной базы данных СУБД «Jatoba» в формате скрипта в файл | 89 |
| 7.3. Восстановление базы данных СУБД «Jatoba» из файла архива..... | 89 |
| 7.4. Создание резервной копии файлов СУБД «Jatoba» | 90 |
| 8. Настройка отказоустойчивого кластера СУБД «Jatoba» | 91 |
| 8.1. Настройка отказоустойчивого кластера СУБД «Jatoba» на ОС Windows Server | 91 |
| 8.2. Настройка отказоустойчивого кластера СУБД «Jatoba» с использованием компонента «jaDog» | 98 |
| 9. Сообщения об ошибках | 99 |
| 10. Действия после сбоев и ошибок эксплуатации СУБД «Jatoba»..... | 113 |
| 10.1. Сбой активации лицензии..... | 113 |
| 10.2. Временная блокировка пользователей СУБД и суперпользователя..... | 114 |
| 10.3. Сбой инициализация расширения «securityprofile» | 116 |
| 10.4. Ошибки создания пользователя | 117 |
| 10.5. Ошибки, возникающие при использовании профиля парольных политик «securityprofile» | 117 |
| 10.6. Ошибка авторизации | 124 |
| 10.7. Контактные данные службы технической поддержки..... | 125 |
| 10.7.1. Версия изделия | 126 |
| Приложение 1 | 127 |
| Приложение 2 | 129 |
| Термины и определения..... | 136 |
| Перечень сокращений | 137 |

1. ОБЩИЕ СВЕДЕНИЯ О СУБД «JATOVA»

1.1. Назначение СУБД «Jatoba»

СУБД «Jatoba» является программным средством, предназначенным для создания и управления реляционными базами данных (далее – БД) на базе электронно-вычислительных машин (далее – ЭВМ) под управлением операционных систем (далее – ОС), представленных в таблице 1.1

Таблица 1.1 – 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 | — | — | — |

1.2. Функции СУБД «Jatoba»

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 следующие 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 контроль 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 и просмотра их состояния СУБД.

1.3. Требования к среде функционирования СУБД «Jatoba»

СУБД «Jatoba» устанавливается на ЭВМ с процессорами, имеющими архитектуру x86, x86-64 и AMD64, удовлетворяющие следующим аппаратным требованиям, указанным в таблице 1.2.

Таблица 1.2 – Программные и аппаратные требования к средствам вычислительной техники, на которых функционируют клиентская и серверная часть СУБД

| Параметр | Характеристика | Сертифицированная ОС |
|---|--|--------------------------|
| 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 1.1 | |
| Требования к программному обеспечению АРМ управления | | |
| Операционная система | Требования приведены в таблице 1.1 | |
| № изменения: _____ | Подпись отв. лица: _____ | Дата внесения изм: _____ |

| Параметр | Характеристика | Сертифицированная ОС |
|---|---|----------------------|
| Требования к аппаратному обеспечению сервера Jatoba data safe | | |
| 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, либо PS/2 интерфейсами | |
| Адаптер Ethernet | 100 Мбит/с | |
| Требования к программному обеспечению сервера Jatoba data safe | | |
| Поддерживаемые платформы | • win-x86; | — |
| | • win-x64; | — |
| | • win-arm; | — |
| | • osx-x64; | — |
| | • linux-x64; | X |
| | • linux-arm | X |
| СУБД | Защищенная система управления базами данных «Jatoba» | |
| Веб-сервер | IIS 10 | — |
| | Nginx | X |
| Компоненты | ASP.NET Core 6.0 Runtime (v6.0.1) – Windows Hosting Bundle Installer | — |
| Internet браузер | • Google Chrome; | X |
| | • Яндекс.Браузер; | X |
| | • Chromium; | X |
| | • Mozilla Firefox; | X |
| | • Opera; | X |
| | • Microsoft Edge | — |

2. СОСТАВ СУБД «ЯТОВА»

В состав СУБД «Jatoba» входят компоненты, указанные в таблице 1.2.

Таблица 2.1 – Программные и аппаратные требования к средствам вычислительной техники, на которых функционируют клиентская и серверная часть СУБД

| № | Наименование | Описание | J4 | | J5 | |
|----|--|---|---------------------|----------------------|---------------------|----------------------|
| | | | Дист. ¹⁾ | Обр.к. ²⁾ | Дист. ¹⁾ | Обр.к. ²⁾ |
| 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 1C | X | X | X | X |
| 5 | fulleq | компонент совместимости с 1C | X | X | X | X |
| 6 | mchar | компонент совместимости с 1C | X | X | X | X |
| 7 | online_analyze | компонент совместимости с 1C | X | X | X | X |
| 8 | plantuner | компонент совместимости с 1C | 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 | — |
| 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 |

| № | Наименование | Описание | J4 | | J5 | |
|----|------------------------|--|---------------------|----------------------|---------------------|----------------------|
| | | | Дист. ¹⁾ | Обр.к. ²⁾ | Дист. ¹⁾ | Обр.к. ²⁾ |
| 18 | pg_Cryogen | компонент компрессии данных СУБД | X | X | X | X |
| 19 | pg_Task | компонент планирования заданий СУБД | X | X | X | X |
| 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 паролями политиками пользователей СУБД | X | X | X | X |
| 24 | pg_ProBackup | компонент расширенного резервного копирования | X | — | X | — |
| 25 | PTrack | компонент расширенного резервного копирования | 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 высокопроизводительного кластера | — | — | X | X |
| 32 | TDS_FDW | компонент поддержки платформы Microsoft SQL Server | — | — | X | X |

Примечание:

- Дистрибутив.
- Образ контейнера.

2.1. Функциональные возможности и функциональные возможности по защите информации

2.1.1. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)

Функциональные возможности по идентификации и аутентификации пользователей (ИАФ.1) выполняются средствами СУБД и описаны в текущем документе:

Руководство администратора 643.72410666.00067-05 95 01

Установление характеристик пароля (ИАФ.4) обеспечивает компонент SecurityProfile, функциональные возможности которого описаны в текущем документе:

Руководство администратора 643.72410666.00067-05 95 01

2.1.2. Управление доступом субъектов доступа к объектам доступа (УПД)

Меры по управлению доступом субъектов доступа выполняются штатными средствами СУБД, описанными в данном документе:

Руководство администратора 643.72410666.00067-05 95 01

Функциональные возможности СУБД по заведению учетных записей пользователей (УПД.1) обеспечивает компонент «ja_Sync_LDAP». Описание компонента представлено в документе:

Руководство по настройке. Часть 8. Синхронизация учетных записей служб каталогов и СУБД. Компонент «ja_Sync_LDAP» 643.72410666.00067-05 98 01-08

Функциональной возможностью по назначению минимально необходимых прав и привилегий пользователям и администраторам (УПД.5) обладает компонент «Jatoba data vault». Описание компонента представлено в документе:

Руководство по настройке. Часть 2. Контроль субъектов доступа. Компонент «Jatoba data vault» 643.72410666.00067-05 98 01-02

2.1.3. Регистрация событий безопасности (РСБ)

Регистрация событий безопасности выполняется средствами СУБД. Для расширенного журналирования используется компонент pgAudit, функциональные возможности которого описаны в текущем документе:

Руководство администратора 643.72410666.00067-05 95 01

| | | |
|--------------------|--------------------------|--------------------------|
| № изменения: _____ | Подпись отв. лица: _____ | Дата внесения изм: _____ |
|--------------------|--------------------------|--------------------------|

Управление передачей событий безопасности выполняется компонентом «ja_Log», функциональные возможности которого описаны в документе:

Руководство по настройке. Часть 12. Централизованный сбор записей событий СУБД. Компонент «ja_Log» 643.72410666.00067-05 98 01-12

Компонент «Jatoba data safe» осуществляет управление передачи событий, а также обеспечивает:

- централизованное автоматизированное управление сбором, записью и хранением информации о событиях безопасности (РСБ.3);
- возможность просмотра и анализа информации о действиях отдельных пользователей в информационной системе (РСБ.8);
- постоянный и периодический контроль за состоянием целевых СУБД, уровнем их безопасности;
- управление кластером.

Подробное описание компонента приведено в документе:

Руководство по настройке. Часть 7. Пользовательский веб-интерфейс для администраторов. Компонент «Jatoba data safe» 643.72410666.00067-05 98 01-07

2.1.4. Обеспечение целостности информационной системы и информации (ОЦЛ)

Контроль целостности собственных компонентов по контрольным суммам осуществляется динамически в процессе работы СУБД (ОЦЛ.1) и обеспечивается компонентом «ja_CSum». Описание компонента приведено в документе:

Руководство по настройке. Часть 14. Компонент контроля целостности «ja_CSum» 643.72410666.00067-05 98 01-14

2.1.5. Обеспечение доступности информации (ОДТ)

Обеспечение доступности информации достигается периодическим резервным копированием информации (ОДТ.4) и обеспечением возможности восстановления информации (ОДТ.5). Функции по защите информации выполняет компонент «pg_ProBackup». Описание приведено в документе:

| | | |
|--------------------|--------------------------|--------------------------|
| № изменения: _____ | Подпись отв. лица: _____ | Дата внесения изм: _____ |
|--------------------|--------------------------|--------------------------|

Руководство по настройке. Часть 4. Расширенное резервное копирование. Компонент «pg_ProBackup» 643.72410666.00067-05 98 01-04

Обеспечение доступности информации также достигается кластеризацией серверов БД (ОДТ.6). Кластеризация БД может быть выполнена компонентом «jaDog». Описание компонента приведено в документе:

Руководство по настройке. Часть 1. Управление режимом работы узлов кластера. Компонент «jaDog» 643.72410666.00067-05 98 01-01 (версия 1.4.2)

Руководство по настройке. Часть 1. Управление режимом работы узлов кластера. Компонент «jaDog» 643.72410666.00067-05 98 02-01 (версия 2.0)

2.1.6. Компоненты, расширяющие функции управления данными

Прочие компоненты, расширяющие функциональные возможности СУБД, описаны в документах:

- *Руководство по настройке. Часть 3. Формирование отчетов по журналам СУБД. Компонент «pgBadger» 643.72410666.00067-05 98 01-03;*
- *Руководство по настройке. Часть 5. Планирование заданий СУБД. Компонент «pg_Task» 643.72410666.00067-05 98 01-05;*
- *Руководство по настройке. Часть 6. Формирование отчетов производительности СУБД. Компонент «pg_Profile» 643.72410666.00067-05 98 01-06;*
- *Руководство по настройке. Часть 9. Обфускация кода PL/pgSQL. Компонент «PLsPgSQL» 643.72410666.00067-05 98 01-09;*
- *Руководство по настройке. Часть 10. Компрессия данных СУБД. Компонент «pg_Cryogen» 643.72410666.00067-05 98 01-10;*
- *Руководство по настройке. Часть 11. Высокопроизводительный кластер. Компонент «ja_Hipe_Cluster» 643.72410666.00067-05 98 01-11;*
- *Руководство по настройке. Часть 13. Поддержка платформы IC 643.72410666.00067-05 98 01-13;*
- *Руководство по настройке. Часть 15. Балансировка подключений пользователей к СУБД. Компонент «jaPooler» 643.72410666.00067-05 98 01-15;*

- *Руководство по настройке. Часть 16. Обеспечение работы с СУБД Oracle. 643.72410666.00067-05 98 01-16;*
- *Руководство по настройке. Часть 17. Выявление и предотвращение исполнения нетипичных SQL-запросов. Компонент «SQL_Firewall» 643.72410666.00067-05 98 01-17;*
- *Руководство по настройке. Часть 18. Соккрытие информации в файлах данных СУБД. Компонент «Jatoba crypto access storage» 643.72410666.00067-05 98 01-18;*
- *Руководство по настройке. Часть 19. Формирование HTTP/HTTPS запросов из СУБД. Компонент «pgSQL-HTTP» 643.72410666.00067-05 98 01-19;*
- *Руководство по настройке. Часть 20. Компонент «TDS_FDW» 643.72410666.00067-05 98 01-20;*
- *Руководство по настройке. Часть 21. Управление планами запросов. Компонент «ja_Plan_Manager» 643.72410666.00067-05 98 01-21.*

3. ПОДГОТОВКА К УСТАНОВКЕ СУБД «JATOBA»

Комплект установочных файлов СУБД «Jatoba» с документацией поставляется заказчику на установочном компакт-диске.

Перед началом установки необходимо:

а) проверить комплектность поставки СУБД «Jatoba» в соответствии с требованиями раздела 4 документа «Защищенная система управления базами данных «Jatoba». Формуляр» 643.72410666.00067-05 30 01;

б) провести визуальный осмотр компакт-диска с дистрибутивными файлами и эксплуатационной документацией на предмет повреждений;

в) выполнить проверку информации, записанной на компакт-диске, на возможность чтения и соответствия имен файлов и их контрольных сумм, указанным в перечне файлов, приведенном в Приложении 1 к документу «Защищенная система управления базами данных «Jatoba». Формуляр» 643.72410666.00067-05 30 01.

Контрольные суммы установочных файлов на дистрибутивном компакт-диске СУБД «Jatoba» получены с помощью программы фиксации и контроля исходного состояния программного комплекса «ФИКС» версии 2.0.2 (производитель ЗАО «ЦБИ-сервис») по алгоритму «Уровень-3».

Установка СУБД проводится в соответствии с документом «Защищенная система управления базами данных «Jatoba». Руководство по установке» 643.72410666.00067-05 97 01.

4. НАСТРОЙКА ПАРАМЕТРОВ СУБД «ЯТОВА»

В данном разделе описываются основные параметры конфигурации, которые влияют на работу БД.

4.1. Использование памяти

```
shared_buffers (integer)
```

Задаёт объем разделяемой памяти, которую сервер баз данных будет использовать для размещения буферов со страницами файлов данных. Данная память будет совместно использоваться всеми процессами СУБД.

По умолчанию значение `shared_buffers` = 128 МВ, но может быть меньше, если такой объем не поддерживается операционной системой (определяется в процессе инициализации директории данных служебной утилитой `initdb`). Значение этого параметра не может быть меньше 128 КВ (килобайт) (минимум зависит от величины `BLCKSZ` – размер блока данных в файле данных, по умолчанию 8 КВ). Для хорошей производительности требуются большие значения.

После настройки данного параметра для вступления его в действие требуется перезапуск сервера.

При использовании сервера с объемом ОЗУ 1 Гб наиболее оптимальным начальным значением `shared_buffers` будет 25% от объема памяти. Увеличение `shared_buffers` обычно требует увеличения `max_wal_size`, чтобы растянуть процесс записи большого объема новых или измененных данных на больший промежуток времени.

При использовании сервера с объемом ОЗУ меньше 1 Гб стоит ограничиться меньшим процентом ОЗУ, чтобы оставить достаточно места операционной системе.

```
huge_pages (enum)
```

Определяет, будут ли запрашиваться страницы большого размера (`huge pages`) из основной области разделяемой памяти.

При `huge_pages` = `try` (по умолчанию) сервер будет запрашивать выделение памяти страницами большого размера. Если сервер получит ошибку выделения памяти, то

он вернется к стандартному поведению (выделение памяти страницами стандартного размера).

При `huge_pages = on` сервер не будет запущен, если в ОС не будет возможности выделять память страницами большого размера.

При `huge_pages = off` выделение памяти будет производиться страницами стандартного размера.



Данный параметр поддерживается только в ОС Linux и Windows. В остальных ОС значение `try` игнорируется.

В результате использования страниц большого размера уменьшаются риски промахов в TLB кэше и процессор тратит меньше времени на преобразование адресов, что приводит к увеличению быстродействия.

Для того, чтобы пользователь мог использовать страницы большого размера в ОС Windows, необходимо дать пользователю Windows, от имени которого работает СУБД «Jatoba», право блокировки страниц в памяти (Lock Pages in Memory в управлении групповой политикой в Windows).

```
temp_buffers (integer)
```

Задаёт максимальное число временных буферов для каждой сессии пользователя.

По умолчанию `temp_buffers = 8` (8MB = 1024 буфера).

Данный параметр можно изменить до первого обращения к временным таблицам в рамках сессии пользователя. После изменить значение этого параметра для текущей сессии будет невозможно.

В рамках сессии временные буферы выделяются по мере необходимости до достижения предела, который задан параметром `temp_buffers`. Если сессия не задействует временные буферы, то для него хранятся только дескрипторы буферов, которые занимают около 64 байт (в количестве `temp_buffers`). Если буфер используется, он будет дополнительно занимать 8192 байта (или `BLCKSZ` байт, в общем случае).

```
max_prepared_transactions (integer)
```

Задаёт максимальное число транзакций, которые могут одновременно находиться в «подготовленном» состоянии.

По умолчанию `max_prepared_transactions = 0` отключается механизм подготовленных транзакций. Задать данный параметр можно только при запуске сервера.

Если нет необходимости использовать подготовленные транзакции, следует обнулить параметр, чтобы не допустить непреднамеренного создания подготовленных транзакций. Если подготовленные транзакции используются, то `max_prepared_transactions` должен быть не меньше, чем `max_connections` для подготовки транзакции в каждом сеансе.



Для ведомого сервера значение этого параметра должно быть больше или равно значению на ведущем. В противном случае, на ведомом сервере запросы будут запрещены.

```
work_mem (integer)
```

Задаёт объем памяти, который будет использоваться для внутренних операций сортировки и хэш-таблиц прежде чем будут задействованы временные файлы на диске.

По умолчанию `work_mem = 4` (4 Мб). В сложных запросах может одновременно выполняться несколько операций сортировки или хэширования, при этом, указанный объем памяти может использоваться в каждой операции перед тем, как данные начнут перемещаться во временные файлы.

Общий объем памяти может превосходить значение `work_mem`. Операции сортировки используются для `ORDER BY`, `DISTINCT` и соединений слиянием.

```
maintenance_work_mem (integer)
```

Задаёт максимальный объем памяти для операций обслуживания БД, таких как `VACUUM`, `CREATE INDEX` и `ALTER TABLE ADD FOREIGN KEY`.

По умолчанию `maintenance_work_mem (integer) = 64 (64 Мб)`. Увеличение данного значения может привести к ускорению операций очистки и восстановления БД из копии.

При работе автовакуума объем памяти выделяется `autovacuum_max_workers` один раз, не рекомендуется устанавливать значение по умолчанию слишком большим. Управлять объемом памяти для автовакуума предпочтительно отдельно, изменяя `autovacuum_work_mem`.



Для сбора идентификаторов мертвых кортежей `VACUUM` может использовать не более 1Гб памяти.

```
autovacuum_work_mem (integer)
```

Задаёт максимальный объем памяти, который будет использовать каждый рабочий процесс автовакуума.

При значении по умолчанию `autovacuum_work_mem = -1` объем определяется значением `maintenance_work_mem`. Данный параметр не влияет на поведение команды `VACUUM`, которая может выполняться в других контекстах. Задать этот параметр можно только в `postgresql.conf` или в командной строке при запуске сервера. Увеличение `autovacuum_work_mem` до большего значения не повлияет на количество обнаруженных удаленных записей, которые автовакуум собирает при сканировании таблицы.



Для сбора идентификаторов мертвых кортежей `VACUUM` может использовать не более 1Гб памяти.

```
max_stack_depth (integer)
```

Задаёт максимальную безопасную глубину стека для исполнителя.

По умолчанию `max_stack_depth = 2 (2 Мб)`. Значение выбрано с запасом, переполнение стека невозможно за исключением выполнения сложных функций. Изменить этот параметр могут только суперпользователи.

Данное значение рекомендуется ставить равным предельному размеру стека, ограниченному ядром (который устанавливается командой `ulimit -s` или аналогичной), за вычетом запаса в 1 Мб. Запас необходим для потенциально рекурсивных процедур.



При превышении значения `max_stack_depth` фактического предела ядра, функция с неограниченной рекурсией сможет вызвать экстренное завершение работы отдельного процесса сервера.

```
dynamic_shared_memory_type (enum)
```

Выбирает механизм динамической разделяемой памяти, который будет использоваться сервером.

— при `dynamic_shared_memory_type = posix` происходит выделение разделяемой памяти POSIX функцией `shm_open` (данный механизм ставится по умолчанию);

— при `dynamic_shared_memory_type = sysv` происходит выделение разделяемой памяти System V функцией `shmget`;

— при `dynamic_shared_memory_type = windows` происходит выделение разделяемой памяти в Windows;

— при `dynamic_shared_memory_type = mmap` происходит эмуляция разделяемой памяти через отображение в память файлов, хранящихся в каталоге данных;

— при `dynamic_shared_memory_type = none` происходит отключение этой функциональности.

4.2. Использование дискового пространства

```
temp_file_limit (integer)
```

Задаёт максимальный объём дискового пространства, который сможет использовать один процесс для временных файлов, например, при сортировке и хэшировании или для сохранения удерживаемого курсора. Транзакция, которая попытается превысить этот предел, будет отменена.

По умолчанию `temp_file_limit = -1` (-1kB) означает, что предел отсутствует. Изменить данный параметр могут только суперпользователи.

Этот параметр ограничивает общий объем, который могут занимать в момент времени все временные файлы, которые задействованы в данном процессе СУБД.



Это не касается файлов явно создаваемых временных таблиц.

Ограничивается объем временных файлов, которые создаются неявно при выполнении запросов.

4.3. Использование ресурсов ядра

```
max_files_per_process (integer)
```

Задаёт максимальное число файлов, которые могут быть одновременно открыты каждым серверным подпроцессом.

По умолчанию `max_files_per_process = 1000` файлов. Задать этот параметр можно только при запуске сервера.

Если ядро реализует безопасное ограничение по процессам, то значение данного параметра можно не менять. На некоторых платформах ядро позволяет отдельному процессу открыть больше файлов, чем могут открыть несколько процессов одновременно. При возникновении ошибки «Too many open files», необходимо уменьшить значение параметра.

4.4. Настройка режима вакуумизации на основе стоимостных оценок

Во время выполнения команд `VACUUM` и `ANALYZE` система ведёт внутренний счетчик, в котором суммируется оцениваемая стоимость различных выполняемых операций ввода/вывода. При превышении накопленной стоимости `vacuum_cost_limit`, процесс, выполняющий эту операцию, отключается на время `vacuum_cost_delay`, после чего счетчик сбрасывается и процесс продолжается.

Данный подход реализован для снижения влияния этих команд на параллельную работу с базой, за счет уменьшения нагрузки на подсистему ввода-вывода. Важно, чтобы команды меньше влияли на выполнение других операций с базой данных. Данным процессом могут управлять администраторы.

| | | |
|--------------------|--------------------------|--------------------------|
| № изменения: _____ | Подпись отв. лица: _____ | Дата внесения изм: _____ |
|--------------------|--------------------------|--------------------------|

По умолчанию данный режим отключен для выполняемых вручную команд VACUUM. Для его включения нужно установить в `vacuum_cost_delay` ненулевое значение.

```
vacuum_cost_delay(integer)
```

Продолжительность времени, в течение которого будет простаивать процесс, превысивший предел стоимости.

По умолчанию `vacuum_cost_delay = 0` (0 мс) – задержка очистки отсутствует. При положительных значениях интенсивность очистки будет зависеть от стоимости.



Разрешение таймера `vacuum_cost_delay` должно быть кратно 10.

При настройке интенсивности очистки для `vacuum_cost_delay` выбираются небольшие значения (например, 10 или 20 мс). Для точного ограничения потребления ресурсов при очистке рекомендуется изменять другие параметры стоимости очистки.

```
vacuum_cost_page_hit (integer)
```

Примерная стоимость очистки буфера, оказавшегося в общем кэше. Содержит в себе блокировку пула буферов, поиск в хэш-таблице и сканирование содержимого страницы.

По умолчанию `vacuum_cost_page_hit = 1`.

```
vacuum_cost_page_miss (integer)
```

Примерная стоимость очистки буфера, который нужно прочитать с диска. Содержит в себе блокировку пула буферов, поиск в хэш-таблице, чтение требуемого блока с диска и сканирование его содержимого.

По умолчанию `vacuum_cost_page_miss = 10`.

```
vacuum_cost_page_dirty (integer)
```

Примерная стоимость очистки, при которой изменяется блок, не модифицированный ранее. В данный параметр включается дополнительная стоимость ввода/вывода, связанная с записью измененного блока на диск.

По умолчанию `vacuum_cost_page_dirty = 20`.

```
vacuum_cost_limit (integer)
```

Общая стоимость, при накоплении которой процесс очистки будет выключаться.

По умолчанию `vacuum_cost_limit = 200`.



Некоторые операции могут устанавливать критические блокировки и должны завершаться как можно быстрее. Во время таких операций задержка очистки по стоимости не осуществляется, поэтому накопленная за это время стоимость может быть больше установленного предела.

Во избежание ненужных длительных задержек фактическая задержка вычисляется по формуле:

$$\text{vacuum_cost_delay} * \text{accumulated_balance} / \text{vacuum_cost_limit} \leq \text{vacuum_cost_delay} * 4.$$

4.5. Настройка режима фоновой записи

В числе специальных процессов сервера есть процесс фоновой записи, задачей которого является осуществление записей новых или измененных («грязных») общих буферов на диск. При недостаточном количестве чистых общих буферов данный процесс записывает грязные буферы в файловую систему и помечает их как чистые. Процесс фоновой записи увеличивает общую нагрузку на подсистему ввода/вывода, так как может записывать изменяемую страницу несколько раз, хотя ее можно было бы записать один раз в момент контрольной точки.

```
bgwriter_delay (integer)
```

Задаёт задержку между раундами активности процесса фоновой записи. Во время раунда процесс осуществляет запись определенного количества загрязненных буферов. Затем данный процесс выключается на время `bgwriter_delay` (в миллисекундах) и так повторяется. Если в пуле не остается загрязненных буферов, он может быть неактивен более длительное время.

По умолчанию `bgwriter_delay = 200 (200ms)`. Задать параметр можно в `postgresql.conf` или в командной строке при запуске сервера.

| | | |
|--------------------|--------------------------|--------------------------|
| № изменения: _____ | Подпись отв. лица: _____ | Дата внесения изм: _____ |
|--------------------|--------------------------|--------------------------|


```
bgwriter_lru_maxpages (integer)
```

Задаёт максимальное число буферов, которое сможет записать процесс фоновой записи за раунд активности.

По умолчанию `bgwriter_lru_maxpages = 100` (100 буферов).

При `bgwriter_lru_maxpages = 0` фоновая запись отключается. Задать параметр можно в `postgresql.conf` или в командной строке при запуске сервера.

```
bgwriter_lru_multiplier (floating point)
```

Число загрязнённых буферов, записываемых в очередном раунде, которое зависит от количества новых буферов, требуемых серверным процессам в предыдущих раундах.

По умолчанию `bgwriter_lru_multiplier = 2.0`. Задать параметр можно в `postgresql.conf` или в командной строке при запуске сервера.

Значение `bgwriter_lru_multiplier` умножается на накопленное усреднённое значение количества использованных буферов на предыдущих раундах и получается значение, равное количеству буферов для следующего раунда. Процесс фоновой записи пишет на диск и освобождает буферы до тех пор, пока число свободных буферов не достигнет целевого значения. Число буферов, которые записаны за раунд, ограничиваются параметром `bgwriter_lru_maxpages`.

```
bgwriter_flush_after (integer)
```

При большем количестве байт, которые записываются процессом фоновой записи, чем `bgwriter_flush_after`, сервер посылает команду ОС произвести запись этих данных в нижележащее хранилище. Это ограничивает объём «грязных» данных в страничном кэше ядра и уменьшает вероятность затормаживания при выполнении `fsync` в конце контрольной точки или, когда ОС сбрасывает данные на диск большими порциями в фоне.

По умолчанию в ОС Linux `bgwriter_flush_after = 512` (512kB). В других ОС `bgwriter_flush_after = 0`.

Параметр действует не на всех платформах и может принимать значение от 0 (управление отложенной записью отключается) до 2 мегабайт (2 Мб). Если `BLCKSZ` отличен от 8 КБ, максимальное значение корректируется пропорционально. Задать этот параметр можно только в `postgresql.conf` или в командной строке при запуске сервера.

4.6. Настройка режима асинхронного поведения

```
effective_io_concurrency (integer)
```

Задаёт допустимое число параллельных операций ввода/вывода, которое могут быть выполнены одновременно. Чем больше это число, тем больше операций ввода/вывода будет пытаться выполнить СУБД параллельно в отдельном сеансе. Допустимые значения находятся в интервале от 1 до 1000, а нулевое значение отключает асинхронные запросы ввода/вывода.

Для магнитных носителей начальным значением этого параметра будет являться число отдельных дисков, составляющих массив RAID 0 или RAID 1, в котором размещена база данных. Если база данных часто обрабатывает множество запросов в различных сеансах, то при небольших значениях дисковый массив может быть полностью загружен. При увеличении этого значения при полной загрузке дисков, это приведет к увеличению нагрузки на процессор.

По умолчанию `effective_io_concurrency = 1`, где данный параметр поддерживается, и `effective_io_concurrency = 0` – в остальных. Значение можно переопределить для таблиц в определенном табличном пространстве, установив одноименный параметр табличного пространства.

```
max_worker_processes (integer)
```

Задаёт максимальное число фоновых процессов, которое можно запустить в текущей системе.

По умолчанию `max_worker_processes = 8`. Параметр можно задать только при запуске сервера.

Для ведомого сервера значение данного параметра должно быть больше или равно значению на ведущем. В противном случае на ведомом сервере не будут разрешены запросы.

```
max_parallel_workers_per_gather (integer)
```

Задаёт максимальное число рабочих процессов, которые могут запускаться одним узлом плана запроса Gather или Gather Merge (сбор результатов с рабочих процессов). Параллельные рабочие процессы берутся из пула процессов, который контролируется параметром `max_worker_processes`, в количестве, ограничиваемом значением `max_parallel_workers`. Запрошенное количество рабочих процессов может быть недоступно во время выполнения. В таком случае параметр будет выполняться с меньшим числом процессов, что может быть неэффективно.

По умолчанию `max_parallel_workers_per_gather = 2`.

При `max_parallel_workers_per_gather = 0` отключается параллельное выполнение запросов.

Параллельные запросы потребляют больше ресурсов, чем непараллельные, так как каждый рабочий процесс является отдельным процессом. Рекомендуется это учитывать, выбирая значение параметра, а также настраивая другие параметры, управляющие использованием ресурсов.

```
max_parallel_maintenance_workers (integer)
```

Задаёт максимальное число рабочих процессов, которые могут запускаться одной служебной командой. Параллельные рабочие процессы берутся из пула процессов, который контролируется параметром `max_worker_processes`, в количестве, ограничиваемом значением `max_parallel_workers`. Запрошенное количество рабочих процессов может быть недоступно во время выполнения. В таком случае служебная операция будет выполняться с меньшим числом процессов, чем ожидалось.

По умолчанию `max_parallel_maintenance_workers = 2`.

При `max_parallel_maintenance_workers = 0` отключается использование параллельных исполнителей служебными командами.

| | | |
|--------------------|--------------------------|--------------------------|
| № изменения: _____ | Подпись отв. лица: _____ | Дата внесения изм: _____ |
|--------------------|--------------------------|--------------------------|

Параллельно выполняемые служебные команды не должны потреблять значительно больше памяти, чем равнозначные непараллельные операции. Это отличает их от параллельных запросов, при выполнении которых ограничения ресурсов действуют на отдельные рабочие процессы.

```
max_parallel_workers (integer)
```

Задаёт максимальное число рабочих процессов, которое система сможет поддерживать для параллельных операций.

По умолчанию `max_parallel_workers = 8`.

Значение данного параметра, которое превышает значение `max_worker_processes`, не будет действовать, так как параллельные рабочие процессы берутся из пула рабочих процессов, ограничиваемого этим параметром.

```
backend_flush_after (integer)
```

Если при одном обслуживающем процессе записывается больше чем `backend_flush_after` байт, сервер даёт указание ОС произвести запись этих данных в нижележащее хранилище. Это ограничивает объём «грязных» данных в страничном кэше ядра и уменьшает вероятность затормаживания при выполнении `fsync` в конце контрольной точки или, когда ОС сбрасывает данные на диск большими порциями в фоне.

По умолчанию `backend_flush_after = 0`, процесс отключен.

Параметр действует не на всех платформах и может принимать значение от 0 (управление отложенной записью отключается) до 2 мегабайт (2 Мб). Если `BLCKSZ` отличен от 8 КБ, максимальное значение корректируется пропорционально.

```
old_snapshot_threshold (integer)
```

Задаёт минимальное время, которое позволяет использовать снимок без ошибки о давности снимка. Данный параметр можно задать только при запуске сервера.

По умолчанию `old_snapshot_threshold = -1` отключает этот процесс. Нужные значения для производственной среды могут лежать в интервале от нескольких часов до нескольких дней. Заданное значение округляется до минут. При многих видах

| | | |
|--------------------|--------------------------|--------------------------|
| № изменения: _____ | Подпись отв. лица: _____ | Дата внесения изм: _____ |
|--------------------|--------------------------|--------------------------|

нагрузки критичное замусоривание базы или заикливание идентификаторов транзакций может происходить за меньший промежуток времени.

4.7. Параметры межсетевого взаимодействия

СУБД «Jatoba» имеет клиент-серверную архитектуру. Для подключения к СУБД используются протоколы Libpq и Jadog.

Libpq – протокол, который используется для подключения к БД пользователей. Протокол Libpq реализован в виде драйвера «Driver Libpq» и обязательно требуется для работы приложений с СУБД. Дополнительно можно использовать ODBC драйвера, если приложения поддерживают подключение к СУБД через API ODBC.

Jadog – проприетарный протокол, используется для подключения к СУБД привилегированных пользователей, который обеспечивает взаимодействие между СВТ и сервером СУБД в среде функционирования изделия. При этом не используется драйвер протокола Libpq. Инициирование подключения осуществляет клиентское приложение.

Протоколы Libpq и Jadog используют стек протоколов TCP/IP и Unix-сокеты в клиент-серверном исполнении Изделия.

Параметры стека протоколов приведены в таблице 4.1.

Таблица 4.1 – Параметры протоколов используемых СУБД

| Наименование | Протокол | Параметры |
|---|----------|--------------|
| Протокол (соединения пользователей) | Libpq | 5432 |
| Протокол (соединения администраторов) | Jadog | 54321, 54322 |
| Протокол аутентификации LDAP | LDAP | 389 |
| Протокол аутентификации GSSAPI | GSSAPI | 389 |
| Протокол аутентификации SSPI | SSPI | 389 |
| Протокол аутентификации Radius | Radius | 389 |
| Протокол передачи данных HTTPS | HTTPS | 443,5000 |
| Протокол аутентификации SSL | SSL | 5432 |
| Протокол электронной почты | SMTP | 25, 587 |
| Протокол передачи сообщений на веб-сервер ZULIP | ZULIP | 443 |

| | | |
|--------------------|--------------------------|--------------------------|
| № изменения: _____ | Подпись отв. лица: _____ | Дата внесения изм: _____ |
|--------------------|--------------------------|--------------------------|

Клиентское приложение образует с серверной частью СУБД канал (сессию) взаимодействия по специальным протоколам, основанным на сообщениях.

Пользователи БД используют протокол Librq и порт 5432.

Администратор СУБД и администраторы БД используют протокол Jadog. Подключение к СУБД может происходить по портам 54321 и 54322. В качестве резервного интерфейса подключения может использоваться подключение по протоколу Librq на порт 5432.

Схема подключения представлена на рисунке 4.1.

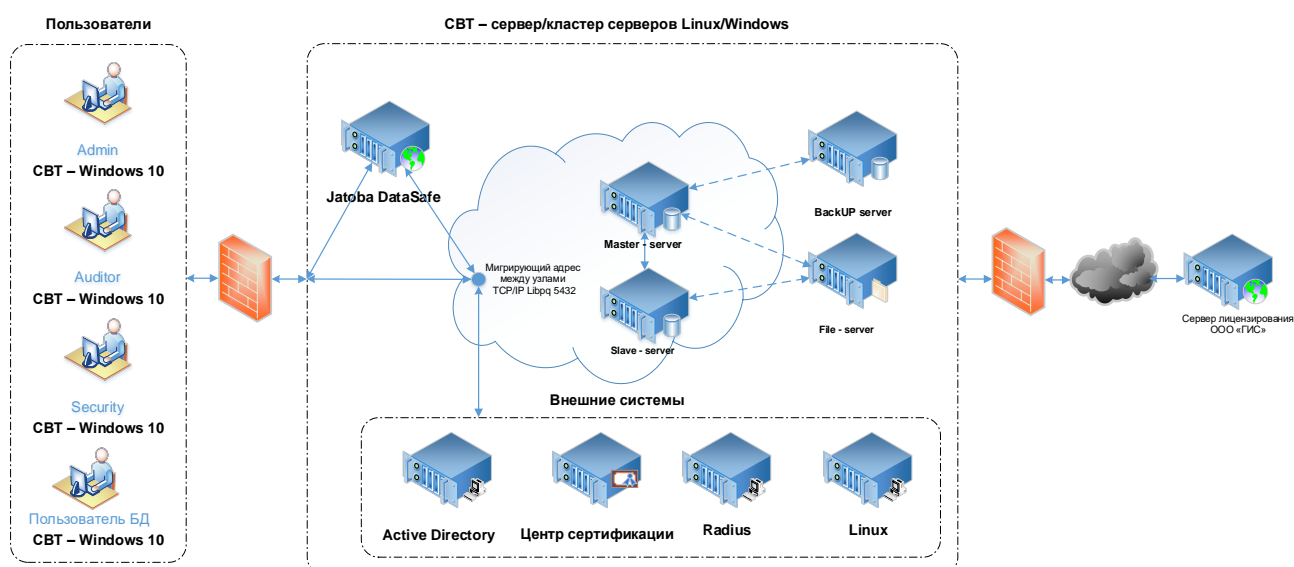


Рисунок 4.1 – Интерфейсы подключения СУБД

Для взаимодействия с сервером лицензирования СУБД использует протокол HTTPS по порту 443.

протокол HTTPS по порту 443 используется для взаимодействия:

- СУБД с сервером лицензирования;
- компонента «Jatoba Data Safe» и служебной СУБД.

4.7.1. Основные параметры, связанные с настройкой сети

```
listen_addresses (string)
```

Указывает TCP/IP-адреса, по которым сервер будет принимать подключения клиентских приложений. Значение принимает форму списка имен и/или числовых IP-адресов компьютеров, разделенную запятыми. Специальный элемент * обозначает все доступные IP-интерфейсы. Запись 0.0.0.0 позволяет задействовать все адреса IPv4, а :: – позволяет задействовать все адреса IPv6. Если список пуст, сервер не будет привязываться ни к какому IP-интерфейсу, в этом случае подключиться к нему можно будет только через Unix-сокеты.

По умолчанию – localhost, что позволяет устанавливать подключение к серверу по TCP/IP только через локальный интерфейс «замыкания». Параметр можно задать только при запуске сервера.

```
port (integer)
```

TCP-порт, запускаемый сервером.

По умолчанию – 5432.

Порт используется для всех IP-адресов, через которые сервер принимает подключения. Параметр можно задать только при запуске сервера.

```
max_connections (integer)
```

Определяет максимальное количество одновременных подключений к серверу БД.

По умолчанию – 100 подключений. Это число может быть меньше, если настройки ядра накладывают ограничения (определяется в процессе initdb). Параметр можно задать только при запуске сервера.

Для ведомого сервера значение параметра должно быть больше или равно значению на ведущем. В обратном случае запросы на ведомом сервере не будут разрешены.

```
superuser_reserved_connections (integer)
```

Определяет количество «слотов» подключений, зарезервированных для соединений суперпользователями. Одновременно могут быть активны не более `max_connections` подключений. Когда число активных одновременных подключений $\geq \text{max_connections} - \text{superuser_reserved_connections}$, новые подключения принимаются только для суперпользователей, все остальные подключения, в том числе подключения для репликации, запрещаются.

По умолчанию резервируются три соединения. Это значение должно быть $< \text{max_connections} - \text{max_wal_senders}$. Задать этот параметр можно только при запуске сервера.

```
unix_socket_directories (string)
```

Задает каталог Unix-сокета, через который сервер будет принимать подключения клиентских приложений. Можно создать несколько сокетов, перечислив в этом значении несколько каталогов через запятую. Пробелы между записями игнорируются, если в пути каталога содержатся пробелы, его нужно прописать в двойных кавычках. При пустом значении сервер не будет работать с Unix-сокетами, в этом случае к нему можно подключиться только по TCP/IP.

Значение по умолчанию обычно `/tmp`. Его можно изменить во время сборки. Задать параметр можно только при запуске сервера.

В дополнение к самому файлу сокета, который называется `.s.PGSQL.nnnn` (где `nnnn` – номер порта сервера), в каждом каталоге `unix_socket_directories` будет создан обычный файл с именем `.s.PGSQL.nnnn.lock`. Ни один из файлов нельзя удалять вручную.

Этот параметр не действует в ОС Windows, так как в ней нет Unix-сокетов.

4.8. Настройка производительности СУБД «Jatoba»

```
std_fuzz_factor(numeric)
```

Глобальный параметр «std_fuzz_factor» позволяет расширить диапазон оценок планов при сравнении различных планов-кандидатов и таким образом, включить больше планов в кандидаты на выяснение лучшего.

Чем больше значение параметра «std_fuzz_factor», тем больше кандидатов будет рассматривать планировщик запросов. В результате в список кандидатов могут быть включены более оптимальные планы с потенциально большей производительностью, но схожие по оценке с другими кандидатами. Таким образом, регулируя значение параметра может повышаться общая производительность СУБД и скорость исполнения запросов.

Значением по умолчанию параметра является – «1,01». Возможный диапазон значений параметра «std_fuzz_factor» варьируется от 0,9 до 1,9.

Увеличение значение параметра приводит к возрастанию временных затрат на формирование планов запросов. Эффективное значение параметра определяется практической эксплуатацией в зависимости от сложности выполняемых запросов в СУБД.

5. ОСНОВНЫЕ ОПЕРАЦИИ В СУБД «ЯТОВА»

5.1. Создание ролей в БД

Роли баз данных являются глобальными для всей СУБД (не для отдельной базы данных).

При начальной установке СУБД содержит одну предопределенную роль postgres, обладающую максимальными привилегиями (SUPERUSER).



Для создания других ролей нужно подключиться под ролью postgres.

Создать роль возможно двумя способами:

- SQL-командой:

```
CREATE ROLE <имя>;
```

- Утилитой командной строки:

```
createuser <имя>
```

Подключение к серверу баз данных выполняется от имени и с правами конкретной учетной записи с указанием конкретной базы данных.

Наличие доступа к объектам СУБД и БД, а также возможность выполнения команд определяется назначенными роли атрибутами и системными привилегиями.

5.2. Удаление ролей в БД

Роль может быть удалена двумя способами:

- SQL-командой:

```
DROP ROLE <имя>;
```

- Утилитой командной строки:

```
dropuser <имя>
```

Роли могут владеть объектами баз данных и иметь права доступа к объектам других пользователей. При удалении роли необходимо убедиться, что объекты, принадлежащие данной роли, были переданы другой роли или удалены.

Право владения объектами можно передавать в индивидуальном порядке с использованием команды ALTER. Например, для таблиц команда ALTER выглядит следующим образом:

```
ALTER TABLE <имя_таблицы> OWNER TO <принимающая_роль>;
```

Переназначение владения для отдельных объектов может быть проблематичным, если в БД пользователя насчитывается большое количество объектов. Для переназначения права владения всеми объектами с удаляемой роли можно воспользоваться командой REASSIGN OWNED.

```
REASSIGN OWNED BY <удаляемая_роль> TO <новая_роль>;
```

При удалении объектов, которыми владеет удаляемая роль, можно использовать следующие команды.

Для удаления отдельных объектов БД используется команда DROP. Например, для удаления отдельной таблицы:

```
DROP TABLE <имя_таблицы>;
```

Для массового удаления объектов, принадлежащих удаляемой роли, используется команда DROP OWNED.

```
DROP OWNED BY <удаляемая_роль>;
```



DROP OWNED не удаляет табличные пространства и базы данных целиком. Это необходимо сделать вручную, убедившись, что удаляемые данные не представляют ценности.

5.3. Создание БД

Для создания базы данных сервер СУБД «Jatoba» должен быть развернут и запущен.



Пользователь, создающий БД, автоматически назначается ее владельцем. Владелец может удалить свою базу, что приведет к удалению всех объектов.

Только пользователь обладающий привилегиями CREATEDB и SUPERUSER, может создавать новые БД.

Создать БД можно двумя способами:

- SQL-командой:

```
CREATE DATABASE <имя>;
```

Для выполнения команды CREATE DATABASE необходимо подключение к серверу баз данных. При установке СУБД всегда содержит служебную БД postgres, к которой необходимо подключиться для создания других БД.

- Утилитой командной строки createdb. Если имя БД не указано в параметрах командной строки, то эта утилита создаст базу данных с именем текущего пользователя:

```
createdb <имя>
```

В случае создания базы данных одним пользователем для другого пользователя и назначении его владельцем используется одна из следующих команд:

- SQL-команда:

```
CREATE DATABASE <имя_базы> OWNER <имя_роли>;
```

- Утилита командной строки:

```
createdb -O <имя_роли> <имя_базы>
```

5.4. Удаление БД

Удалить базу данных могут только или владелец базы данных, или пользователь, обладающий максимальными привилегиями (SUPERUSER).

Удалить БД можно двумя способами:

- SQL-командой:

```
DROP DATABASE <имя>;
```

- Утилитой командной строки

```
dropdb <имя>
```

Выполнить команду удаления БД невозможно, пока существует хоть одно подключение к базе.



При удалении БД удаляются все ее объекты. Удаление БД необратимая операция.

6. НАСТРОЙКА БЕЗОПАСНОСТИ СУБД «ЯТОВА»

6.1. Идентификация и аутентификация субъектов доступа

Идентификация пользователей в СУБД «Jatoba» осуществляется по уникальным именам. Для создания пользователей в СУБД «Jatoba» необходимо от учетной записи администратора СУБД выполнить следующую команду:

```
CREATE ROLE <имя учетной записи пользователя>;
```

Аутентификация пользователей осуществляется с использованием паролей (метод аутентификации (md5, password)).

Для настройки аутентификации пользователей необходимо:

- а) настроить конфигурационный файл `pg_hba.conf` под необходимый метод аутентификации;
- б) настроить парольную политику.

6.1.1. Настройка конфигурационного файла `pg_hba.conf`

Для настройки конфигурационного файла `pg_hba.conf` необходимо выполнить следующие действия:

- а) от учетной записи администратора СУБД подключиться к ОС и открыть файл `pg_hba.conf`¹⁾;
- б) в открывшемся файле `pg_hba.conf` внести необходимые записи в определенном формате:

| TYPE | DATABASE | USER | ADDRESS | METHOD |
|----------------|-------------|---------------------|--------------|-----------------------------|
| <i>local</i> | <i>база</i> | <i>пользователь</i> | ----- | <i>метод-аутентификации</i> |
| <i>host</i> | <i>база</i> | <i>пользователь</i> | <i>адрес</i> | <i>метод-аутентификации</i> |
| <i>hostssl</i> | <i>база</i> | <i>пользователь</i> | <i>адрес</i> | <i>метод-аутентификации</i> |

¹⁾ Местонахождение файла `pg_hba.conf` по умолчанию:

- ОС семейства GNU/Linux: `/var/lib/jatoba/4/data/pg_hba.conf`;
- ОС Windows: `C:\Program Files\GIS\Jatoba\4\data\pg_hba.conf`.

| TYPE | DATABASE | USER | ADDRESS | METHOD |
|-----------------|-------------|---------------------|---------------------------------|--------------------------------|
| <i>hostnssl</i> | <i>база</i> | <i>пользователь</i> | <i>адрес</i> | <i>метод-аутентификации</i> |
| <i>host</i> | <i>база</i> | <i>пользователь</i> | <i>IP-адрес</i> <i>маска</i> | <i>IP-метод-аутентификации</i> |
| <i>hostssl</i> | <i>база</i> | <i>пользователь</i> | <i>IP-адрес</i> <i>маска</i> | <i>IP-метод-аутентификации</i> |
| <i>hostnssl</i> | <i>база</i> | <i>пользователь</i> | <i>IP-адрес</i> <i>маска</i> | <i>IP-метод-аутентификации</i> |

Значение полей из файла `pg_hba.conf` представлены в Приложении 1;

в) перезагрузить сервис СУБД «Jatoba» в:

– ОС Windows Server при помощи команд:

```
net stop JatobaServer;  
net start JatobaServer
```

– ОС семейства GNU/Linux при помощи команды:

```
systemctl restart jatoba-4
```

6.1.2. Настройка парольной политики

Существует два основных метода формирования парольной политики. Первый метод – это использование парольной политики по умолчанию. Второй метод – это формирование новой схемы «securityprofile».



Необходимо обратить внимание, что целесообразнее формировать парольную политику до создания учетных записей пользователей

Установка компонента SecurityProfile описана в документе «Защищенная система управления базами данных «Jatoba». Руководство по установке».

Использовать следующие функциональные возможности компонента SecurityProfile может привилегированный пользователь или пользователь имеющий право доступа к схеме «securityprofile»:

– смена пароля пользователя;

| | | |
|--------------------|--------------------------|--------------------------|
| № изменения: _____ | Подпись отв. лица: _____ | Дата внесения изм: _____ |
|--------------------|--------------------------|--------------------------|

- снятие блокировки пользователя;
- создание профиля парольной политики;
- назначение пользователю профиля парольной политики;
- смена параметров профиля парольной политики и т.д.

6.1.2.1 Параметры парольной политики по умолчанию

Парольная политика по умолчанию применяется активацией компонента SecurityProfile.

Для активации модуля в СУБД «Jatoba» необходимо выполнить следующие действия:

- от учетной записи администратора СУБД подключиться к ОС и открыть файл `postgresql.conf`²⁾;
- в файле `postgresql.conf` прописать следующую строку:

```
shared_preload_libraries = 'securityprofile'
```



Указание в конфигурационном файле `postgresql.conf` опции `shared_preload_libraries = 'securityprofile'` активирует компонент управления парольными политиками и создается политика по умолчанию с именем «default».

- в файле `postgresql.conf` прописать следующую строку:

```
securityprofile.db_name = 'dbname'
```

Параметр «dbname» определяет имя БД, в которой будет создаваться или уже создано расширение `securityprofile`, значение по умолчанию `postgres`.



Служебный фоновый процесс «`securityprofile_bgworker_main`» выполняет синхронизацию автоматически в БД, которая указана в параметре «`securityprofile.db_name`».

²⁾ Местонахождение файла `postgresql.conf` по умолчанию в:

- ОС семейства GNU/Linux: `/var/lib/jatoba/4/data/postgresql.conf`;
- ОС Windows Server: `C:\Program Files\GIS\Jatoba\4\data\postgresql.conf`.

г) в файле `postgresql.conf` прописать параметры парольной политики, приведенные в таблице 6.1;



В случае, когда параметры парольной политики не будут прописаны в файле `postgresql.conf`, они будут применяться автоматически по умолчанию

Таблица 6.1 – Параметры профиля «default»

| Параметр | Примечание | Параметры в профиле по умолчанию | Мин-е значение | Макс-е значение |
|--|--|--|----------------|-----------------|
| Параметры для конфигурирования парольной политики | | | | |
| <code>securityprofile.profile_name</code> | имя профиля по умолчанию | 'default' | | |
| <code>securityprofile.special_chars</code> | пароль должен содержать указанные символы (набор символов не является обязательным и может быть изменен) | <code>\!"#\$%&()*+,-./:;<=>?@[!^_`{}~</code> | | |
| <code>securityprofile.lower_case_count</code> | пароль должен содержать как минимум 1 символ в нижнем регистре | 1 | 0 | 256 |
| <code>securityprofile.upper_case_count</code> | пароль должен содержать как минимум 1 символ в верхнем регистре | 1 | 0 | 256 |
| <code>securityprofile.numbers_count</code> | пароль должен содержать как минимум 1 цифру | 1 | 0 | 256 |
| <code>securityprofile.special_count</code> | пароль должен содержать как минимум 1 спец. символ из заданного набора <code>special_chars</code> | 1 | 0 | 256 |
| <code>securityprofile.minimum_length</code> | минимальная длина пароля равна 6 символам | 6 | 6 | 256 |
| <code>securityprofile.maximum_length</code> | максимальная длина пароля равна 32 символам | 32 | 6 | 256 |
| <code>securityprofile.minimum_changes</code> | минимальное количество изменений, которое должен содержать новый пароль по сравнению с предыдущим | 0 | 0 | 256 |
| <code>securityprofile.failed_login_attempts</code> | количество неудачных попыток входа в СУБД | 10 | 0 | Int_Max |

| | | |
|--------------------|--------------------------|--------------------------|
| № изменения: _____ | Подпись отв. лица: _____ | Дата внесения изм: _____ |
|--------------------|--------------------------|--------------------------|

| Параметр | Примечание | Параметры в профиле по умолчанию | Мин-е значение | Макс-е значение |
|--|--|----------------------------------|----------------|-----------------|
| securityprofile.password_lock_time | время, на которое блокируется пользователь в СУБД (1 час в секундах) | 3600 | -1 | Int_Max |
| securityprofile.failed_login_attempts_max_time_sec | время в течении которого допустимо ошибиться | 0 | 0 | Int_Max |
| securityprofile.password_min_life_time | время в секундах, в течение которого пароль должен использоваться и не может быть изменен | 0 | 0 | Int_Max |
| securityprofile.password_life_time | время в секундах, в течение которого может быть использован текущий пароль (180 дней в секундах) | 15 552 000 | -1 | Int_Max |
| securityprofile.password_grace_time | время в секундах, в течение которого пользователь может использовать текущий пароль с напоминанием о необходимости его сменить до блокировки аккаунта. Время прибавляется к времени, установленному в securityprofile.password_life_time | 0 | -1 | Int_Max |
| securityprofile.password_reuse_time | время между повторным использованием одного и того же пароля (в секундах) | 0 | -1 | Int_Max |
| securityprofile.password_reuse_max | повторное использование пароля запрещено (Для повторного использования пароля без ограничений надо указать password_reuse_time=-1 и password_reuse_max = -1) | -1 | -1 | Int_Max |
| securityprofile.store_password_encrypted | хранение паролей в закрытом виде | True | True | False |

№ изменения: _____ Подпись отв. лица: _____ Дата внесения изм: _____

| Параметр | Примечание | Параметры в профиле по умолчанию | Мин-е значение | Макс-е значение |
|---|---|----------------------------------|----------------|-----------------|
| Параметры для конфигурирования размера кэша расширения | | | | |
| securityprofile.profiles_cache_limit | максимальное количество профилей, хранимых в кэше | 10 | 0 | Int_Max |
| securityprofile.accounts_cache_limit | максимальное количество пользовательских аккаунтов, хранимых в кэше | 1000 | 0 | Int_Max |
| securityprofile.password_history_cache_limit | максимальное количество парольных хэшей (md5) хранимых в кэше | 10000 | 0 | Int_Max |

В таблице 6.1 указываемые параметры после знака «=» не являются абсолютными. Они могут быть изменены в диапазоне от минимального до максимального значения в соответствии с требованиями парольной политики. Значение «INT_MAX» обозначает числовое значение для переменной «INT» равным значению 2 147 483 647.

Значение «-1» означает запрет или блокировку.

По умолчанию все создаваемые пользователи будут привязаны к профилю «default».

д) перезагрузить сервис СУБД «Jatoba» в:

– ОС Windows Server:

```
net stop JatobaServer;
net start JatobaServer
```

– ОС семейства GNU/Linux:

```
systemctl restart jatoba-4
```

е) подключиться к СУБД «Jatoba» от учетной записи администратора СУБД и затем выполнить следующую команду:

```
create extension securityprofile;
```

| | | |
|--------------------|--------------------------|--------------------------|
| № изменения: _____ | Подпись отв. лица: _____ | Дата внесения изм: _____ |
|--------------------|--------------------------|--------------------------|



Использование по умолчанию данного метода управления параметрами парольной политики будет доступно только через конфигурационный файл `postgresql.conf`

6.1.2.2 Обязательные действия, выполняемые сразу после установки расширения

Для учетной записи администратора СУБД, в обязательном порядке, требуется задать новый пароль сразу после выполнения команды установки расширения.

В тех случаях, когда учетная запись пользователя в СУБД была создана по умолчанию до применения парольной политики, необходимо изменить пароль учетной записи при помощи команды:

```
alter role <имя учетной записи пользователя> password '<пароль пользователя>';
```

После чего учетная запись пользователя привяжется к профилю «default».

Создание ролей пользователей при активированной парольной политике описано в п. 6.2.3.

6.1.2.3 Встроенные профили парольных политик

Компонент «securityprofile» имеет функциональную возможность распределять учетные записи по применяемым к ним парольным политикам. Как было описано ранее, возможно применять парольные политики по умолчанию, создавать собственные, либо использовать преднастроенные профили парольных политик.

К преднастроенным относятся:

- `FSTEC_1_class` – профиль для ИС первого класса защищенности (Таблица 6.2);
- `FSTEC_2_class` – профиль для ИС второго класса защищенности (Таблица 6.3);
- `CIS` – профиль, основанный на рекомендациях Center for Internet Security (Таблица 6.4);
- `Corporate_1` – корпоративный профиль первого уровня для учетных записей пользователей (Таблица 6.5);

– Corporate_2 – корпоративный профиль второго уровня для учетных записей администраторов программных (программно-аппаратных средств) (Таблица 6.6);

– 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 (Таблица 6.7).

Параметры в профиле установлены в зависимости от требований и могут быть изменены в сторону уменьшения до минимальных значений, как в профиле по умолчанию (default) (см. таблицу 6.1), так и в сторону увеличения до максимальных значений.

Максимальные значения обозначены параметром «INT_MAX». Это обозначение максимального значения для переменной «INT». При установке параметра максимального значения «INT_MAX» допускается числовое значение, которое меньше или равно 2 147 483 647.

Параметры в профилях парольных политик сформированы исходя из принципа «разумной достаточности» и установлены по минимальным значениям от требуемых, либо усредненные.

Например

Рассмотрим реализацию части требований к усилению ИАФ.4 (1г) в соответствии с документом "Методический документ. Меры защиты информации в государственных информационных системах" (утв. ФСТЭК России 11.02.2014):

г) длина пароля не менее восьми символов, алфавит пароля не менее 70 символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 4 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 15 до 60 минут, смена паролей не более чем через 60 дней.

Длина пароля не менее восьми символов.

Требование выполняется параметром «securityprofile.minimum_length» со значением равным 8, что соответствует требованиям и менять его в меньшую сторону нельзя.

| | | |
|--------------------|--------------------------|--------------------------|
| № изменения: _____ | Подпись отв. лица: _____ | Дата внесения изм: _____ |
|--------------------|--------------------------|--------------------------|

Максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 4 попыток.

Требование выполняется параметром «securityprofile.failed_login_attempts» с значением равным 4, что соответствует максимальному значению и параметр может быть изменен, только до значения равному 3.

Блокировка учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 15 до 60 минут.

Требование выполняется параметром «securityprofile.password_lock_time» с установленным значением 2700 сек, что равняется 45 минутам. Значение равно усредненному значению. В этом случае значение параметра «securityprofile.password_lock_time» могут быть изменены в диапазоне:

- от 15 минут (900 сек.);
- до 60 минут (3 600 сек.).

6.1.2.3.1 FSTEC_1_class

Профиль парольной политики «FSTEC_1_class» разработан в соответствии с требованиями к усилению ИАФ.4 (1г) в соответствии с документом "Методический документ. Меры защиты информации в государственных информационных системах" (утв. ФСТЭК России 11.02.2014) и может быть использован для ИС первого класса защищенности.

Таблица 6.2 – Параметры парольной политики FSTEC _1_Class по умолчанию

| Параметр | Примечание | Параметры в профиле | Макс-е значение |
|--|--|--|-----------------|
| Параметры для конфигурирования парольной политики | | | |
| securityprofile.profile_name | имя профиля по умолчанию | = ' FSTEC _1_Class ' | |
| securityprofile.special_chars | пароль должен содержать указанные символы (набор символов не является обязательным и может быть изменен) | \\!\"#\$%&()*+ , - ./:;<=>?@[\\^ _`{ }~ | |
| securityprofile.lower_case_count | пароль должен содержать как минимум 1 символ в нижнем регистре | 1 | 256 |

| | | |
|--------------------|--------------------------|--------------------------|
| № изменения: _____ | Подпись отв. лица: _____ | Дата внесения изм: _____ |
|--------------------|--------------------------|--------------------------|

| Параметр | Примечание | Параметры в профиле | Макс-е значение |
|--|--|---------------------|-----------------|
| securityprofile.upper_case_count | пароль должен содержать как минимум 1 символ в верхнем регистре | 1 | 256 |
| securityprofile.numbers_count | пароль должен содержать как минимум 1 цифру | 1 | 256 |
| securityprofile.special_count | пароль должен содержать как минимум 1 спец. символ из заданного набора special_chars | 1 | 256 |
| securityprofile.minimum_length | минимальная длина пароля | 8 | 256 |
| securityprofile.maximum_length | максимальная длина пароля | 256 | 256 |
| securityprofile.minimum_changes | минимальное количество изменений, которое должен содержать новый пароль по сравнению с предыдущим | 0 | 256 |
| securityprofile.failed_login_attempts | количество неудачных попыток входа в СУБД | 4 | Int_Max |
| securityprofile.password_lock_time | время, на которое блокируется пользователь при превышении количества неудачных попыток входа в СУБД (в секундах) | 2700 | Int_Max |
| securityprofile.failed_login_attempts_max_time_sec | время в течении которого допустимо ошибиться | 300 | Int_Max |
| securityprofile.password_min_life_time | время в секундах, в течение которого пароль должен использоваться и не может быть изменен | 0 | Int_Max |
| securityprofile.password_life_time | время в секундах, в течение которого может быть использован текущий пароль (в секундах) | 5184000 | Int_Max |
| securityprofile.password_grace_time | время в секундах, в течение которого пользователь может использовать текущий пароль с напоминанием о необходимости его сменить до блокировки аккаунта. Время прибавляется к времени, установленному в securityprofile.password_life_time | 0 | Int_Max |

| Параметр | Примечание | Параметры в профиле | Макс-е значение |
|--|---|---------------------|-----------------|
| securityprofile.password_reuse_time | время между повторным использованием одного и того же пароля (в секундах) | 0 | Int_Max |
| securityprofile.password_reuse_max | повторное использование пароля | -1 | Int_Max |
| securityprofile.store_password_encrypted | хранение паролей в закрытом виде | True | False |

6.1.2.3.2 FSTEC_2_class

Профиль парольной политики «FSTEC_1_class» разработан в соответствии с требованиями к усилению ИАФ.4 (1в) в соответствии с документом "Методический документ. Меры защиты информации в государственных информационных системах" (утв. ФСТЭК России 11.02.2014) и может быть использован для ИС второго класса защищенности.

Таблица 6.3 – Параметры парольной политики FSTEC_2_Class по умолчанию

| Параметр | Примечание | Параметры в профиле | Макс-е значение |
|--|--|--|-----------------|
| Параметры для конфигурирования парольной политики | | | |
| securityprofile.profile_name | имя профиля по умолчанию | ' FSTEC_2_Class ' | |
| securityprofile.special_chars | пароль должен содержать указанные символы (набор символов не является обязательным и может быть изменен) | \\!\"#\$%&()*+ ,- ./:;<=>?@[\\]^ _`{ }~ | |
| securityprofile.lower_case_count | пароль должен содержать как минимум 1 символ в нижнем регистре | 1 | 256 |
| securityprofile.upper_case_count | пароль должен содержать как минимум 1 символ в верхнем регистре | 1 | 256 |
| securityprofile.numbers_count1 | пароль должен содержать как минимум 1 цифру | 1 | 256 |
| securityprofile.special_count | пароль должен содержать как минимум 1 спец. символ из заданного набора special_chars | 1 | 256 |
| securityprofile.minimum_length | минимальная длина пароля | 8 | 256 |
| securityprofile.maximum_length | максимальная длина пароля | 256 | 256 |

| | | |
|--------------------|--------------------------|--------------------------|
| № изменения: _____ | Подпись отв. лица: _____ | Дата внесения изм: _____ |
|--------------------|--------------------------|--------------------------|

| Параметр | Примечание | Параметры в профиле | Макс-е значение |
|--|--|---------------------|-----------------|
| securityprofile.minimum_changes | минимальное количество изменений, которое должен содержать новый пароль по сравнению с предыдущим | 0 | 256 |
| securityprofile.failed_login_attempts | количество неудачных попыток входа в СУБД | 5 | Int_Max |
| securityprofile.password_lock_time | время, на которое блокируется пользователь при превышении количества неудачных попыток входа в СУБД (в секундах) | 1200 | Int_Max |
| securityprofile.failed_login_attempts_max_time_sec | время в течении которого допустимо ошибиться | 0 | Int_Max |
| securityprofile.password_min_life_time | время в секундах, в течение которого пароль должен использоваться и не может быть изменен | 0 | Int_Max |
| securityprofile.password_life_time | время в секундах, в течение которого может быть использован текущий пароль | 7776000 | Int_Max |
| securityprofile.password_grace_time | время в секундах, в течение которого пользователь может использовать текущий пароль с напоминанием о необходимости его сменить до блокировки аккаунта. Время прибавляется к времени, установленному в securityprofile.password_life_time | 0 | Int_Max |
| securityprofile.password_reuse_time | время между повторным использованием одного и того же пароля (в секундах) | 0 | Int_Max |
| securityprofile.password_reuse_max | повторное использование пароля | 1 | Int_Max |
| securityprofile.store_password_encrypted | хранение паролей в закрытом виде | True | False |

6.1.2.3.3 CIS

Профиль парольной политики «CIS», разработан на основе рекомендаций Center for Internet Security – Центра интернет-безопасности, являющегося некоммерческой организацией, которая разрабатывает собственные контрольные показатели и рекомендации.

Таблица 6.4 – Параметры парольной политики CIS по умолчанию

| Параметр | Примечание | Параметры в профиле | Макс-е значение |
|--|--|---|--------------------------|
| Параметры для конфигурирования парольной политики | | | |
| securityprofile.profile_name | имя профиля по умолчанию | 'CIS' | |
| securityprofile.special_chars | пароль должен содержать указанные символы | \\!\"#\$%&()*+ , - ./:;<=>?@[\\ _`{ }~ | |
| securityprofile.lower_case_count | пароль должен содержать как минимум 0 символов в нижнем регистре | 0 | 256 |
| securityprofile.upper_case_count | пароль должен содержать как минимум 0 символов в верхнем регистре | 0 | 256 |
| securityprofile.numbers_count | пароль должен содержать как минимум 1 цифру | 1 | 256 |
| securityprofile.special_count | пароль должен содержать как минимум 0 спец. символ из заданного набора special_chars | 0 | 256 |
| securityprofile.minimum_length | минимальная длина пароля | 14 | 256 |
| securityprofile.maximum_length | максимальная длина пароля | 256 | 256 |
| securityprofile.minimum_changes | минимальное количество изменений, которое должен содержать новый пароль по сравнению с предыдущим | 0 | 256 |
| securityprofile.failed_login_attempts | количество неудачных попыток входа в СУБД | 5 | Int_Max |
| securityprofile.password_lock_time | время, на которое блокируется пользователь при превышении количества неудачных попыток входа в СУБД (в секундах) | 900 | Int_Max |
| securityprofile.failed_login_attempts_max_time_sec | время в течении которого допустимо ошибиться | 0 | Int_Max |
| securityprofile.password_min_life_time | время в секундах, в течение которого пароль должен | 6400 | Int_Max |
| № изменения: _____ | | Подпись отв. лица: _____ | Дата внесения изм: _____ |

| Параметр | Примечание | Параметры в профиле | Макс-е значение |
|--|--|---------------------|-----------------|
| | использоваться и не может быть изменен | | |
| securityprofile.password_life_time | время в секундах, в течение которого может быть использован текущий пароль (в секундах) | 7776000 | Int_Max |
| securityprofile.password_grace_time | время в секундах, в течение которого пользователь может использовать текущий пароль с напоминанием о необходимости его сменить до блокировки аккаунта. Время прибавляется к времени, установленному в securityprofile.password_life_time | 0 | Int_Max |
| securityprofile.password_reuse_time | время между повторным использованием одного и того же пароля (в секундах) | 0 | Int_Max |
| securityprofile.password_reuse_max | повторное использование пароля | 5 | Int_Max |
| securityprofile.store_password_encrypted | хранение паролей в закрытом виде | True | False |

6.1.2.3.4 Corporate_1

Профиль парольной политики «Corporate_1» – корпоративный профиль первого уровня для учетных записей пользователей.

Таблица 6.5 – Параметры парольной политики Corporate_1

| Параметр | Примечание | Параметры в профиле | Макс-е значение |
|--|--|--|-----------------|
| Параметры для конфигурирования парольной политики | | | |
| securityprofile.profile_name | имя профиля по умолчанию | 'Corporate_1' | |
| securityprofile.special_chars | пароль должен содержать указанные символы | \!"#\$%&()*+ ,- ./:;<=>?@[]^ _`{ }~ | |
| securityprofile.lower_case_count | пароль должен содержать как минимум 1 символ в нижнем регистре | 1 | 256 |

| Параметр | Примечание | Параметры в профиле | Макс-е значение |
|--|--|---------------------|-----------------|
| securityprofile.upper_case_count | пароль должен содержать как минимум 1 символ в верхнем регистре | 1 | 256 |
| securityprofile.numbers_count | пароль должен содержать как минимум 2 цифры | 2 | 256 |
| securityprofile.special_count | пароль должен содержать как минимум 1 спец. символ из заданного набора special_chars | 1 | 256 |
| securityprofile.minimum_length | минимальная длина пароля | 6 | 256 |
| securityprofile.maximum_length | максимальная длина пароля | 256 | 256 |
| securityprofile.minimum_changes | минимальное количество изменений, которое должен содержать новый пароль по сравнению с предыдущим | 0 | 256 |
| securityprofile.failed_login_attempts | количество неудачных попыток входа в СУБД | 5 | Int_Max |
| securityprofile.password_lock_time | время, на которое блокируется пользователь при превышении количества неудачных попыток входа в СУБД | -1 | Int_Max |
| securityprofile.failed_login_attempts_max_time_sec | время в течении которого допустимо ошибиться | 0 | Int_Max |
| securityprofile.password_min_life_time | время в секундах, в течение которого пароль должен использоваться и не может быть изменен | 0 | Int_Max |
| securityprofile.password_life_time | время в секундах, в течение которого может быть использован текущий пароль (в секундах) | 3888000 | Int_Max |
| securityprofile.password_grace_time | время в секундах, в течение которого пользователь может использовать текущий пароль с напоминанием о необходимости его сменить до блокировки аккаунта. | 0 | Int_Max |
| securityprofile.password_reuse_time | время между повторным использованием одного и того же пароля (в секундах) | 0 | Int_Max |
| securityprofile.password_reuse_max | повторное использование пароля | 5 | Int_Max |

| | | |
|--------------------|--------------------------|--------------------------|
| № изменения: _____ | Подпись отв. лица: _____ | Дата внесения изм: _____ |
|--------------------|--------------------------|--------------------------|

| Параметр | Примечание | Параметры в профиле | Макс-е значение |
|--|----------------------------------|---------------------|-----------------|
| securityprofile.store_password_encrypted | хранение паролей в закрытом виде | True | False |

6.1.2.3.5 Corporate_2

Профиль парольной политики «Corporate_2» – корпоративный профиль второго уровня для учетных записей администраторов программных (программно-аппаратных средств).

Таблица 6.6 – Параметры парольной политики Corporate_2

| Параметр | Примечание | Параметры в профиле | Макс-е значение |
|--|---|---|-----------------|
| Параметры для конфигурирования парольной политики | | | |
| securityprofile.profile_name | имя профиля по умолчанию | 'Corporate_2' | |
| securityprofile.special | пароль должен содержать указанные символы | \\!\"#\$%&()*+ ,- ./:;<=>?@[\\^ _`{ }~ | |
| securityprofile.lower_case_count | пароль должен содержать как минимум 1 символ в нижнем регистре | 1 | 256 |
| securityprofile.upper_case_count | пароль должен содержать как минимум 1 символ в верхнем регистре | 1 | 256 |
| securityprofile.numbers_count | пароль должен содержать как минимум 2 цифры | 2 | 256 |
| securityprofile.special_count | пароль должен содержать как минимум 1 спец. символ из заданного набора special_chars | 1 | 256 |
| securityprofile.minimum_length | минимальная длина пароля | 12 | 256 |
| securityprofile.maximum_length | максимальная длина пароля | 256 | 256 |
| securityprofile.minimum_changes | минимальное количество изменений, которое должен содержать новый пароль по сравнению с предыдущим | 0 | 256 |
| securityprofile.failed_login_attempts | количество неудачных попыток входа в СУБД | 5 | Int_Max |
| securityprofile.password_lock_time | время, на которое блокируется пользователь при превышении количества неудачных попыток входа в СУБД | -1 | Int_Max |

| | | |
|--------------------|--------------------------|--------------------------|
| № изменения: _____ | Подпись отв. лица: _____ | Дата внесения изм: _____ |
|--------------------|--------------------------|--------------------------|

| Параметр | Примечание | Параметры в профиле | Макс-е значение |
|--|--|---------------------|-----------------|
| securityprofile.failed_login_attempts_max_time_sec | время в течении которого допустимо ошибиться | 0 | Int_Max |
| securityprofile.password_min_life_time | время в секундах, в течение которого пароль должен использоваться и не может быть изменен | 0 | Int_Max |
| securityprofile.password_life_time | время в секундах, в течение которого может быть использован текущий пароль (в секундах) | 7776000 | Int_Max |
| securityprofile.password_grace_time | время в секундах, в течение которого пользователь может использовать текущий пароль с напоминанием о необходимости его сменить до блокировки аккаунта. Время прибавляется к времени, установленному в securityprofile.password_life_time | 0 | Int_Max |
| securityprofile.password_reuse_time | время между повторным использованием одного и того же пароля (в секундах) | 0 | Int_Max |
| securityprofile.password_reuse_max | повторное использование пароля | 5 | Int_Max |
| securityprofile.store_password_encrypted | хранение паролей в закрытом виде | True | False |

6.1.2.3.6 Corporate_3

Профиль парольной политики «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.

Таблица 6.7 – Параметры парольной политики Corporate_3

| Параметр | Примечание | Параметры в профиле | Макс-е значение |
|--|---|--------------------------|-----------------|
| Параметры для конфигурирования парольной политики | | | |
| securityprofile.profile_name | имя профиля по умолчанию | 'Corporate_3' | |
| securityprofile.special | пароль должен содержать указанные символы | \\!\"#\$%&()*+ ,- | |
| № изменения: _____ | Подпись отв. лица: _____ | Дата внесения изм: _____ | |

| Параметр | Примечание | Параметры в профиле | Макс-е значение |
|--|---|-------------------------|-----------------|
| | | ./:;<=>?@[]^ _`{ }~ | |
| securityprofile.lower_case_count | пароль должен содержать как минимум 1 символов в нижнем регистре | 1 | 256 |
| securityprofile.upper_case_count | пароль должен содержать как минимум 1 символ в верхнем регистре | 1 | 256 |
| securityprofile.numbers_count | пароль должен содержать как минимум 2 цифры | 2 | 256 |
| securityprofile.special_count | пароль должен содержать как минимум 1 спец. символ из заданного набора special_chars | 1 | 256 |
| securityprofile.minimum_length | минимальная длина пароля | 16 | 256 |
| securityprofile.maximum_length | максимальная длина пароля | 256 | 256 |
| securityprofile.minimum_changes | минимальное количество изменений, которое должен содержать новый пароль по сравнению с предыдущим | 2 | 256 |
| securityprofile.failed_login_attempts | количество неудачных попыток входа в СУБД | 5 | Int_Max |
| securityprofile.password_lock_time | время, на которое блокируется пользователь при превышении количества неудачных попыток входа в СУБД | -1 | Int_Max |
| securityprofile.failed_login_attempts_max_time_sec | время в течении которого допустимо ошибиться | 0 | Int_Max |
| securityprofile.password_min_life_time | время в секундах, в течение которого пароль должен использоваться и не может быть изменен | 30 | Int_Max |
| securityprofile.password_life_time | время в секундах, в течение которого может быть использован текущий пароль (в секундах) | 7776000 | Int_Max |
| securityprofile.password_grace_time | время в секундах, в течение которого пользователь может использовать текущий пароль с напоминанием о необходимости его сменить до блокировки аккаунта. Время прибавляется к времени, установленному в | -1 | Int_Max |

№ изменения: _____ Подпись отв. лица: _____ Дата внесения изм: _____

| Параметр | Примечание | Параметры в профиле | Макс-е значение |
|--|---|---------------------|-----------------|
| | securityprofile.password_life_time | | |
| securityprofile.password_reuse_time | время между повторным использованием одного и того же пароля (в секундах) | 0 | Int_Max |
| securityprofile.password_reuse_max | повторное использование пароля | 5 | Int_Max |
| securityprofile.store_password_encrypted | хранение паролей в закрытом виде | True | False |

6.1.2.4 Взаимодействие параметров парольных политик

6.1.2.4.1 Время жизни пароля пользователя

Время жизни пароля пользователя состоит из трех параметров:

- максимальное время действия пароля (securityprofile.password_life_time);
- минимальное время действия пароля (securityprofile.password_min_life_time);
- льготный период действия пароля (securityprofile.password_grace_time).

На рисунке 6.1 показана схема взаимодействия временных параметров. На отрезке времени min_life_time пароль пользователя нельзя изменить.

Если временной параметр grace_time активен, то установленное в нем время прибавится к времени параметра life_time и после окончания суммарного срока действия пароля учетная запись пользователя будет заблокирована.

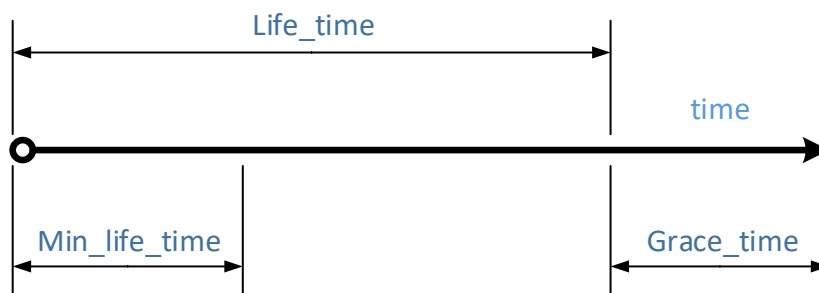


Рисунок 6.1 – Схема взаимодействия временных параметров

6.1.2.4.2 Количество изменений в пароле пользователя

Параметр securityprofile.minimum_changes определяет минимальное количество знаков, которыми должен отличаться новый пароль от предыдущего. Этот параметр

| | | |
|--------------------|--------------------------|--------------------------|
| № изменения: _____ | Подпись отв. лица: _____ | Дата внесения изм: _____ |
|--------------------|--------------------------|--------------------------|

взаимосвязан с параметром хранения паролей в закрытом виде securityprofile.store_password_encrypted. По умолчанию параметр securityprofile.store_password_encrypted имеет значение true, т.е. включен.

Если параметр равен false, то будет доступен параметр securityprofile.minimum_changes, при этом аутентификационная информация пользователей будет доступна только роли с атрибутом Superuser.

Повторное использование пароля пользователя осуществляется в несколько этапов, проверяется:

— история паролей; она проверяется вне зависимости от способа хранения аутентификационной информации, указанного в параметре securityprofile.store_password_encrypted;

— заданное время между использованием последнего пароля, указанного в параметре securityprofile.password_reuse_time; если параметр не задан, то проверка пропускается;

— заданный параметр разрешенного количества ранее использованных паролей, указанных в параметре securityprofile.password_reuse_max; если параметр не задан, то проверка пропускается.

Проверки проходят параллельно.

6.1.2.4.3 Повторное использование пароля пользователя

Политика в отношении повторного использования пароля может иметь следующие варианты:

- 1) разрешено установить ранее использованный пароль;
- 2) разрешено установить ранее использованный пароль через определенное время;
- 3) разрешено установить ранее использованный пароль определенное количество раз;
- 4) разрешено установить ранее использованный пароль определенное количество раз через определенное время;

5) запрещено установить ранее использованный пароль.

Параметр «securityprofile.password_reuse_time» (промежуток времени, который должен пройти между использованием одинаковых паролей) может принимать три типа значений:

- «-1» – бесконечный промежуток (повторно использовать пароль нельзя);
- «0» – промежуток отсутствует, можно ставить бывший в использовании пароль сразу;
- более «0», но не более максимального значения переменной INT_MAX.

Параметр «securityprofile.password_reuse_max» (минимальное количество смен пароля между использованием одинаковых паролей) может принимать следующие значения:

- «-1» – бесконечное количество (повторно использовать пароль нельзя);
- «0» – количество смен паролей равно нулю, т.е. разрешено использовать предыдущий пароль при текущей смене пароля;
- более «0», но не более максимального значения переменной INT_MAX.

Взаимодействие параметров представлено в матрице.

Таблица 6.8 – Матрица параметров

| Повторное использование пароля в течение времени (securityprofile.password_reuse_time) | Количество ранее использованных паролей (securityprofile.password_reuse_max) | | |
|--|--|---------------|---|
| | Запрещено (-1) | Разрешено (0) | Кол-во паролей больше указанного значения |
| Запрещено (-1) | Запрещено | Запрещено | Запрещено |
| Разрешено (0) | Запрещено | Разрешено | Разрешено |
| Период времени (более 0) | Запрещено | Разрешено | Разрешено |

Таким образом, для формирования одной из политик следует установить значения для параметров securityprofile.password_reuse_time и securityprofile.password_reuse_max приведенные в таблице 6.9.

Таблица 6.9 – Комбинации параметров значений политик повторного использования пароля

| № | Политика | Параметры | Значение |
|---|---|-------------------------------------|--------------------|
| 1 | Использование ранее использованного пароля запрещено | securityprofile.password_reuse_time | -1 |
| | | securityprofile.password_reuse_max | -1 |
| 2 | Использование ранее использованного пароля запрещено, вне зависимости от количества смен пароля | securityprofile.password_reuse_time | -1 |
| | | securityprofile.password_reuse_max | 0 (или более 0) |
| 3 | Использование ранее использованного пароля разрешено через определенное количество раз смены пароля | securityprofile.password_reuse_time | Более 0 |
| | | securityprofile.password_reuse_max | Более 0 |
| 4 | Использование ранее использованного пароля запрещено. Все пароли уникальные | securityprofile.password_reuse_time | 0 (или более 0) |
| | | securityprofile.password_reuse_max | -1 |
| 5 | Использование ранее использованного пароля разрешено | securityprofile.password_reuse_time | 0 |
| | | securityprofile.password_reuse_max | 0 |

6.1.2.4.4 Взаимодействие параметров парольных политик при реализации мер защиты информации ИАФ.4 (1г) и УПД.6 (1)

В компоненте SecurityProfile реализована часть требований ИАФ.4 (1г) и УПД.6 (1), описанных в документе «Методический документ. Меры защиты информации в государственных информационных системах» (утв. ФСТЭК России 11.02.2014):

В мере защиты информации ИАФ.4 (1г) пользователь блокируется после достижения установленного максимального количества неуспешных попыток аутентификации на период от 15 до 60 минут.

В мере защиты информации УПД.6 (1) пользователь блокируется после достижения установленного максимального количества неуспешных попыток аутентификации за установленный период времени до момента разблокирования его администратором.

Для реализации указанных мер используются параметры:

- securityprofile.failed_login_attempts – количество неуспешных попыток аутентификации;
- securityprofile.password_lock_time – время блокировки пользователя;

| | | |
|--------------------|--------------------------|--------------------------|
| № изменения: _____ | Подпись отв. лица: _____ | Дата внесения изм: _____ |
|--------------------|--------------------------|--------------------------|

- `securityprofile.failed_login_attempts_max_time_sec` – время, в течение которого допустимо ошибиться.

Ключевым моментом является соотношение временных параметров и количество попыток аутентификации пользователя в разрезе времени.

Далее рассматриваются примеры взаимодействия параметров SecurityProfile.

Пример № 1

Установлены параметры:

- `securityprofile.failed_login_attempts` = 5 – пять неудачных попыток аутентификации;
- `securityprofile.failed_login_attempts_max_time_sec` = 0 – время, в течение которого допустимо ошибиться, не установлено;
- `securityprofile.password_lock_time` = 3600 – время блокирования пользователя 1 час.

Пользователь проводит пять неудачных попыток аутентификации и по параметру `securityprofile.password_lock_time` = 3600 он блокируется на один час. По истечении времени пользователь может предпринять попытки аутентификации.

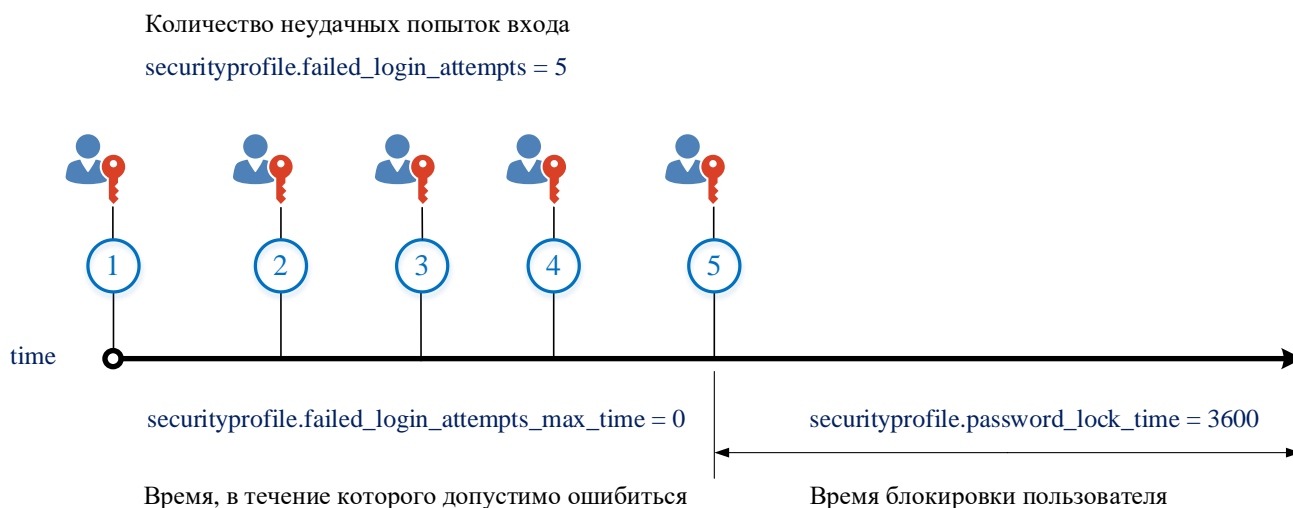


Рисунок 6.2 – Временная диаграмма примера № 1

Таким образом выполняется мера защиты информации ИАФ.4 (1г).

Пример № 2

Установлены параметры:

- `securityprofile.failed_login_attempts = 5` – пять неудачных попыток аутентификации;
- `securityprofile.failed_login_attempts_max_time_sec = 300` – время, в течение которого допустимо ошибиться, установлено 5 минут;
- `securityprofile.password_lock_time = 3600` – время блокирования пользователя 1 час.

Пользователь проводит пять неудачных попыток аутентификации в течение пяти минут. В этом случае параметр `password_lock_time` игнорируется, и пользователь блокируется до момента разблокирования его администратором.

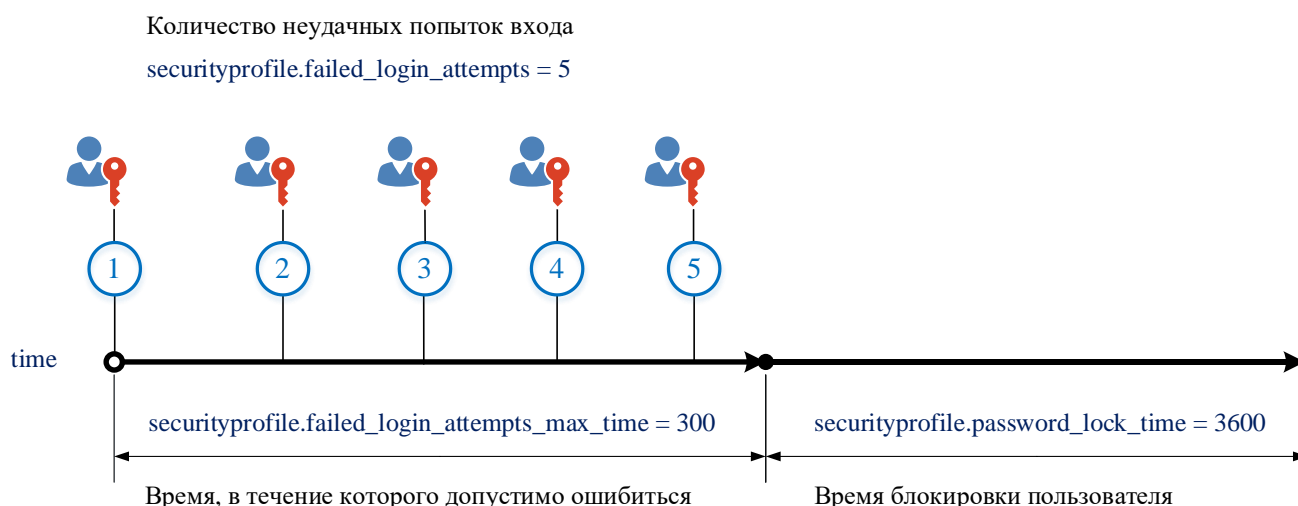


Рисунок 6.3 – Временная диаграмма примера № 2

Таким образом выполняется мера защиты информации УПД.6 (1).

Пример № 3

Установлены параметры:

- `securityprofile.failed_login_attempts = 5` – пять неудачных попыток аутентификации;
- `securityprofile.failed_login_attempts_max_time_sec = 300` – время, в течение которого допустимо ошибиться, установлено 5 минут;

- `securityprofile.password_lock_time = 3600` – время блокирования пользователя 1 час.

Пользователь проводит четыре неудачные попытки аутентификации, но пятая попытка аутентификации удачная и проходит после времени, в течение которого допустимо ошибиться. Пользователь не блокируется, т.к. не превышены установленные параметры.

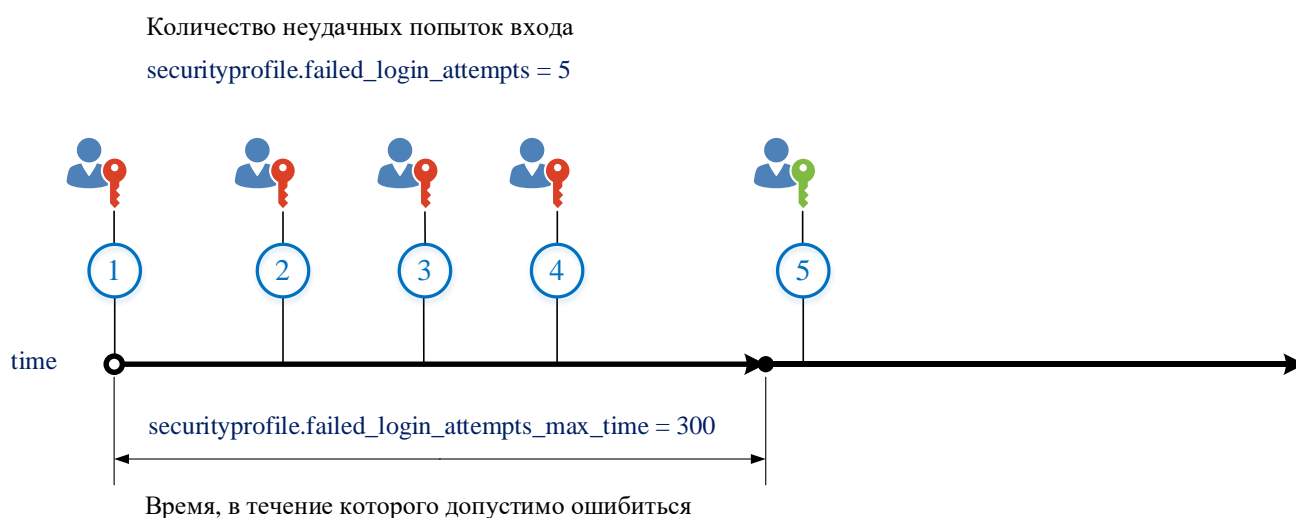


Рисунок 6.4 – Временная диаграмма примера № 3

Пример № 4

Установлены параметры:

- `securityprofile.failed_login_attempts = 5` – пять неудачных попыток аутентификации;
- `securityprofile.failed_login_attempts_max_time_sec = 300` – время, в течение которого допустимо ошибиться, установлено 5 минут;
- `securityprofile.password_lock_time = 3600` – время блокирования пользователя 1 час.

Пользователь проводит четыре неудачные попытки аутентификации. Пятая неудачная попытка происходит после истечения времени, установленного в параметре `securityprofile.failed_login_attempts_max_time_sec`, т.е. с момента первой неудачной аутентификации прошло более пяти минут.

Далее срабатывает параметр `securityprofile.password_lock_time` и пользователь блокируется на один час. Вмешательство администратора не потребуется, и пользователь

сможет предпринять попытки аутентификации через час с момента пятой неудачной попытки аутентификации.

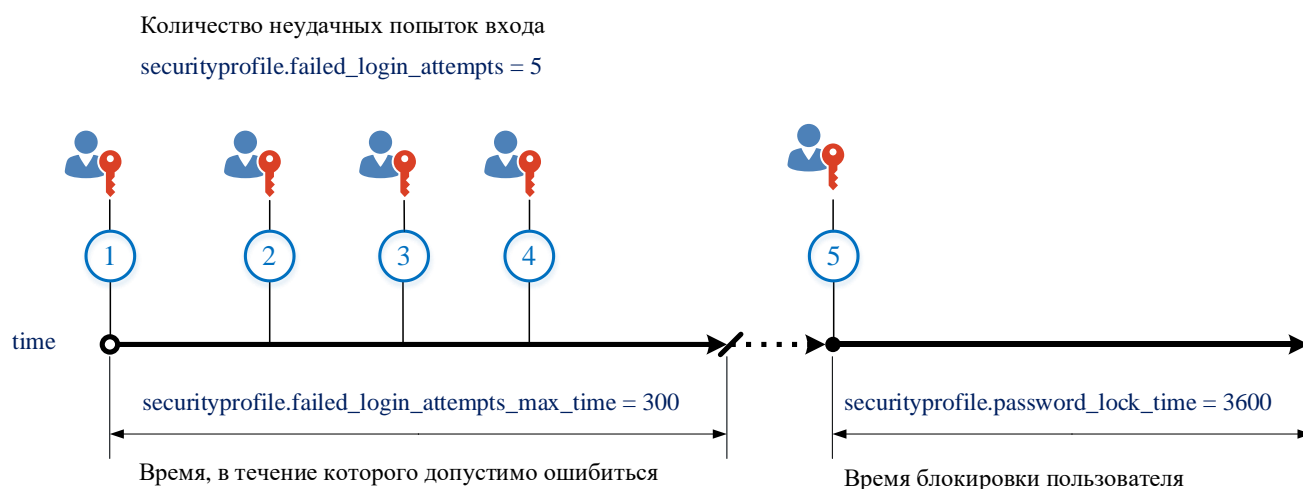


Рисунок 6.5 – Временная диаграмма примера № 4

Таким образом выполняется мера защиты информации ИАФ.4 (1г).

6.1.2.5 Параметры парольной политики по схеме securityprofile

Для активации парольной политики по схеме securityprofile в СУБД «Jatoba» необходимо выполнить следующие действия:

а) от учетной записи администратора СУБД подключиться к ОС и открыть файл postgresql.conf³⁾;

б) в файле postgresql.conf прописать следующую строку:

```
shared_preload_libraries = 'securityprofile'
```

в) перезагрузить сервис СУБД «Jatoba» в:

– ОС Windows Server при помощи команд:

```
net stop JatobaServer;  
net start JatobaServer
```

– ОС семейства GNU/Linux при помощи команды:

³⁾ Местонахождение файла postgresql.conf по умолчанию в:

– ОС семейства GNU/Linux: /var/lib/jatoba/4/data/postgresql.conf;

– ОС Windows Server: C:\Program Files\GIS\Jatoba\4\data\postgresql.conf.

```
systemctl restart jatoba-4
```

! Необходимо обратить внимание, что указание в конфигурационном файле postgresql.conf опции `shared_preload_libraries = 'securityprofile'` активируется компонент управления парольными политиками и создается политика по умолчанию с именем «default». Для создания новых политик выполняется п. г)

г) от учетной записи администратора СУБД подключиться к СУБД «Jatoba» и затем выполнить следующую команду:

```
create extension securityprofile;
```

После чего сформируется служебная схема `securityprofile` (см. рисунок 6.6)

! Для корректной работы компонента SecurityProfile допустима единственная установка расширения SecurityProfile для СУБД.

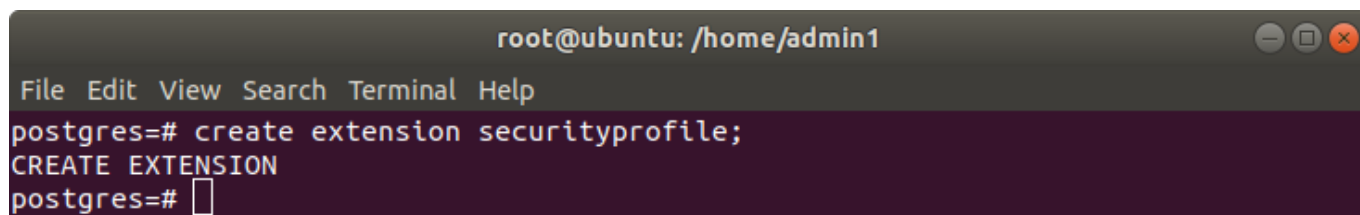


Рисунок 6.6 – Установка расширения 'securityprofile'

Будет создан профиль по умолчанию с именем «default».

В таблице 6.10 представлены команды управления параметрами служебной схемой в СУБД «Jatoba».

Таблица 6.10 – Команды управления параметрами профиля в СУБД «Jatoba»

| Команда | Примечание |
|---|--|
| Количество неуспешных попыток аутентификации | |
| <code>select set_profile_failed_login_attempts ('имя_профиля', bigint);</code> | Установка максимального количества неудачных попыток входа в СУБД. Если порог превышен, то применяется временная блокировка |
| <code>select set_profile_failed_login_attempts_max_time_seconds ('имя_профиля', bigint);</code> | Установка времени, в течение которого пользователь навсегда блокируется при достижении установленного максимального количества неуспешных попыток аутентификации |

№ изменения: _____ Подпись отв. лица: _____ Дата внесения изм: _____

| Команда | Примечание |
|--|--|
| select set_profile_password_lock_time ('имя_профиля', bigint); | Установка времени, на которое блокируется пользователь в днях, -1 - вечная блокировка |
| select set_profile_password_lock_time_seconds ('имя_профиля', bigint); | Установка времени, на которое блокируется пользователь в секундах |
| Время действия пароля | |
| select set_profile_password_min_life_time('имя_профиля', bigint); | Установка времени в днях, в течение которого пароль должен использоваться и не может быть изменен. |
| select set_profile_password_min_life_time_seconds ('имя_профиля', bigint); | Установка времени в секундах, в течение которого пароль должен использоваться и не может быть изменен |
| select set_profile_password_life_time('имя_профиля', bigint); | Установка времени в днях, в течение которого может быть использован текущий пароль (в днях). (-1 - вечность. Значение, указанное в опции VALID UNTIL при создании/смене пароля будет проигнорировано). |
| select set_profile_password_life_time_seconds ('имя_профиля', bigint); | Установка времени в секундах, в течение которого может быть использован текущий пароль. |
| select set_profile_password_grace_time ('имя_профиля', bigint); | Установка времени в днях, в течение которого пользователь может использовать текущий пароль с напоминанием о необходимости его сменить до блокировки аккаунта. (-1 - вечность. Аккаунт суперпользователя заблокирован не будет.) |
| select set_profile_password_grace_time_seconds ('имя_профиля', bigint); | Установка времени в секундах, в течение которого пользователь может использовать текущий пароль с напоминанием о необходимости его сменить до блокировки аккаунта. (-1 - вечность. Аккаунт суперпользователя заблокирован не будет.) |
| Повторное использование пароля | |
| select set_profile_password_reuse_time ('имя_профиля', bigint); | Установка времени в днях между повторным использованием одного и того же пароля. (-1 – вечность) |
| select set_profile_password_reuse_time_seconds ('имя_профиля', bigint); | Установка времени в секундах между повторным использованием одного и того же пароля. |
| select set_profile_password_reuse_max ('имя_профиля', integer); | Установка количества смен пароля перед возвращением к старому значению (Для повторного использования пароля без ограничений надо указать password_reuse_time=-1 и password_reuse_max = -1) |
| Характеристики пароля | |
| select set_profile_password_lower_case_count ('имя_профиля', integer); | Установка минимального количества символов в нижнем регистре, которые должен содержать пароль. (0 - наличие не обязательно) |

| Команда | Примечание |
|---|--|
| select set_profile_password_upper_case_count ('имя_профиля', integer); | Установка минимального количества символов в верхнем регистре, которые должен содержать пароль. (0 - наличие не обязательно) |
| set_profile_password_numbers_count ('имя_профиля', integer); | Установка параметра минимального количества цифр, которые должен содержать пароль (0 - наличие не обязательно) |
| select set_profile_password_special_chars ('имя_профиля', 'набор спец.символов'); | Параметр указывающий на перечень набора спец.символов, которые должны использоваться в пароле |
| select set_profile_password_special count ('имя_профиля', integer); | Установка параметра, при котором пароль должен содержать минимальное количество спецсимволов (0 - наличие не обязательно) |
| select set_profile_password_min_len ('имя_профиля', integer); | Установка минимальной длины пароля |
| select set_profile_password_max_len ('имя_профиля', integer); | Параметр устанавливающий максимальную длину пароля |
| select set_profile_password_min_changes ('имя_профиля', integer); | Параметр устанавливающий минимальное количество изменений, которое должен содержать новый пароль по сравнению с предыдущим. (Работает только при условии хранения истории паролей в открытом виде) |
| select set_profile_store_password_encrypted ('имя_профиля', boolean) – true | Параметр, устанавливающий хранение истории паролей в закрытом виде (в md5 хэшах), false - в открытом |

Кроме того, есть функциональная возможность создавать дополнительные схемы и привязывать к ним учетные записи пользователей.

В таблице 6.11 представлены команды управления профилем в СУБД «Jatoba».

Таблица 6.11 – Команды управления профилем в СУБД «Jatoba»

| Команда | Примечание |
|--|---------------------------------|
| select securityprofile.create_profile ('имя_нового_профиля'); | Создание нового профиля |
| select * from securityprofile.show_profiles; | Просмотр списка профилей |
| select securityprofile.drop_profile ('имя_нового_профиля'); | Удаление профиля |
| select securityprofile.bind_profile ('имя_профиля', 'имя_пользователя'); | Привязка пользователя к профилю |



Необходимо обратить внимание, что для применения схемы «securityprofile» к ранее созданным учетным записям, необходимо выполнить команду:

```
bind_profile ('имя_профиля', 'имя_пользователя')
```

Пример1. Создание профиля парольной политики

| | | |
|--------------------|--------------------------|--------------------------|
| № изменения: _____ | Подпись отв. лица: _____ | Дата внесения изм: _____ |
|--------------------|--------------------------|--------------------------|

Задание. Требуется создать дополнительный профиль парольной политики с именем «password_user», в котором будет установлена длина пароля пользователя равная 9 символам. При этом пользователь «test1» должен быть привязан к профилю «password_user».

Шаг 1. Создать профиль парольной политики с именем «password_user» на основании схемы «securityprofile», выполнив следующую команду:

```
select securityprofile.create_profile('password_user');
```

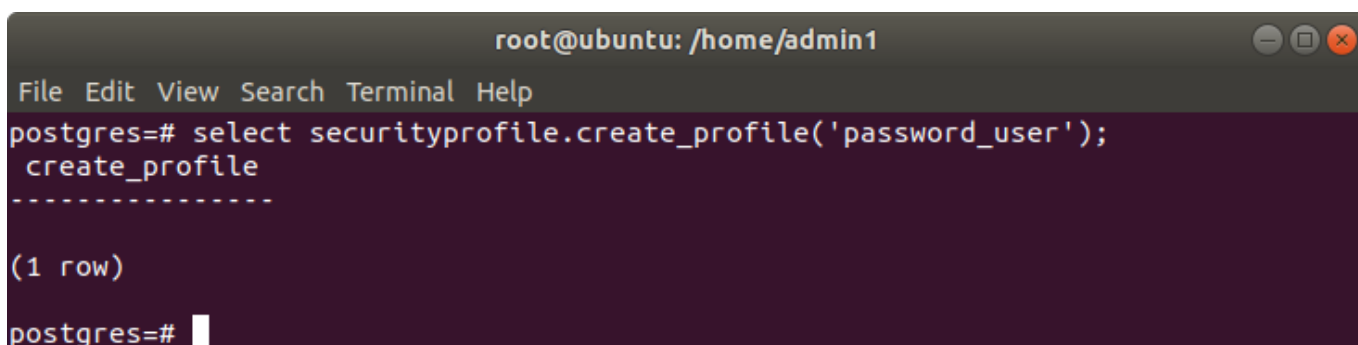


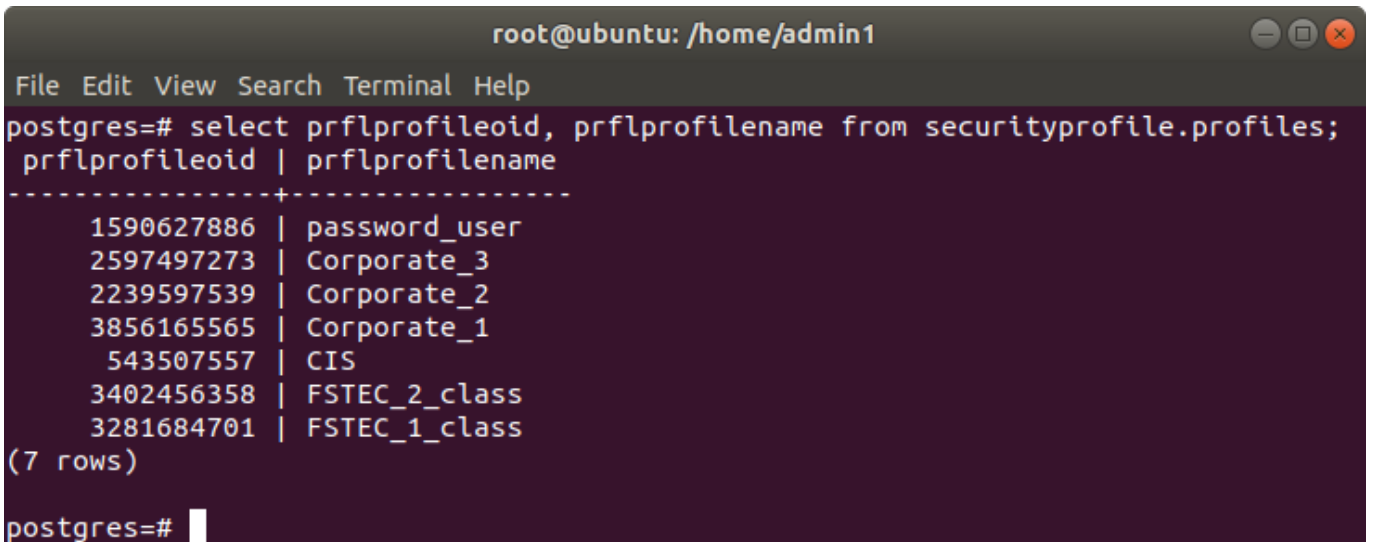
Рисунок 6.7 – Создание профиля «password_user»

Шаг 2. Просмотреть список имеющихся профилей, выполнив SQL-команду:

```
select * from securityprofile.show_profiles;
```

либо посмотреть несколько столбцов из таблицы «securityprofile.profiles», выполнив SQL-команду:

```
select prflprofileoid, prflprofilename from  
securityprofile.profiles;
```



```
root@ubuntu: /home/admin1
File Edit View Search Terminal Help
postgres=# select prflprofileoid, prflprofilename from securityprofile.profiles;
 prflprofileoid | prflprofilename
-----+-----
      1590627886 | password_user
      2597497273 | Corporate_3
      2239597539 | Corporate_2
      3856165565 | Corporate_1
       543507557 | CIS
      3402456358 | FSTEC_2_class
      3281684701 | FSTEC_1_class
(7 rows)

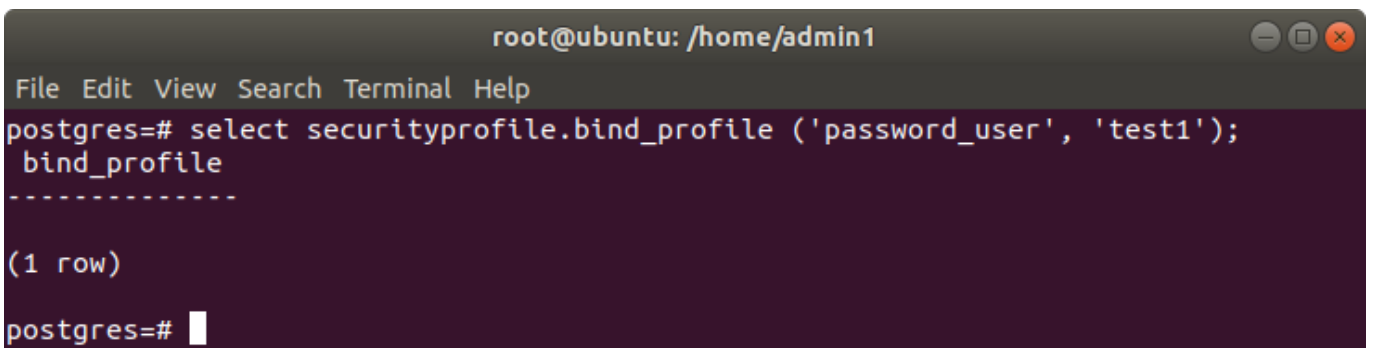
postgres=#
```

Рисунок 6.8 – Список профилей парольных политик

В результате видно, что новый профиль создан и унаследовал параметры парольной политики по умолчанию.

Шаг 3. Привязать пользователя «test1» к профилю «password_user», выполнив команду:

```
select securityprofile.bind_profile ('password_user', 'test1');
```



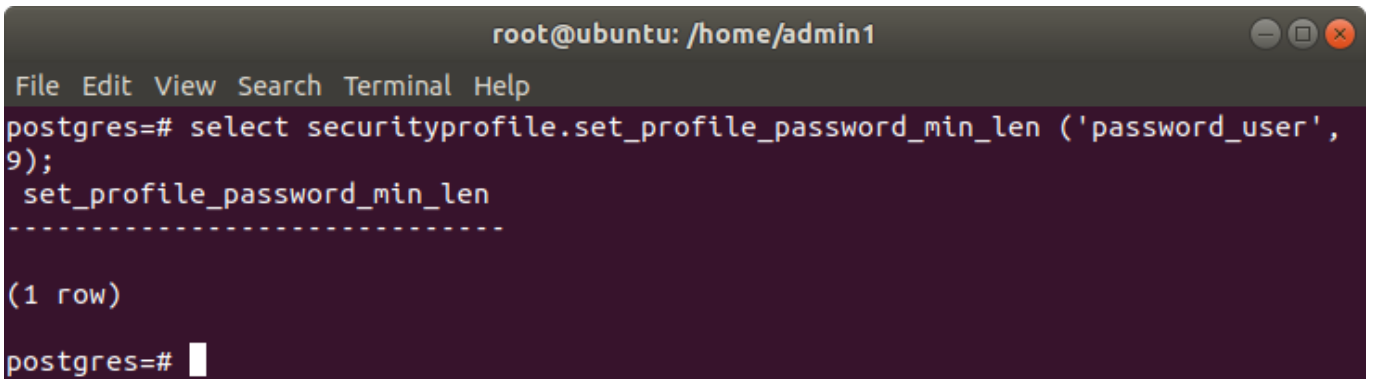
```
root@ubuntu: /home/admin1
File Edit View Search Terminal Help
postgres=# select securityprofile.bind_profile ('password_user', 'test1');
 bind_profile
-----
(1 row)

postgres=#
```

Рисунок 6.9 – Привязка пользователя к профилю

Шаг 4. Установить минимальную длину пароля пользователя равную 9 символам, выполнив команду:

```
select securityprofile.set_profile_password_min_len
('password_user', 9);
```



```
root@ubuntu: /home/admin1
File Edit View Search Terminal Help
postgres=# select securityprofile.set_profile_password_min_len ('password_user',
9);
 set_profile_password_min_len
-----
(1 row)
postgres=#
```

Рисунок 6.10 – Установка длины пароля в профиле «password_user»

На данном шаге требуемое задание выполнено.

6.1.2.6 Взаимодействие с компонентом управления кластером «ja_Dog»

Компонент «securityprofile» может использоваться с компонентом управления кластером «ja_Dog».

При таком использовании на резервном узле после выполнения репликации, в конфигурационный файл «postgresql.conf» необходимо добавить параметр:

```
securityprofile.sync_delay
```

со значением от «0» до «Int_Max».

Параметр задерживает синхронизацию кеша расширения.

Значение «0» соответствует отключению синхронизации кеша расширения.

Значения от «0» до «Int_Max» задают время в миллисекундах синхронизации кеша расширения. Такие значения должны быть целыми, положительными числами.

После установки параметра следует перезагрузить кластер.

При последующих ручных или автоматических сменах ролей узлов следует вручную на новом главном узле в конфигурационном файле закомментировать или удалить строку с добавленным параметром «securityprofile.sync_delay», а на резервном – добавить.

6.2. Управление доступом субъектов доступа к объектам доступа

6.2.1. Блокирование и разблокирование учетных записей

Для блокировки учетных записей пользователей необходимо администратору СУБД выполнить следующую команду:

```
select securityprofile.lock_account('имя_пользователя',  
bigint);
```

Примечание: bigint – задержка, с которой будет выполнена блокировка в днях.

select lock_account_seconds('имя_пользователя', bigint) – задержка, с которой будет выполнена блокировка в секундах.

Для разблокировки учетных записей пользователей администратору СУБД необходимо выполнить следующую команду:

```
select securityprofile.unlock_account ('имя_пользователя',  
bigint);
```

Примечание: bigint – задержка, с которой будет выполнено снятие блокировки в днях.

unlock_account_seconds ('имя_пользователя', bigint) – задержка, с которой будет выполнено снятие блокировки в секундах.

Для проверки факта блокировки и времени, в течение которого она будет действовать, администратору СУБД необходимо выполнить следующую команду:

```
select * from securityprofile.is_locked('имя_пользователя');
```

Вывод информации о всех пользователях выполняется SQL-командой:

```
select * from securityprofile.is_locked ('');
```

6.2.2. Создание новых ролей, присвоение атрибутов и системных привилегий

СУБД «Jatoba» поддерживает создание новых ролей (пользователей) с атрибутами ролей, приведенных в таблице 6.12. Для назначения атрибутов ролям необходимо выполнить следующую команду:

```
alter role <имя учетной записи пользователя> with <атрибут ролей из таблицы 6.12>;
```

Таблица 6.12 – Атрибуты ролей

| Атрибут | Условный перевод | Описание |
|-------------|----------------------------|---|
| SUPERUSER | Суперпользователь | Роль «Суперпользователь» обладает полными правами доступа к СУБД |
| INHERIT | Наследование | Роли, имеющие атрибут «INHERIT», автоматически используют права всех ролей, членами которых они являются, в том числе и унаследованные этими ролями права. |
| CREATEROLE | Право создание роли | Роль имеет разрешение на создание других ролей. Роль с правом «CREATEROLE» может не только создавать, но и изменять и удалять другие роли, а также выдавать и отзывать членство в ролях |
| CREATEDB | Право создания базы данных | Роль имеет разрешение на создание базы данных. |
| LOGIN | Право входа | Роль с атрибутом «LOGIN» рассматривается, как роль пользователя базы данных, а также может использоваться для начального подключения к базе данных. |
| REPLICATION | Право репликации | Роль имеет разрешение на запуск потоковой репликации. |
| BypassRls | | Атрибут роли, определяющий игнорирование все политики защиты на уровне строк (RLS – Row Level Security) |

СУБД «Jatoba» регулирует системные привилегии для ролей с атрибутом «Login» в соответствии с таблицей 6.13.

Таблица 6.13 – Системные привилегии для ролей с атрибутом «LOGIN»

| Наименование | Синтаксис предоставления разрешений роли на конкретные объекты | Описание |
|---------------------|--|---|
| SELECT LARGE OBJECT | GRANT { { SELECT UPDATE } [, ...] ALL [PRIVILEGES] } | Получение больших объектов |
| UPDATE LARGE OBJECT | ON LARGE OBJECT <идентификатор большого объекта> [, ...] TO { [GROUP] <название роли> PUBLIC } [, ...] [WITH GRANT OPTION] | Изменение данных в больших объектах |
| SELECT SEQUENCE | GRANT { { USAGE SELECT UPDATE } [, ...] ALL [PRIVILEGES] } | Получение значения последовательностей |
| UPDATE SEQUENCE | ON { SEQUENCE <название последовательности> [, ...] | Обновление значения последовательностей |
| USAGE SEQUENCE | | Использование последовательности |

№ изменения: _____ Подпись отв. лица: _____ Дата внесения изм: _____

| Наименование | Синтаксис предоставления разрешений роли на конкретные объекты | Описание |
|-------------------------|---|--|
| | ALL SEQUENCES IN SCHEMA <название схемы> [, ...] TO { [GROUP] <название роли> PUBLIC } [, ...] [WITH GRANT OPTION] | |
| TRIGGER TABLE | GRANT { { TRIGGER } [, ...] ALL [PRIVILEGES] } ON { [TABLE] <название таблицы> [, ...] ALL TABLES IN SCHEMA <название схемы> [, ...] } TO { [GROUP] <название роли> PUBLIC } [, ...] [WITH GRANT OPTION] | Установка триггеров на таблицы |
| REFERENCES TABLE | GRANT { { REFERENCES } [, ...] ALL [PRIVILEGES] } ON { [TABLE] <название таблицы> [, ...] ALL TABLES IN SCHEMA <название схемы> [, ...] } TO { [GROUP] <название роли> PUBLIC } [, ...] [WITH GRANT OPTION] | Использование зависимых таблиц |
| REFERENCES TABLE COLUMN | GRANT { { REFERENCES } (<название столбца> [, ...]) [, ...] ALL [PRIVILEGES] (<название столбца> [, ...]) } ON [TABLE] <название таблицы> [, ...] TO { [GROUP] <название роли> PUBLIC } [, ...] [WITH GRANT OPTION] | Использование колонок зависимых таблиц |
| CREATE DATABASE | GRANT { { CREATE CONNECT TEMPORARY } [, ...] ALL [PRIVILEGES] } | Создание базы данных |
| CONNECT DATABASE | ON DATABASE <название базы данных> [, ...] | Подключение к базе данных |
| TEMPORARY DATABASE | TO { [GROUP] <название роли> PUBLIC } [, ...] [WITH GRANT OPTION] | Использование временных баз данных |
| CREATE SCHEMA | GRANT { { CREATE USAGE } [, ...] ALL [PRIVILEGES] } | Создание схемы |
| USAGE SCHEMA | ON SCHEMA <название схемы> [, ...] TO { [GROUP] <<название роли> PUBLIC } [, ...] [WITH GRANT OPTION] | Использование схемы |
| CREATE TABLESPACE | GRANT { CREATE ALL [PRIVILEGES] } | Создание табличного пространства |

| Наименование | Синтаксис предоставления разрешений роли на конкретные объекты | Описание |
|----------------------------|--|---|
| | <p>ON TABLESPACE <название табличного пространства> [, ...]</p> <p>TO { [GROUP] <название роли> PUBLIC } [, ...]</p> <p>[WITH GRANT OPTION]</p> | |
| EXECUTE FUNCTION | <p>GRANT { EXECUTE ALL [PRIVILEGES] }</p> <p>ON { FUNCTION <название функции> ([[<режим аргумента>] [<название аргумента>] <тип данных аргументов функции> [, ...])) [, ...]</p> <p> ALL FUNCTIONS IN SCHEMA <название схемы> [, ...] }</p> <p>TO { [GROUP] <название роли> PUBLIC } [, ...]</p> <p>[WITH GRANT OPTION]</p> | Выполнение функций |
| USAGE DOMAIN | <p>GRANT { USAGE ALL [PRIVILEGES] }</p> <p>ON DOMAIN <название домена> [, ...]</p> <p>TO <название роли> [, ...] [WITH GRANT OPTION]</p> | Использование домена |
| USAGE FOREIGN DATA WRAPPER | <p>GRANT { USAGE ALL [PRIVILEGES] }</p> <p>ON FOREIGN DATA WRAPPER <название внешнего источника данных> [, ...]</p> <p>TO { [GROUP] <название роли> PUBLIC } [, ...]</p> <p>[WITH GRANT OPTION]</p> | Использование внешних источников данных |
| USAGE FOREIGN SERVER | <p>GRANT { USAGE ALL [PRIVILEGES] }</p> <p>ON FOREIGN SERVER <название сервера> [, ...]</p> <p>TO { [GROUP] <название роли> PUBLIC } [, ...]</p> <p>[WITH GRANT OPTION]</p> | Использование внешних серверов |
| USAGE LANGUAGE | <p>GRANT { USAGE ALL [PRIVILEGES] }</p> <p>ON LANGUAGE <название языка программирования> [, ...]</p> <p>TO { [GROUP] <название роли> PUBLIC } [, ...]</p> <p>[WITH GRANT OPTION]</p> | Использования языка программирования |
| USAGE TYPE | <p>GRANT { USAGE ALL [PRIVILEGES] }</p> <p>ON TYPE <название типа> [, ...]</p> <p>TO <название роли> [, ...] [WITH GRANT OPTION]</p> | Использование тип |

СУБД «Jatoba» поддерживает права субъекта доступа, указанные в таблице 6.14, к объектам доступа. Для предоставления привилегий необходимо использовать инструкции «GRANT».

Таблица 6.14 – Права субъекта доступа к объектам доступа

| Право | Синтаксис | Описание |
|--------|---|---|
| Select | <p>на таблицу: GRANT { { SELECT } [, ...] ALL [PRIVILEGES] } ON { [TABLE] <название таблицы> [, ...] ALL TABLES IN SCHEMA <название схемы> [, ...] } TO { [GROUP] <название роли> PUBLIC } [, ...] [WITH GRANT OPTION]</p> <p>на столбец: GRANT { { SELECT } [, ...] ALL [PRIVILEGES] } ON { [TABLE] <название таблицы> [, ...] ALL TABLES IN SCHEMA <название схемы> [, ...] } TO { [GROUP] <название роли> PUBLIC } [, ...] [WITH GRANT OPTION]</p> | <p>Позволяет читать содержание объекта, а также выполнять команду «SELECT» для любого столбца или перечисленных столбцов в заданной таблице, представлении или последовательности</p> |
| Insert | <p>GRANT { { INSERT } [, ...] ALL [PRIVILEGES] } ON { [TABLE] <название таблицы> [, ...] ALL TABLES IN SCHEMA <название схемы> [, ...] } TO { [GROUP] <название роли> PUBLIC } [, ...] [WITH GRANT OPTION]</p> | <p>Позволяет вставлять строки в заданную таблицу с помощью команды «Insert»</p> |
| Update | <p>на таблицу: GRANT { { UPDATE } [, ...] ALL [PRIVILEGES] } ON { [TABLE] <название таблицы> [, ...] ALL TABLES IN SCHEMA <название схемы> [, ...] } TO { [GROUP] <название роли> PUBLIC } [, ...] [WITH GRANT OPTION]</p> <p>на столбец: GRANT { { UPDATE } [, ...] ALL [PRIVILEGES] } ON { [TABLE] <название таблицы> [, ...] ALL TABLES IN SCHEMA <название схемы> [, ...] } TO { [GROUP] <название роли> PUBLIC } [, ...] [WITH GRANT OPTION]</p> | <p>Позволяет изменять с помощью команды «UPDATE» данные во всех либо только перечисленных столбцах в заданной таблице</p> |
| Delete | <p>GRANT { { DELETE } [, ...] ALL [PRIVILEGES] } ON { [TABLE] <название таблицы> [, ...] ALL TABLES IN SCHEMA <название схемы> [, ...] } TO { [GROUP] <название роли> PUBLIC } [, ...] [WITH GRANT OPTION]</p> | <p>Позволяет удалять строки из заданной таблицы с помощью команды «DELETE»</p> |

| Право | Синтаксис | Описание |
|----------|--|---|
| Truncate | GRANT { { TRUNCATE } [, ...] ALL [PRIVILEGES] } ON { [TABLE] <название таблицы> [, ...] ALL TABLES IN SCHEMA <название схемы> [, ...] } TO { [GROUP] <название роли> PUBLIC } [, ...] [WITH GRANT OPTION] | Позволяет опустошить заданную таблицу или набор таблиц с помощью команды «TRUNCATE» |

6.2.3. Создание ролей при активированной парольной политике

При активированной парольной политике, новые пользователи должны создаваться в два этапа. На первом этапе создается роль без пароля. На втором этапе устанавливается пароль. Пароль устанавливается при помощи команды:

```
alter role <имя учетной записи пользователя> password '<пароль пользователя>';
```

Смена пароля через команду «password» недоступна. СУБД «Jatoba» блокирует выполнение данной команды и предложит сменить пароль через команду «alter role».

```
admin1@ubuntu: ~
File Edit View Search Terminal Help
postgres@ubuntu:/home/admin1$ cd /usr/jatoba-4/bin/
postgres@ubuntu:/usr/jatoba-4/bin$ psql
psql (14.5)
Type "help" for help.

postgres=# \password
Enter new password for user "postgres":
Enter it again:
ERROR: Can not check password validity.
DETAIL: Password may be changed only by ALTER ROLE query.
postgres=#
```

Рисунок 6.11 – Ошибка установки пароля пользователя через команду «password»

6.3. Регистрация событий безопасности СУБД «Jatoba»

6.3.1. Настройки регистраций событий безопасности СУБД «Jatoba» под управлением ОС Windows Server

Функциональная возможность СУБД, а именно функция syslogcollector (внутренний механизм), позволяет отправлять события в хранилище ОС Windows Server.

Для настройки регистрации событий безопасности СУБД «Jatoba» необходимо выполнить ряд действий:

- а) от учетной записи администратора СУБД подключиться к ОС и открыть файл «postgresql.conf»⁴;
- б) в файле «postgresql.conf» прописать следующие параметры:

```
log_destination = 'eventlog'
logging_collector = on
log_connections = on
log_disconnections = on
log_statement = 'mod'
log_hostname = on
```

- в) перезагрузить СУБД «Jatoba» при помощи команды:

```
net stop JatobaServer
net start JatobaServer
```

Расшифровка параметров по регистрации событий СУБД «Jatoba», которая установлена в ОС Windows Server, представлены в таблице 6.15.

Таблица 6.15 – Расшифровка параметров по регистрации событий СУБД «Jatoba»

| Параметр | Описание |
|-------------------|--|
| log_destination | Данный параметр указывает на то, где будут храниться события СУБД «Jatoba» |
| logging_collector | Данный параметр позволяет включать сборщик журналов, который перенаправляет сообщения в файл журнала |
| log_connections | Включение данного параметра позволяет регистрировать все подключения к СУБД «Jatoba», включая неуспешные |

⁴ Местонахождение файла «postgresql.conf» в ОС Windows Server: C:\Program Files\GIS\Jatoba\4\data\postgresql.conf

| Параметр | Описание |
|--------------------|--|
| log_disconnections | Включение данного параметра позволяет регистрировать завершение сеанса |
| log_statement | Данный параметр управляет, тем какие SQL-команды будут регистрироваться. Параметр mod позволяет записывать следующие команды: все команды DDL (CREATE, ALTER, DROP), а так же INSERT, UPDATE, DELETE, TRUNCATE и COPY FROM. PREPARE, EXECUTE и EXPLAIN ANALYZE |
| log_hostname | Включение данного параметра позволяет регистрировать имя хоста |

6.3.2. Настройки регистрации событий безопасности СУБД «Jatoba» под управлением ОС семейства GNU/Linux

Функциональная возможность СУБД, а именно функция syslogcollector (внутренний механизм), позволяет отправлять события из папки в хранилище ОС семейства GNU/Linux.

Для настройки регистрации событий безопасности СУБД «Jatoba» необходимо выполнить ряд действий:

- а) от учетной записи администратора СУБД подключиться к ОС и открыть файл «postgresql.conf»⁵⁾;
- б) в файле «postgresql.conf» прописать следующие параметры:

```
log_destination = 'syslog'
syslog_facility = 'LOCAL2'
syslog_ident = 'jatoba'
log_timezone = 'Europe/Moscow'
log_connections = on
log_disconnections = on
log_statement = 'mod'
log_hostname = on
```

- в) перезагрузить СУБД «Jatoba» при помощи команды:

```
# systemctl start jatoba-4
```

⁵⁾ Местонахождение файла «postgresql.conf» в ОС семейства GNU/Linux: /var/lib/jatoba/4/data/postgresql.conf

Расшифровка параметров по регистрации событий СУБД «Jatoba», которая установлена в ОС семейства GNU/Linux, представлены в таблице 6.16.

Таблица 6.16 – Расшифровка параметров по регистрации событий СУБД «Jatoba»

| Параметр | Описание |
|--------------------|--|
| log_destination | Данный параметр указывает на то, где будут храниться события СУБД «Jatoba» |
| syslog_facility | Данный параметр используется при включенном при использовании syslog |
| syslog_ident | При использовании syslog данный параметр указывает имя программы, используемое для идентификации сообщений |
| log_timezone | Данный параметр указывает на часовой пояс, используемых для отметок времени, записываемых в журнале |
| log_connections | Включение данного параметра позволяет регистрировать все подключения к СУБД «Jatoba», включая неуспешные |
| log_disconnections | Включение данного параметра позволяет регистрировать завершения сеанс |
| log_statement | Данный параметр управляет, тем какие SQL-команды будут регистрироваться. Параметр mod позволяет записывать следующие команды: все команды DDL (CREATE, ALTER, DROP), а так же INSERT, UPDATE, DELETE, TRUNCATE и COPY FROM. PREPARE, EXECUTE и EXPLAIN ANALYZE |
| log_hostname | Включение данного параметра позволяет регистрировать имя хоста |

6.3.3. Настройка расширенной регистрации событий безопасности

Компонент «pgAudit» обеспечивает расширенное журналирование событий. Компонент выполнен в виде расширения СУБД.

Установка компонента описана в документе 643.72410666.00067-05 97 01 «Руководство по установке».

После установки компонента поле «error message» расширяется данными:

- тип записи события;
- № выражения;
- № подвыражения;
- класс события;
- SQL–операция;
- тип объекта БД;
- имя объекта БД;

- полный текст SQL–запроса (скрипта);
- параметры SQL–запроса (скрипта).

Структура полей событий безопасности меняется, как представлено в таблице 6.17.

Таблица 6.17 – Структура полей событий безопасности

| № | Стандартные поля событий безопасности | |
|--------------------------|---------------------------------------|--------------------------------------|
| | Поля событий безопасности с pgAudit | |
| 1 | Time stamp with milliseconds | Штамп времени с миллисекундами |
| 2 | Criticality | Критичность события |
| 3 | Class | Тип события |
| 4 | User name | Имя пользователя |
| 5 | Database name | Имя базы данных |
| 6 | Process ID | Идентификатор процесса |
| 7 | Client host | Клиентский узел |
| 8 | Port number | Номер порта |
| 9 | Session ID | Идентификатор сессии |
| 10 | Per-session line numbe | Номер строки каждой сессии |
| 11 | Command tag | Тег команды |
| 12 | Session start time | Время начала сессии |
| 13 | Virtual transaction ID | Виртуальный идентификатор транзакции |
| 14 | Regular transaction ID | Идентификатор транзакции |
| 15 | Error severity | Уровень важности ошибки |
| 16 | SQLSTATE code | Код ошибки SQLSTATE |
| 17 | Error message | Сообщение об ошибке |
| 17.1 | Audit_type | Тип записи события |
| 17.2 | Statement_id | № выражения |
| 17.3 | Substatement_id | № подвыражения |
| 17.4 | Class | класс события |
| 17.5 | Command | SQL–операция |
| 17.6 | Object_type | Тип объекта БД |
| 17.7 | Object_name | Имя объекта БД |
| 17.8 | Statement | Полный текст SQL–запроса (скрипта) |
| 17.9 | Parameter | Параметры SQL–запроса (скрипта) |
| № изменения: _____ | | |
| Подпись отв. лица: _____ | | Дата внесения изм: _____ |

| Стандартные поля событий безопасности | |
|---------------------------------------|---|
| Поля событий безопасности с pgAudit | |
| 18 | Error message detail Подробности к сообщению об ошибке |
| 19 | Hint Подсказка к сообщению об ошибке |
| 20 | Internal query that led to the error Внутренний запрос |
| 21 | Character count of the error position therein Номер символа внутреннего запроса, где произошла ошибка |
| 22 | Error context Контекст ошибки |
| 23 | User query that led to the error Запрос пользователя |
| 24 | Character count of the error position therein Номер символа в запросе пользователя |
| 25 | Location of the error in the PostgreSQL source code Расположение ошибки в исходном коде |

6.3.3.1 Установка расширения pgAudit

Для установки расширения pgAudit необходимо:

1) Открыть конфигурационный файл:

- в ОС Windows:

```
C:\Program Files\GIS\Jatoba\4\data\postgresql.conf
```

- в GNU Linux:

```
nano /var/lib/jatoba/4/data/postgresql.conf
```

2) Установить параметр в конфигурационном файле в postgresql.conf:

```
shared_preload_libraries = 'pgaudit'
```

3) Перезапустить СУБД «Jatoba»:

- в ОС Windows:

```
net stop JatobaServer
net start JatobaServer
```

- в GNU Linux:

```
systemctl restart jatoba-4
```


4) Войти в СУБД от имени и с правами пользователя «SUPERUSER», выполнить SQL-команду:

```
CREATE EXTENSION pgaudit;
```

5) Перезапустить СУБД:

- в ОС Windows:

```
net stop JatobaServer  
net start JatobaServer
```

- в GNU Linux:

```
systemctl restart jatoba-4
```

После чего установку расширения можно считать оконченной.

6.3.3.2 Функциональные возможности компонента pgAudit

Для корректной работы компонента потребуется, чтобы в конфигурационном файле был установлен параметр «log_statement», как было выше описано в п. 6.3.1, 6.3.2.

pgaudit.log

Обязательно должен быть установлен параметр pgaudit.log. По умолчанию установлено значение «none». При помощи SQL-команды можно установить какие классы операторов будут регистрироваться в журнале событий.

Значения параметра могут быть следующими:

- READ – регистрируются SQL-команды SELECT, COPY в случае если источником является отношение или запрос;
- WRITE – регистрируются SQL-команды INSERT, UPDATE, DELETE, TRUNCATE, и COPY;
- FUNCTION – регистрируются функции CALLS и DO;
- ROLE – регистрируются SQL-команды относящиеся к ролям и системным привилегиям такие как, GRANT, REVOKE, CREATE/ALTER/DROP ROLE;
- DDL – регистрируются SQL-команды DDL не относящиеся к параметру ROLE;

| | | |
|--------------------|--------------------------|--------------------------|
| № изменения: _____ | Подпись отв. лица: _____ | Дата внесения изм: _____ |
|--------------------|--------------------------|--------------------------|

- MISC – регистрируются прочие команды SQL-команды, такие как DISCARD, FETCH, CHECKPOINT, VACUUM, SET;
- MISC_SET – регистрируются SQL-команды типа SET;
- ALL – регистрируются все перечисленные SQL-команды.

Сравнение регистрируемых SQL-команд при стандартной регистрации событий безопасности СУБД и с применением компонента pgAudit приведены в таблице 6.18.

Таблица 6.18 – Сравнительная таблица регистрируемых SQL-команд

| log_statement | | pg_Audit | |
|---------------|---------------------------------|----------|---|
| Параметр | SQL-команды записывать в журнал | Параметр | SQL-команды записывать в журнал |
| ALL | | ALL | |
| | | READ | SELECT COPY TO |
| MOD | INSERT | WRITE | INSERT |
| | UPDATE | | UPDATE |
| | DELETE | | DELETE |
| | TRUNCATE | | TRUNCATE |
| | COPY FROM | | COPY FROM |
| | PREPARE | | |
| | EXECUTE | | |
| | EXPLAIN ANALYZE | | |
| DDL | CREATE | DDL | CREATE |
| | ALTER | | ALTER |
| | DROP | | DROP |
| | | FUNCTION | CALL DO |
| | | ROLE | GRANT REVOKE ALTER DEFAULT PRIVILEGES SET ROLE |
| | | MISC | DISCARD FETCH CHECKPOINT VACUUM SET |
| | | MISC_SET | SET |
| NONE | | NONE | |

pgaudit.log_catalog

Указывает, что ведение журнала сеанса должно быть включено в случае, когда все отношения в операторе находятся в pg_catalog.

Значение по умолчанию – on.

pgaudit.log_client

Указывает, будут ли сообщения журнала видны клиентскому процессу, такому как psql. Обычно этот параметр следует оставлять отключенным, но он может быть полезен для отладки или других целей.

Значение по умолчанию – off.

pgaudit.log_level

Указывает уровень детализации журнала, который будет использоваться для записей журнала.

Уровни детализации журнала FATAL и PANIC запрещены.

Этот параметр используется для регрессионного тестирования, а также может быть полезен конечным пользователям для тестирования или других целей.

Значение по умолчанию – log.

pgaudit.log_parameter

Параметр указывает, что журнал аудита должен включать параметры, которые были переданы с оператором. При наличии параметров они будут включены в CSV формат после текста оператора.

Значение по умолчанию – off.

pgaudit.log_relation

Параметр указывает должны ли отражаться в журнале регистрации событий отдельные записи для каждого отношения (TABLE, VIEW, и т.д.), указанного в операторе SELECT или DML.

Значение по умолчанию – off.

pgaudit.log_rows

Параметр указывает, что журнал аудита должен включать строки, извлеченные или затронутые оператором. Если включено, поле строк будет включено после поля параметров.

Значение по умолчанию – off.

pgaudit.log_statement

Параметр указывает, будет ли протоколирование включать текст инструкции и параметры (если включено). В зависимости от требований журнал аудита может не требовать этого, и журналы становятся менее подробными.

Значение по умолчанию – on.

pgaudit.log_statement_once

Параметр указывает, будет ли протоколирование включать текст оператора и параметры с первой записью журнала для комбинации оператора/подоператора или с каждой записью. Отключение этого параметра приведет к менее подробному журналированию, но может затруднить определение инструкции, сгенерировавшей запись в журнале, хотя пары оператор/подоператор вместе с идентификатором процесса должно быть достаточно для идентификации текста оператора, зарегистрированного с предыдущей записью.

Значение по умолчанию – off.

pgaudit.role

Указывает основную роль, используемую для ведения журнала аудита объектов. Можно определить несколько ролей аудита, назначив их главной роли. Это позволяет нескольким группам отвечать за различные аспекты ведения журналов аудита.

По умолчанию роли нет.

Пример № 1. Создание записи журнала аудита для всех событий

Для создания записи журнала аудита для всех событий потребуется:

- 1) От имени и с правами пользователя «Superuser» авторизоваться в СУБД:

```
psql -U postgres
```

| | | |
|--------------------|--------------------------|--------------------------|
| № изменения: _____ | Подпись отв. лица: _____ | Дата внесения изм: _____ |
|--------------------|--------------------------|--------------------------|

- 2) Задать запись всех событий в журнал аудита, выполнив SQL-команду:

```
ALTER SYSTEM SET pgaudit.log = 'All';
```

- 3) Проверить заданный параметр записи всех событий:

```
SELECT name, setting FROM pg_settings WHERE name LIKE  
'pgaudit%';
```

Пример № 2. Создание записей аудита событий для определенной роли

Для создания записи журнала аудита для определенной роли потребуется:

- 1) От имени и с правами пользователя «Superuser» авторизоваться в СУБД:

```
psql -U postgres
```

- 2) Создать роль "auditor":

```
CREATE ROLE auditor;
```

- 3) Задать запись событий "Чтение" для роли "auditor":

```
ALTER ROLE auditor SET pgaudit.log = 'Read';
```

- 4) Проверить заданный параметр записи "Чтение" всех событий для роли "auditor":

```
select rolname, rolconfig from pg_roles;
```

- 5) Создать несколько команд в СУБД от роли "auditor":

```
CREATE TABLE Test (Id int NOT NULL, LastName varchar(255) NOT  
NULL, FirstName varchar(255), Age int, PRIMARY KEY (ID));  
INSERT INTO Test (Id, LastName, FirstName, Age) VALUES  
(1, 'Testov', 'Test', 123);  
SELECT * FROM test;
```

- 6) Создать несколько команд в СУБД от роли "postgres":

```
CREATE TABLE Test1 (Id int NOT NULL, LastName varchar(255) NOT  
NULL, FirstName varchar(255), Age int, PRIMARY KEY (ID));
```

```
INSERT INTO Test1 (Id, LastName, FirstName, Age) VALUES  
(1, 'Testov', 'Test', 123);  
SELECT * FROM test1;
```

- 7) Проверить созданные записи в логе аудита:

```
nano /var/lib/jatoba/4/data/log/jatoba-день_недели.log
```

Пример № 3. Создание записей аудита событий для определенной колонки в таблице

Для создания записи журнала аудита для определенной колонки в таблице потребуется:

- 1) От имени и с правами пользователя «Superuser» авторизоваться в СУБД

```
psql -U postgres
```

- 2) Создать роль "auditor":

```
CREATE ROLE auditor;
```

- 3) Добавить роль в таблицу "pgaudit"

```
set pgaudit.role = 'auditor';
```

- 4) Создать таблицу "Test":

```
CREATE TABLE Test (Id int NOT NULL, LastName varchar(255) NOT  
NULL, FirstName varchar(255), Age int, PRIMARY KEY (ID));
```

- 5) Добавить запись в таблицу:

```
INSERT INTO Test (Id, LastName, FirstName, Age) VALUES  
(1, 'Testov', 'Test', 123);
```

6) Задать запись событий только для выражения "UPDATE" для колонки "age" в таблице "Test" для пользователя "auditor":

```
GRANT update (age) ON Test TO auditor;
```

7) Выполнить команды:

```
UPDATE Test SET Age = 1234 WHERE Age = 123;  
UPDATE Test SET LastName = 'Booba' WHERE LastName = 'Testov';
```

8) Проверить созданные записи в логе аудита:

```
nano /var/lib/jatoba/4/data/log/jatoba-день_недели.log
```

Пример № 4. Создание записей аудита событий для определенной базы

1) От имени и с правами пользователя «Superuser» авторизоваться в СУБД:

```
psql -U postgres
```

2) Создать новую базу:

```
CREATE DATABASE test1;
```

3) Задать запись всех событий в журнал аудита для базы данных "test1":

```
ALTER DATABASE test1 SET pgaudit.log = 'All';
```

4) Выполнить команды:

```
CREATE TABLE Test (Id int NOT NULL, LastName varchar(255) NOT  
NULL, FirstName varchar(255), Age int, PRIMARY KEY (ID));  
INSERT INTO Test (Id, LastName, FirstName, Age) VALUES  
(1, 'Testov', 'Test', 123);  
SELECT * FROM test;
```

5) Подключиться к созданной базе:

```
\c test1
```

6) Создать несколько команд в СУБД:

```
CREATE TABLE Test1 (Id int NOT NULL, LastName varchar(255) NOT  
NULL, FirstName varchar(255), Age int, PRIMARY KEY (ID));  
INSERT INTO Test1 (Id, LastName, FirstName, Age) VALUES  
(1, 'Testov', 'Test', 123);  
SELECT * FROM test1;
```

7) Проверить созданные записи в логе аудита:

```
nano /var/lib/jatoba/4/data/log/jatoba-день_недели.log
```


7. РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ БАЗ ДАННЫХ

7.1. Выгрузка кластера баз данных СУБД «Jatoba» в формате скрипта

Выгрузка кластера всех баз данных СУБД «Jatoba» в формате скрипта осуществляется с помощью следующей команды:

```
pg_dumpall -f <каталог с базы данных>all.dump
```

Более подробную информацию о параметрах *pg_dumpall* можно узнать с помощью команды:

```
pg_dumpall --help
```

7.2. Выгрузка определенной базы данных СУБД «Jatoba» в формате скрипта в файл

Выгрузка определенной базы данных СУБД «Jatoba» в формате скрипта в файл осуществляется при помощи команды:

```
pg_dump -Fc <наименование базы данных> -f <каталог с базы данных><наименование базы данных>.dump
```

Более подробную информацию о параметритах *pg_dump* можно узнать с помощью команды:

```
pg_dump --help
```

7.3. Восстановление базы данных СУБД «Jatoba» из файла архива

Восстановление базы данных СУБД «Jatoba» из файла архива, созданного командой *pg_dump*, осуществляется с помощью команды:

```
pg_restore -d <наименование базы данных> <каталог с базы данных><наименование базы данных>.dump
```

Более подробную информацию о параметритах *pg_restore* можно узнать с помощью команды:

```
pg_restore --help
```

7.4. Создание резервной копии файлов СУБД «Jatoba»

Создание резервной копии файлов СУБД «Jatoba» осуществляется при помощи команды:

```
pg_basebackup -D <каталог, где будет храниться копия файлов из каталога «data» СУБД «Jatoba»>
```

Более подробную информацию о параметрах *pg_basebackup* можно узнать с помощью команды:

```
pg_basebackup --help
```

8. НАСТРОЙКА ОТКАЗОУСТОЙЧИВОГО КЛАСТЕРА СУБД «ЯТОВА»

8.1. Настройка отказоустойчивого кластера СУБД «Jatoba» на ОС Windows Server

До настройки отказоустойчивого кластера СУБД «Jatoba» на ОС Windows Server необходимо, чтобы были выполнены следующие условия/требования:

а) два сервера СУБД (физических или виртуальных машин) минимальные требования:

- 1xCPU 1,4GHz;
- RAM 6Gb;
- HDD 50Gb;
- 2xLAN 1Gbit;
- ОС Windows Server 2016.

б) серверы СУБД должны быть в домене.

Настройка производится от имени пользователя, обладающего правами локального администратора и администратора домена, необходимо создавать записи в DNS и ActiveDirectory.

в) два диска iSCSI-3, один минимум 600Мб (для диска кворума кластера Windows Server Failover Cluster (далее – WSFC)), второй в зависимости от предполагаемого размера БД.

г) серверы СУБД должны быть объединены WSFC.

Для настройки отказоустойчивого кластера СУБД «Jatoba» на ОС Windows Server 2016 необходимо выполнить следующие действия:

а) на каждом сервере в переменную среды Path добавить путь:

```
C:\Program Files\GIS\Jatoba\4\bin
```

б) на первом сервере СУБД:

– если отсутствует диск E то, через консоль диспетчера отказоустойчивости кластера, необходимо подключить диск E (см. рисунок 8.1) к первому серверу.

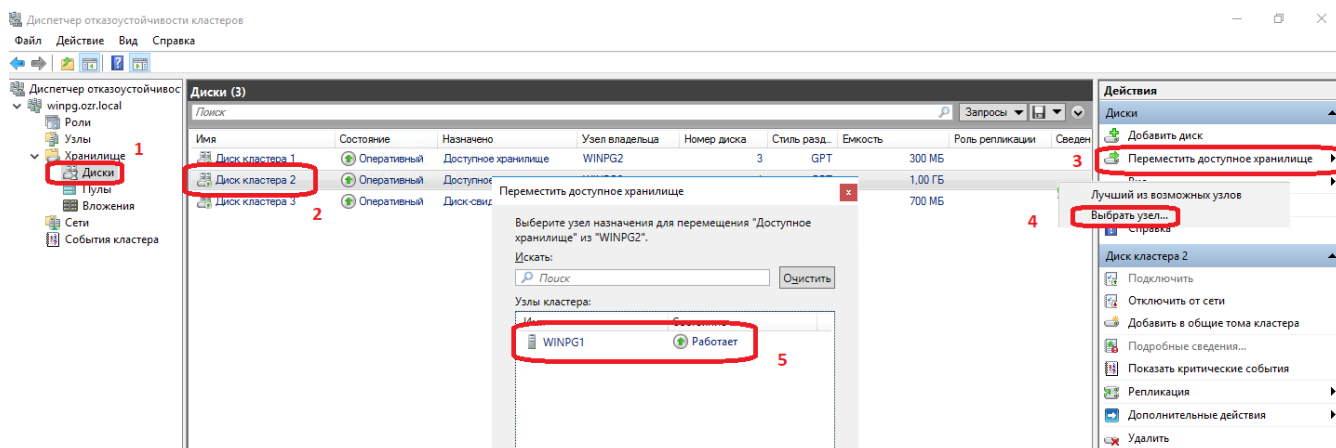


Рисунок 8.1 – Консоль диспетчера отказоустойчивости кластера. Подключение диска E

- создать на диске E каталог pgdata.
- запустить установку СУБД «Jatoba» из дистрибутива. Во время установки указать путь к БД e:\pgbase (см. рисунок 8.2), остальные параметры необходимо выбрать стандартно (пароль для пользователя postgres –должен быть доменный, локализация, порт и т.д.).

Data Directory

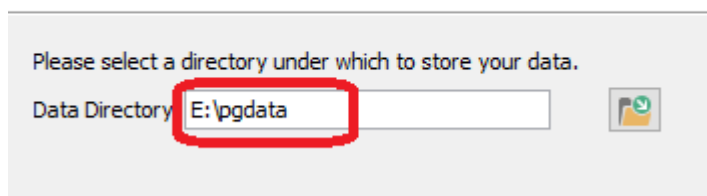


Рисунок 8.2 – Путь к БД

- остановить службу JatobaServer. Удалить содержимое каталога e:\pgdata.
- в) проделать данные шаги на втором сервере, пароль и порт указать точно такие, как на первом сервере, только без остановки службы и удаления содержимого каталога e:\pgdata.
- г) выдать необходимые доступы в файле e:\pgbase\ph_hba.conf.
- д) в файле e:\pgbase\ppstgresql.conf изменить параметр:

```
listen_addresses = '*'
```

- е) перезапустить службу JatobaServer.

ж) добавить роль универсальной службы. Эта роль позволяет автоматически переключать БД на другой сервер, в случае отказа первого;

з) запустить диспетчер отказоустойчивого кластера. Добавить необходимую роль, как показано на рисунке 8.3;

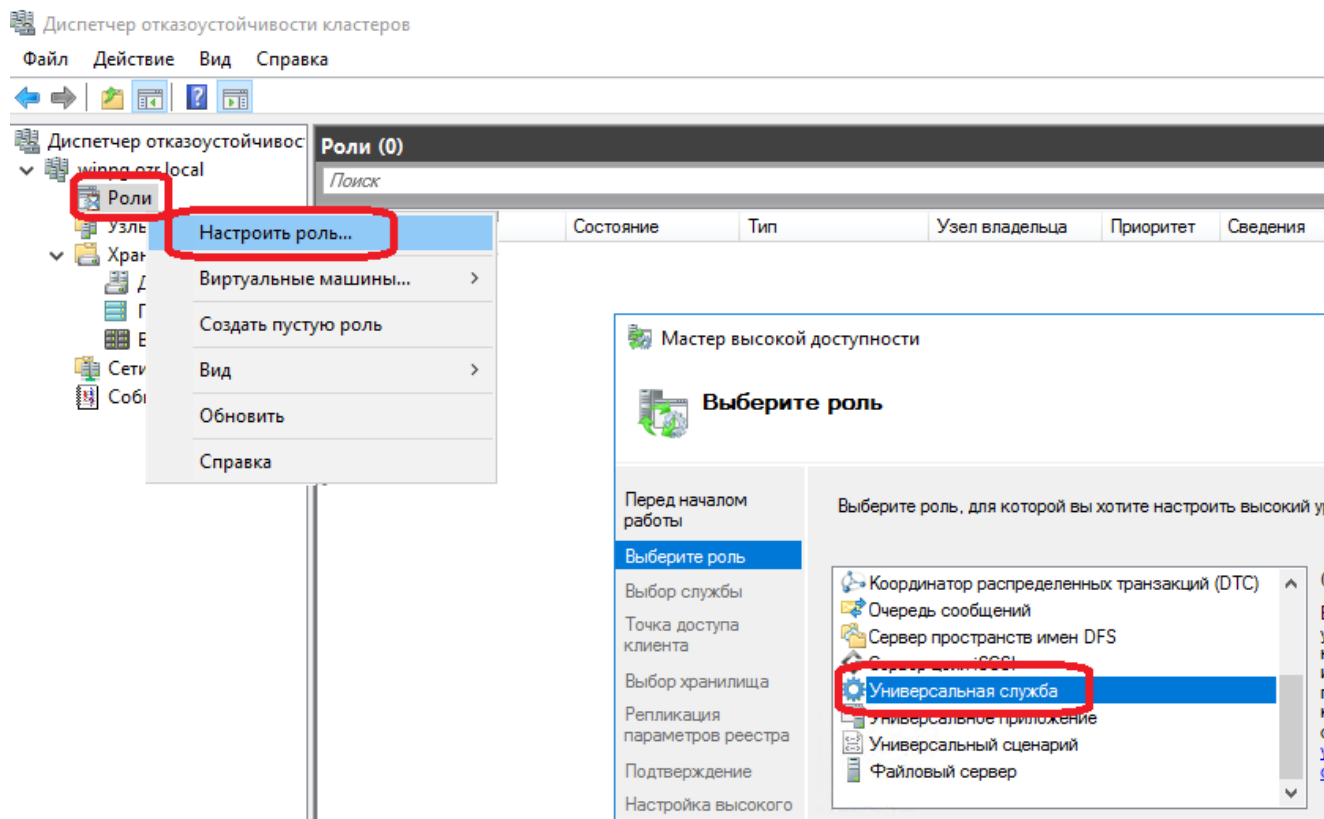


Рисунок 8.3– Добавление роли

и) нажать на кнопку далее и выбрать службу JatobaServer, как показано на рисунке 8.4;

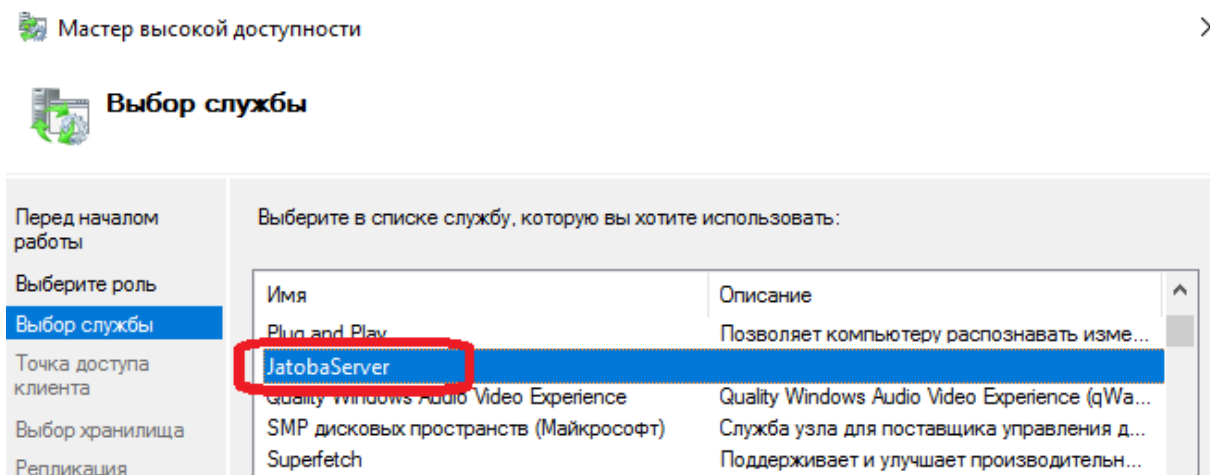


Рисунок 8.4 – Выбор службы JatobaServer

к) нажать кнопку «Далее» и затем выбрать имя и IP-адреса точки подключения к СУБД «Jatoba» (см. пример на рисунке 8.5);

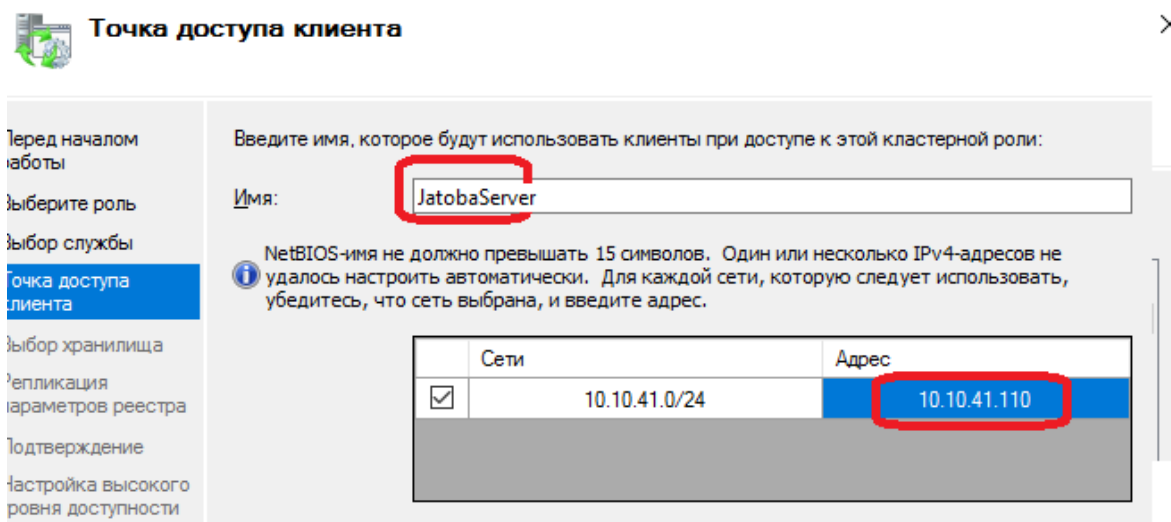


Рисунок 8.5 – Выбор имя и IP-адреса точки подключения к Jatoba

л) нажать «Далее» и выбрать хранилище, на рисунке 8.6 – диск E.

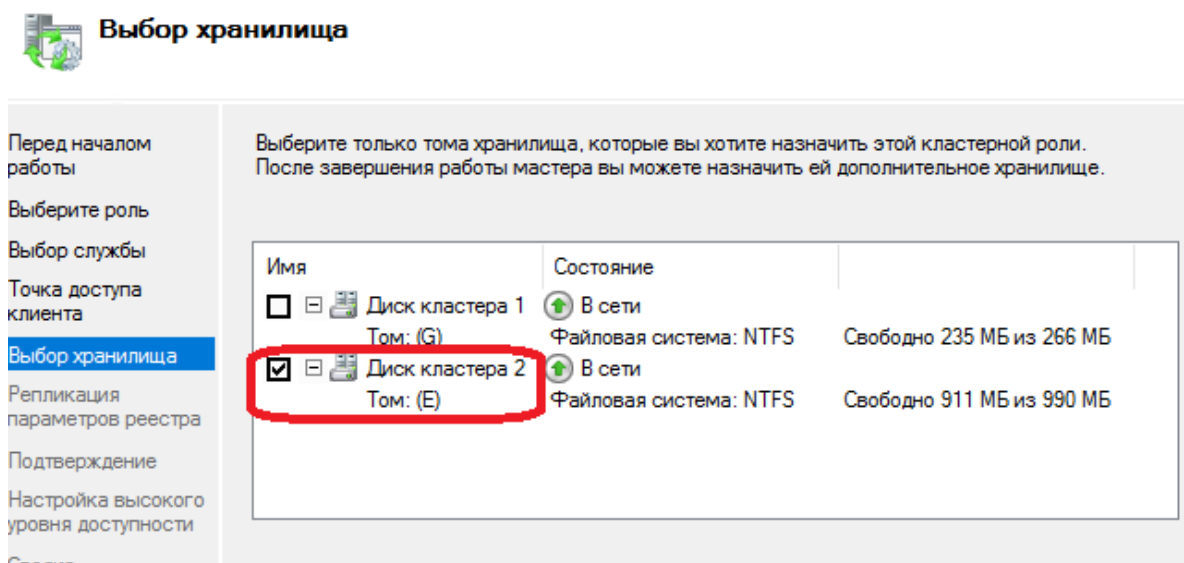


Рисунок 8.6 – Выбор хранилища

м) нажать «Далее» и затем кнопку «Готово». На этом роль отказоустойчивости службы PG настроена;

н) добавить контроль доступности подключения к PG;

о) создать локального администратора на каждом сервере (в примере это пользователь rna);

п) на рабочем столе этого пользователя создать файл скрипта Powershell pg_check.ps1 со следующим содержимым:

```
$pg_status = "C:\tmp\pg_status.txt"
```

```
function pg_check {  
    $stream = [System.IO.StreamWriter] $pg_status  
  
    pg_isready -p 8080 -h 127.0.0.1 -U postgres  
    $? | % { $stream.WriteLine($_) }  
    $stream.close()  
    # Таймаут ожидания ответа от запроса pg_isready  
    Start-Sleep -Seconds 3  
}  
  
function loop_check {  
    foreach($i in 1..3) {  
        if((Get-Content $pg_status) -eq $False) {  
            pg_check  
        }  
        # Таймаут повтора проверки запроса. При увеличении необходимо  
        # корректировать частоты выполнения скрипта в планировщике.  
        Start-Sleep -Seconds 10  
    }  
    # Перезагружаем компьютер после трех неудачных проверок pg_isready  
    Restart-Computer -force  
}  
  
pg_check  
  
if((((Get-Service -Name JatobaServer).Status -eq "Running") -and ((Get-Content  
    $pg_status) -eq $False)) {  
    loop_check  
  
}
```

Этот скрипт проверяет доступность подключения к локальному PG и если после трех попыток не может подключиться, то перезапускает локальный Windows сервер, в результате

| | | |
|--------------------|--------------------------|--------------------------|
| № изменения: _____ | Подпись отв. лица: _____ | Дата внесения изм: _____ |
|--------------------|--------------------------|--------------------------|

чего физические подключения к БД пойдут через второй сервер (сработает кластерная роль). Количество попыток подключения, таймаут ожидания повтора можно изменять, при увеличении таймаута необходимо увеличить время повтора выполнения скрипта в планировщике заданий.

- р) создать задачу в планировщике;
- с) в задании используется именно пользователь «postgres»;
- т) добавить триггер, как показано на рисунке 8.7;

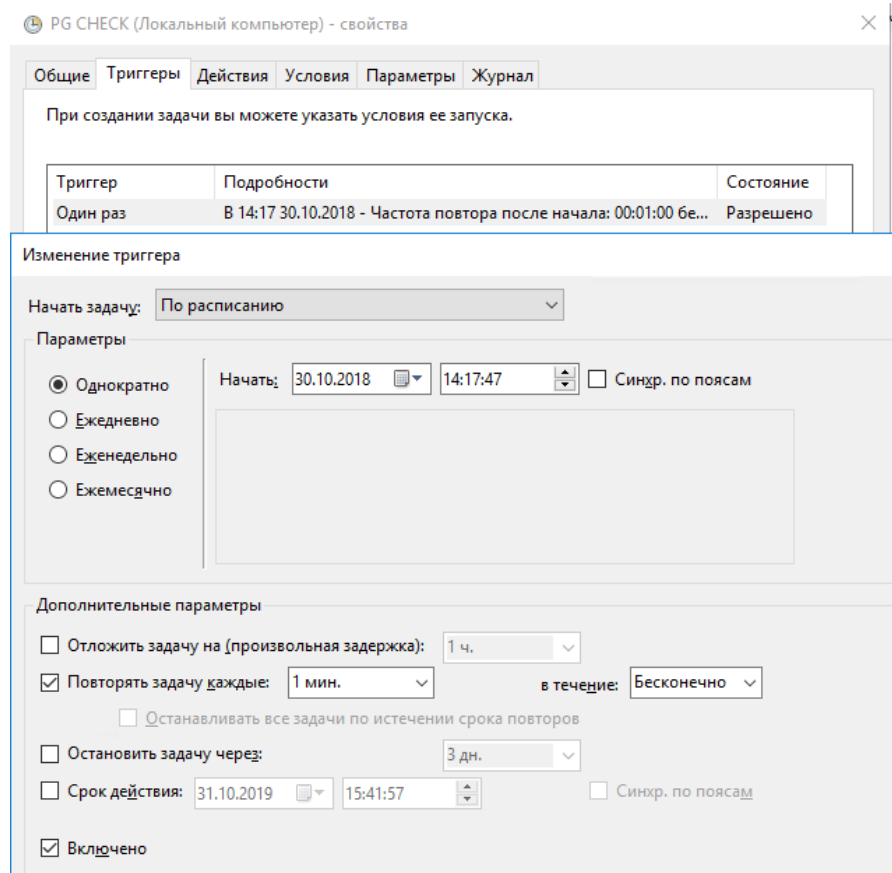


Рисунок 8.7 – Добавление триггера

- у) указать путь к PowerShell на локальном компьютере:

```
C:\Windows\System32\WindowsPowerShell\v1.1\powershell.exe
```

и файл скрипта как показано на рисунке 8.8:

```
-File "C:\tmp\pg_check.ps1",
```

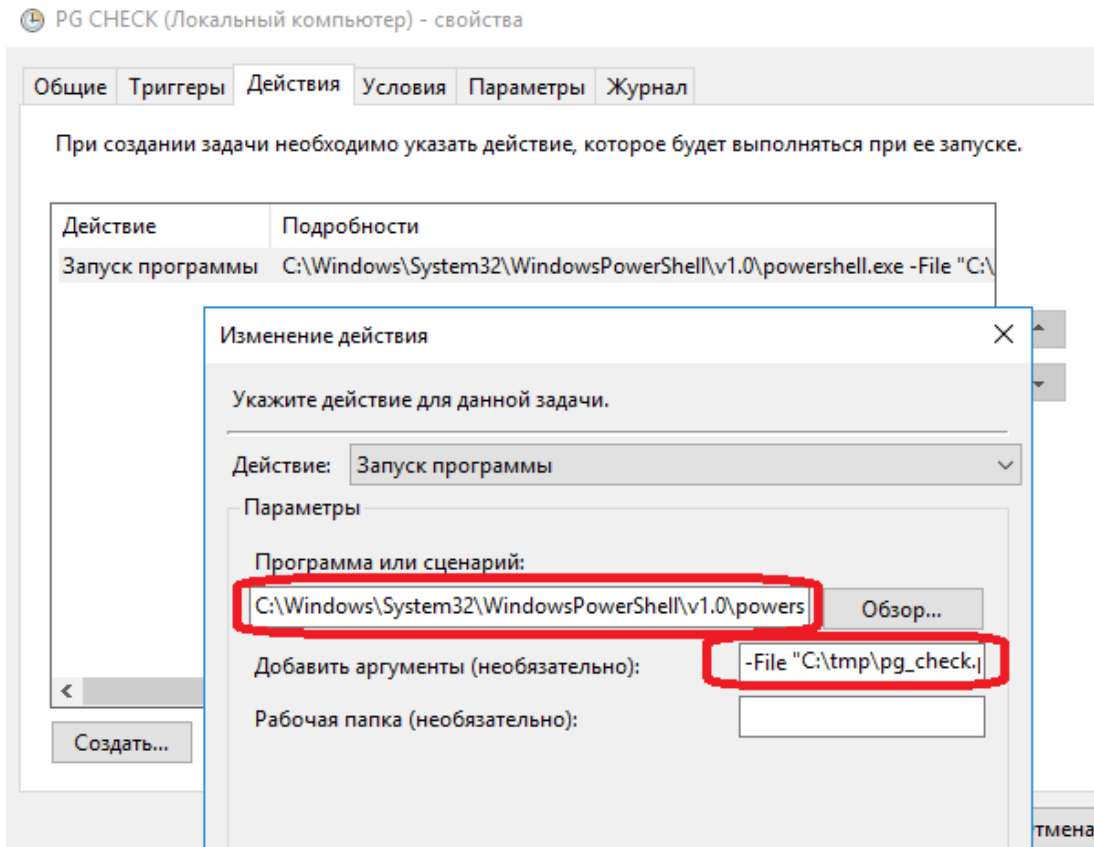



Рисунок 8.8 – Путь к PowerShell. Путь к файлу скрипта

ф) указать условия запуска, как показано на рисунке 8.9.

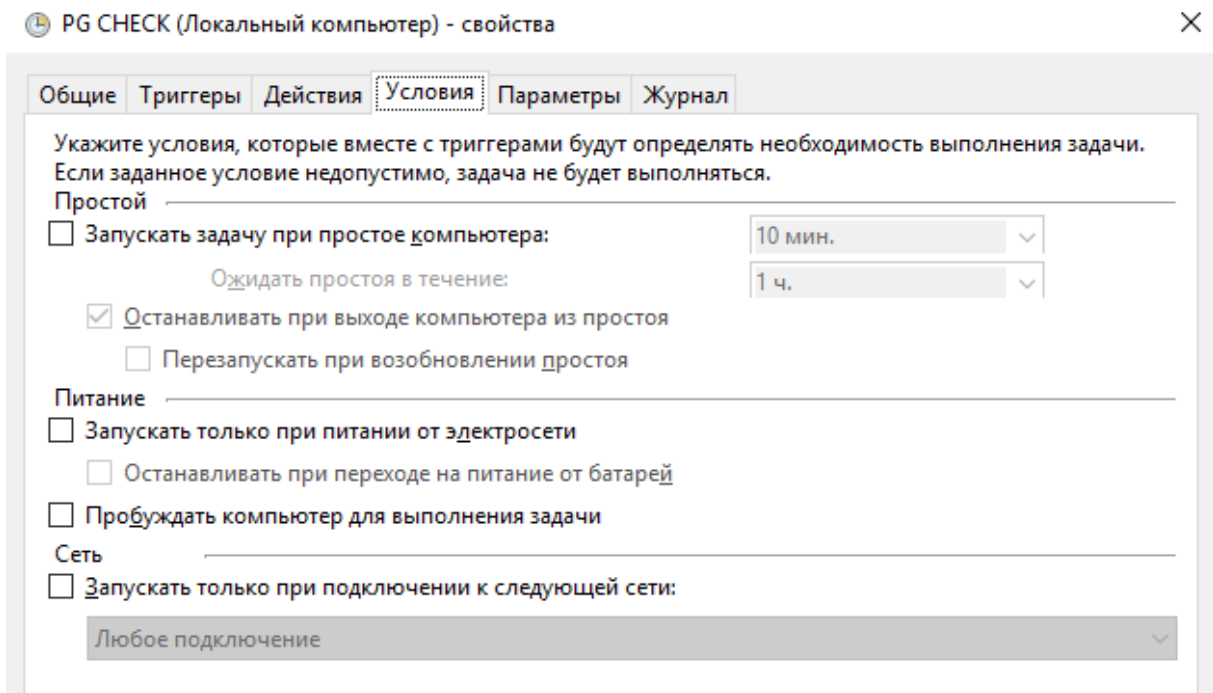


Рисунок 8.9 – Условия запуска

х) затем параметры, как показано на рисунке 8.10.

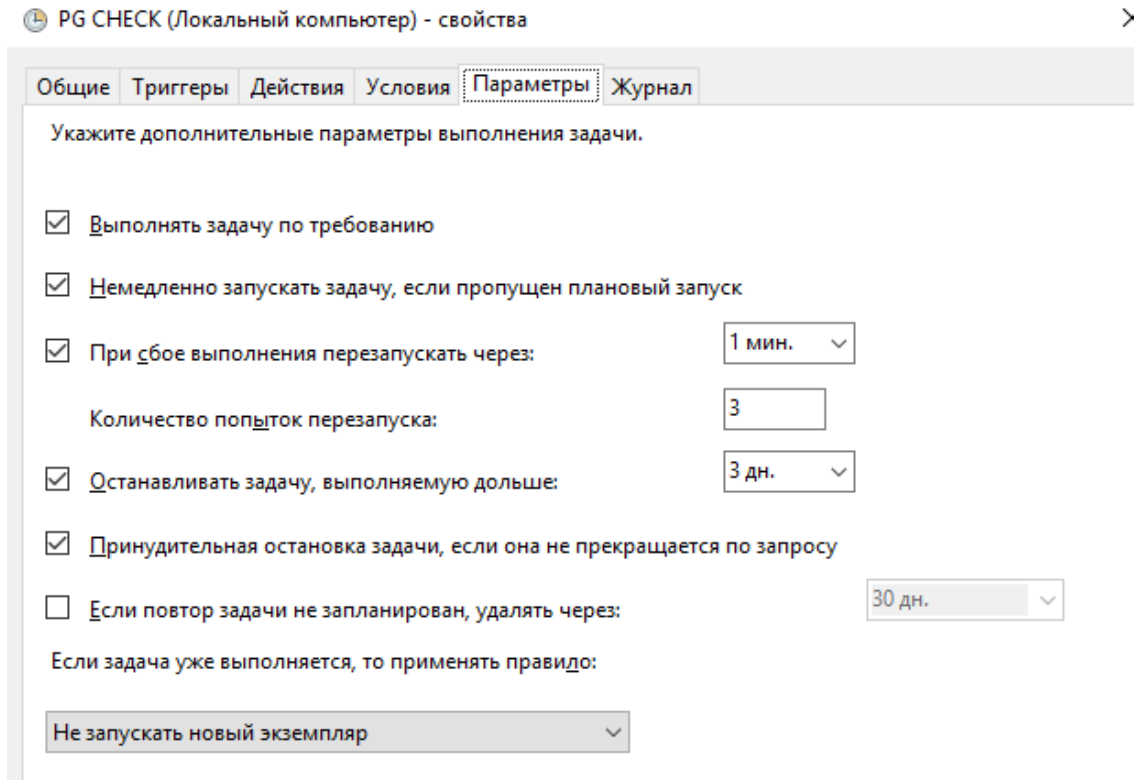


Рисунок 8.10 – Параметры

8.2. Настройка отказоустойчивого кластера СУБД «Jatoba» с использованием компонента «jaDog»

Настройка отказоустойчивого кластера СУБД «Jatoba» с использованием встроенного модуля jaDog описана в документах:

- «643.72410666.00067-05 98 01-01 «Руководство по настройке. Часть 1. Управление режимом работы узлов кластера. Компонент «jaDog» (версия 1.4.2);
- «643.72410666.00067-05 98 02-01 «Руководство по настройке. Часть 1. Управление режимом работы узлов кластера. Компонент «jaDog» (версия 2.0).

9. СООБЩЕНИЯ ОБ ОШИБКАХ

СУБД «Jatoba» использует пятисимвольные коды ошибок, описанные в стандарте SQL ISO/IEC 9075 «Язык баз данных SQL».

Перечень данных ошибок приведен в таблице 9.1.

Таблица 9.1 – Коды ошибок СУБД «Jatoba» по стандарту SQL ISO/IEC 9075

| Код ошибки | Имя условия |
|-------------------|---|
| Класс 00 | Успешное завершение |
| 00000 | successful_completion |
| Класс 01 | Предупреждение |
| 01000 | warning |
| 0100C | dynamic_result_sets_returned |
| 01008 | implicit_zero_bit_padding |
| 01003 | null_value_eliminated_in_set_function |
| 01007 | privilege_not_granted |
| 01006 | privilege_not_revoked |
| 01004 | string_data_right_truncation |
| 01P01 | deprecated_feature |
| Класс 02 | Нет данных (это также класс предупреждений согласно стандарту SQL) |
| 02000 | no_data |
| 02001 | no_additional_dynamic_result_sets_returned |
| Класс 03 | SQL-оператор еще не завершен |
| 03000 | sql_statement_not_yet_complete |
| Класс 08 | Исключение, связанное с подключением |
| 08000 | connection_exception |
| 08003 | connection_does_not_exist |
| 08006 | connection_failure |
| 08001 | sqlclient_unable_to_establish_sqlconnection |
| 08004 | sqlserver_rejected_establishment_of_sqlconnection |
| 08007 | transaction_resolution_unknown |
| 08P01 | protocol_violation |
| Класс 09 | Исключение с действием триггера |
| 09000 | triggered_action_exception |
| Класс 0A | Неподдерживаемая функциональность |
| 0A000 | feature_not_supported |
| Класс 0B | Неверное начало транзакции |
| 0B000 | invalid_transaction_initiation |
| Класс 0F | Исключение с указателем на данные |
| 0F000 | locator_exception |
| 0F001 | invalid_locator_specification |
| Класс 0L | Неверный праводатель |
| 0L000 | invalid_grantor |
| 0LP01 | invalid_grant_operation |
| Класс 0P | Неверное указание роли |

| | | |
|--------------------|--------------------------|--------------------------|
| № изменения: _____ | Подпись отв. лица: _____ | Дата внесения изм: _____ |
|--------------------|--------------------------|--------------------------|

| Код ошибки | Имя условия |
|-------------------|---|
| 0P000 | invalid_role_specification |
| Класс 0Z | Исключение диагностики |
| 0Z000 | diagnostics_exception |
| 0Z002 | stacked_diagnostics_accessed_without_active_handler |
| Класс 20 | Case не найден |
| 20000 | case_not_found |
| Класс 21 | Нарушение количества |
| 21000 | cardinality_violation |
| Класс 22 | Исключение в данных |
| 22000 | data_exception |
| 2202E | array_subscript_error |
| 22021 | character_not_in_repertoire |
| 22008 | datetime_field_overflow |
| 22012 | division_by_zero |
| 22005 | error_in_assignment |
| 2200B | escape_character_conflict |
| 22022 | indicator_overflow |
| 22015 | interval_field_overflow |
| 2201E | invalid_argument_for_logarithm |
| 22014 | invalid_argument_for_ntile_function |
| 22016 | invalid_argument_for_nth_value_function |
| 2201F | invalid_argument_for_power_function |
| 2201G | invalid_argument_for_width_bucket_function |
| 22018 | invalid_character_value_for_cast |
| 22007 | invalid_datetime_format |
| 22019 | invalid_escape_character |
| 2200D | invalid_escape_octet |
| 22025 | invalid_escape_sequence |
| 22P06 | nonstandard_use_of_escape_character |
| 22010 | invalid_indicator_parameter_value |
| 22023 | invalid_parameter_value |
| 2201B | invalid_regular_expression |
| 2201W | invalid_row_count_in_limit_clause |
| 2201X | invalid_row_count_in_result_offset_clause |
| 2202H | invalid_tablesample_argument |
| 2202G | invalid_tablesample_repeat |
| 22009 | invalid_time_zone_displacement_value |
| 2200C | invalid_use_of_escape_character |
| 2200G | most_specific_type_mismatch |
| 22004 | null_value_not_allowed |
| 22002 | null_value_no_indicator_parameter |
| 22003 | numeric_value_out_of_range |
| 22026 | string_data_length_mismatch |
| 2001 | string_data_right_truncation |
| 22011 | substring_error |
| 22027 | trim_error |

| | | |
|--------------------|--------------------------|--------------------------|
| № изменения: _____ | Подпись отв. лица: _____ | Дата внесения изм: _____ |
|--------------------|--------------------------|--------------------------|

| Код ошибки | Имя условия |
|-------------------|---|
| 22024 | unterminated_c_string |
| 2200F | zero_length_character_string |
| 22P01 | floating_point_exception |
| 22P02 | invalid_text_representation |
| 22P03 | invalid_binary_representation |
| 22P04 | bad_copy_file_format |
| 22P05 | untranslatable_character |
| 2200L | not_an_xml_document |
| 2200M | invalid_xml_document |
| 2200N | invalid_xml_content |
| 2200S | invalid_xml_comment |
| 2200T | invalid_xml_processing_instruction |
| Класс 23 | Нарушение ограничения целостности |
| 23000 | integrity_constraint_violation |
| 23001 | restrict_violation |
| 23502 | not_null_violation |
| 23503 | foreign_key_violation |
| 23505 | unique_violation |
| 23514 | check_violation |
| 23P01 | exclusion_violation |
| Класс 24 | Неверное состояние курсора |
| 24000 | invalid_cursor_state |
| Класс 25 | Неверное состояние транзакции |
| 25000 | invalid_transaction_state |
| 25001 | active_sql_transaction |
| 25002 | branch_transaction_already_active |
| 25008 | held_cursor_requires_same_isolation_level |
| 25003 | inappropriate_access_mode_for_branch_transaction |
| 25004 | inappropriate_isolation_level_for_branch_transaction |
| 25005 | no_active_sql_transaction_for_branch_transaction |
| 25006 | read_only_sql_transaction |
| 25007 | schema_and_data_statement_mixing_not_supported |
| 25P01 | no_active_sql_transaction |
| 25P02 | in_failed_sql_transaction |
| Класс 26 | Неверное имя SQL-оператора |
| 26000 | invalid_sql_statement_name |
| Класс 27 | Нарушение при изменении данных в триггере |
| 27000 | triggered_data_change_violation |
| Класс 28 | Неверное указание авторизации |
| 28000 | invalid_authorization_specification |
| 28P01 | invalid_password |
| Класс 2B | Зависимые описания привилегий все еще существуют |
| 2B000 | dependent_privilege_descriptors_still_exist |
| 2BP01 | dependent_objects_still_exist |
| Класс 2D | Неверное завершение транзакции |
| 2D000 | invalid_transaction_termination |

| | | |
|--------------------|--------------------------|--------------------------|
| № изменения: _____ | Подпись отв. лица: _____ | Дата внесения изм: _____ |
|--------------------|--------------------------|--------------------------|

| Код ошибки | Имя условия |
|-------------------|--|
| Класс 2F | Исключение в подпрограмме SQL |
| 2F000 | sql_routine_exception |
| 2F005 | function_executed_no_return_statement |
| 2F002 | modifying_sql_data_not_permitted |
| 2F003 | prohibited_sql_statement_attempted |
| 2F004 | reading_sql_data_not_permitted |
| Класс 34 | Неверное имя курсора |
| 34000 | invalid_cursor_name |
| Класс 38 | Исключение во внешней подпрограмме |
| 38000 | external_routine_exception |
| 38001 | containing_sql_not_permitted |
| 38002 | modifying_sql_data_not_permitted |
| 38003 | prohibited_sql_statement_attempted |
| 38004 | reading_sql_data_not_permitted |
| Класс 39 | Исключение при вызове внешней подпрограммы |
| 39001 | invalid_sqlstate_returned |
| 39000 | external_routine_invocation_exception |
| 39004 | null_value_not_allowed |
| 39P01 | trigger_protocol_violated |
| 39P02 | srf_protocol_violated |
| 39P03 | event_trigger_protocol_violated |
| Класс 3В | Исключение точки сохранения |
| 3В000 | savepoint_exception |
| 3В001 | invalid_savepoint_specification |
| Класс 3D | Неверное имя каталога |
| 3D000 | invalid_catalog_name |
| Класс 3F | Неверное имя схемы |
| 3F000 | invalid_schema_name |
| Класс 40 | Откат транзакции |
| 40000 | transaction_rollback |
| 40002 | transaction_integrity_constraint_violation |
| 40001 | serialization_failure |
| 40003 | statement_completion_unknown |
| 40P01 | deadlock_detected |
| Класс 42 | Ошибка синтаксиса или нарушение правила доступа |
| 42000 | syntax_error_or_access_rule_violation |
| 42601 | syntax_error |
| 42501 | insufficient_privilege |
| 42846 | cannot_coerce |
| 42803 | grouping_error |
| 42P20 | windowing_error |
| 42P19 | invalid_recursion |
| 42830 | invalid_foreign_key |
| 42602 | invalid_name |
| 42622 | name_too_long |
| 42939 | reserved_name |

№ изменения: _____ Подпись отв. лица: _____ Дата внесения изм: _____

| Код ошибки | Имя условия |
|-------------------|---|
| 42804 | datatype_mismatch |
| 42P18 | indeterminate_datatype |
| 42P21 | collation_mismatch |
| 42P22 | indeterminate_collation |
| 42809 | wrong_object_type |
| 42703 | undefined_column |
| 42883 | undefined_function |
| 42P01 | undefined_table |
| 42P02 | undefined_parameter |
| 42704 | undefined_object |
| 42701 | duplicate_column |
| 42P03 | duplicate_cursor |
| 42P04 | duplicate_database |
| 42723 | duplicate_function |
| 42P05 | duplicate_prepared_statement |
| 42P06 | duplicate_schema |
| 42P07 | duplicate_table |
| 42712 | duplicate_alias |
| 42710 | duplicate_object |
| 42702 | ambiguous_column |
| 42725 | ambiguous_function |
| 42P08 | ambiguous_parameter |
| 42P09 | ambiguous_alias |
| 42P10 | invalid_column_reference |
| 42611 | invalid_column_definition |
| 42P11 | invalid_cursor_definition |
| 42P12 | invalid_database_definition |
| 42P13 | invalid_function_definition |
| 42P14 | invalid_prepared_statement_definition |
| 42P15 | invalid_schema_definition |
| 42P16 | invalid_table_definition |
| 42P17 | invalid_object_definition |
| Класс 44 | Нарушение WITH CHECK OPTION |
| 44000 | with_check_option_violation |
| Класс 53 | Нехватка ресурсов |
| 53000 | insufficient_resources |
| 53100 | disk_full |
| 53200 | out_of_memory |
| 53300 | too_many_connections |
| 53400 | configuration_limit_exceeded |
| Класс 54 | Превышение ограничения программы |
| 54000 | program_limit_exceeded |
| 54001 | statement_too_complex |
| 54011 | too_many_columns |
| 54023 | too_many_arguments |
| Класс 55 | Объект не в требуемом состоянии |

| | | |
|--------------------|--------------------------|--------------------------|
| № изменения: _____ | Подпись отв. лица: _____ | Дата внесения изм: _____ |
|--------------------|--------------------------|--------------------------|

| Код ошибки | Имя условия |
|-------------------|--|
| 55000 | object_not_in_prerequisite_state |
| 55006 | object_in_use |
| 55P02 | cant_change_runtime_param |
| 55P03 | lock_not_available |
| Класс 57 | Вмешательство оператора |
| 57000 | operator_intervention |
| 57014 | query_canceled |
| 57P01 | admin_shutdown |
| 57P02 | crash_shutdown |
| 57P03 | cannot_connect_now |
| 57P04 | database_dropped |
| Класс 58 | Ошибка системы |
| 58000 | system_error |
| 58030 | io_error |
| 58P01 | undefined_file |
| 58P02 | duplicate_file |
| Класс F0 | Ошибка файла конфигурации |
| F0000 | config_file_error |
| F0001 | lock_file_exists |
| Класс HV | Ошибка обертки сторонних данных (SQL/MED) |
| HV000 | fdw_error |
| HV005 | fdw_column_name_not_found |
| HV002 | fdw_dynamic_parameter_value_needed |
| HV010 | fdw_function_sequence_error |
| HV021 | fdw_inconsistent_descriptor_information |
| HV024 | fdw_invalid_attribute_value |
| HV007 | fdw_invalid_column_name |
| HV008 | fdw_invalid_column_number |
| HV004 | fdw_invalid_data_type |
| HV006 | fdw_invalid_data_type_descriptors |
| HV091 | fdw_invalid_descriptor_field_identifier |
| HV00B | fdw_invalid_handle |
| HV00C | fdw_invalid_option_index |
| HV00D | fdw_invalid_option_name |
| HV090 | fdw_invalid_string_length_or_buffer_length |
| HV00A | fdw_invalid_string_format |
| HV009 | fdw_invalid_use_of_null_pointer |
| HV014 | fdw_too_many_handles |
| HV001 | fdw_out_of_memory |
| HV00P | fdw_no_schemas |
| HV00J | fdw_option_name_not_found |
| HV00K | fdw_reply_handle |
| HV00Q | fdw_schema_not_found |
| HV00R | fdw_table_not_found |
| HV00L | fdw_unable_to_create_execution |
| HV00M | fdw_unable_to_create_reply |

| | | |
|--------------------|--------------------------|--------------------------|
| № изменения: _____ | Подпись отв. лица: _____ | Дата внесения изм: _____ |
|--------------------|--------------------------|--------------------------|

| | |
|-------------------|------------------------------------|
| Код ошибки | Имя условия |
| HV00N | fdw_unable_to_establish_connection |
| Класс P0 | Ошибка PL/pgSQL |
| P0000 | plpgsql_error |
| P0001 | raise_exception |
| P0002 | no_data_found |
| P0003 | too_many_rows |
| P0004 | assert_failure |
| Класс XX | Внутренняя ошибка |
| XX000 | internal_error |
| XX001 | data_corrupted |
| XX002 | index_corrupted |

Возможные сообщения об ошибках, связанные с действиями по выполнению функций безопасности, приведены в таблице 9.2.

Таблица 9.2 – Перечень ошибок при выполнении ФБО

| Мера | Код | Сообщение | Сообщение в транскрипции |
|-------|--------|---|--|
| (ИАФ) | c:43 | msgid "could not look up effective user ID %ld: %s" | msgstr "выяснить эффективный идентификатор пользователя (%ld) не удалось: %s" |
| (ИАФ) | c:554 | msgid "user does not exist" | msgstr "пользователь не существует" |
| (ИАФ) | c:60 | msgid "user name lookup failure: error code %lu" | msgstr "распознать имя пользователя не удалось (код ошибки: %lu)" |
| (ИАФ) | c:1796 | msgid "Enter new password: " | msgstr "Введите новый пароль: " |
| (ИАФ) | c:1801 | msgid "Passwords didn't match.\n" | msgstr "Пароли не совпадают.\n" |
| (ИАФ) | c:3329 | msgid "Cannot login" | msgstr "Вход запрещен" |
| (ИАФ) | c:3358 | msgid "Password valid until " | msgstr "Пароль действует до " |
| (ИАФ) | c:140 | msgid " -w, --no-password never prompt for password\n" | msgstr " -w, --no-password не запрашивать пароль\n" |
| (ИАФ) | c:141 | msgid " -W, --password force password prompt (should happen \"automatically)\n" | msgstr " -W, --password запрашивать пароль всегда (обычно не требуется)\n" |
| (ИАФ) | c:297 | msgid " \\password [USERNAME] securely change the password for a user\n" | msgstr " \\password [ИМЯ] безопасно сменить пароль пользователя\n" |
| (ИАФ) | c:1093 | msgid "password too long" | msgstr "слишком длинный пароль" |
| (ИАФ) | c:249 | msgid "client selected an invalid SASL authentication mechanism" | msgstr "клиент выбрал неверный механизм аутентификации SASL" |
| (ИАФ) | c:296 | msgid "password authentication failed for user \"%s\"" | msgstr "пользователь \"%s\" не прошел проверку подлинности (по паролю)" |
| (ИАФ) | c:322 | msgid "authentication failed for user \"%s\": invalid authentication method" | msgstr "пользователь \"%s\" не прошел проверку подлинности: неверный метод проверки" |
| (ИАФ) | c:3282 | msgid "could not perform MD5 encryption of received packet" | msgstr "не удалось вычислить MD5 для принятого пакета" |
| (ИАФ) | c:80 | msgid "User \"%s\" has an expired password." | msgstr "Срок пароля пользователя \"%s\" истек." |

| | | |
|--------------------|--------------------------|--------------------------|
| № изменения: _____ | Подпись отв. лица: _____ | Дата внесения изм: _____ |
|--------------------|--------------------------|--------------------------|

| | | | |
|-------|-------------------------|---|--|
| (ИАФ) | c:182 | msgid "User \"%s\" has a password that cannot be used with MD5 authentication." | msgstr "Пользователь \"%s\" имеет пароль, неподходящий для аутентификации по MD5." |
| (ИАФ) | c:206 c:247 c:271 | msgid "Password does not match for user \"%s\"." | msgstr "Пароль не подходит для пользователя \"%s\"." |
| (ИАФ) | c:290 | msgid "Password of user \"%s\" is in unrecognized format." | msgstr "Пароль пользователя \"%s\" представлен в неизвестном формате." |
| (ИАФ) | c:408 | msgid "%s: real and effective user IDs must match\n" | msgstr "%s: фактический и эффективный ID пользователя должны совпадать\n" |
| (ИАФ) | c:2397 | msgid "Sets the maximum allowed time to complete client authentication." | msgstr "Ограничивает время, за которое клиент должен пройти аутентификацию." |
| (ИАФ) | y:1026 | msgid "UNENCRYPTED PASSWORD is no longer supported" | msgstr "вариант UNENCRYPTED PASSWORD более не поддерживается" |
| (ИАФ) | y:1027 | msgid "Remove UNENCRYPTED to store the password in encrypted form instead." | msgstr "Удалите слово UNENCRYPTED, чтобы сохранить пароль в зашифрованном виде." |
| (ИАФ) | l:1556 | #~ msgid "%s: could not determine user name (GetUserName failed)\n" | #~ msgstr "%s: не удалось определить имя пользователя (ошибка в GetUserName)\n" |
| (ИАФ) | l:1556 | #~ msgid "User \"%s\" has an empty password." | #~ msgstr "У пользователя \"%s\" пустой пароль." |
| (УПД) | c:45 | msgid "command not executable" | msgstr "неисполняемая команда" |
| (УПД) | c:552 | msgid "could not get home directory for user ID %ld: %s\n" | msgstr "не удалось получить домашний каталог пользователя с ид. %ld: %s\n" |
| (УПД) | c:1098 | msgid "The server (version %s) does not support altering default privileges.\n" | msgstr "Сервер (версия %s) не поддерживает изменение прав по умолчанию.\n" |
| (УПД) | c:3323 | msgid "Create role" | msgstr "Создает роли" |
| (УПД) | c:3326 | msgid "Create DB" | msgstr "Создает БД" |
| (УПД) | c:3408 | msgid "The server (version %s) does not support per-database role settings.\n" | "Сервер (версия %s) не поддерживает назначение параметров ролей для баз " |
| (УПД) | c:3444 | msgid "Did not find any settings for role \"%s\" and database \"%s\".\n" | msgstr "Параметры для роли \"%s\" и базы данных \"%s\" не найдены.\n" |
| (УПД) | c:3447 | msgid "Did not find any settings for role \"%s\".\n" | msgstr "Параметры для роли \"%s\" не найдены.\n" |
| (УПД) | c:3450 | msgid "Did not find any settings.\n" | msgstr "Никакие параметры не найдены.\n" |
| (УПД) | c:3364 | msgid "permission denied for aggregate %s" | msgstr "нет доступа к агрегату %s" |
| (УПД) | c:3367 | msgid "permission denied for collation %s" | msgstr "нет доступа к правилу сортировки %s" |
| (УПД) | c:3370 | msgid "permission denied for column %s" | msgstr "нет доступа к столбцу %s" |
| (УПД) | c:3373 | msgid "permission denied for conversion %s" | msgstr "нет доступа к преобразованию %s" |

| | | | |
|-------|--------|---|--|
| (УПД) | c:3376 | msgid "permission denied for database %s" | msgstr "нет доступа к базе данных %s" |
| (УПД) | c:3379 | msgid "permission denied for domain %s" | msgstr "нет доступа к домену %s" |
| (УПД) | c:3382 | msgid "permission denied for event trigger %s" | msgstr "нет доступа к событийному триггеру %s" |
| (УПД) | c:3385 | msgid "permission denied for extension %s" | msgstr "нет доступа к расширению %s" |
| (УПД) | c:3388 | msgid "permission denied for foreign-data wrapper %s" | msgstr "нет доступа к обертке сторонних данных %s" |
| (УПД) | c:3391 | msgid "permission denied for foreign server %s" | msgstr "нет доступа к стороннему серверу %s" |
| (УПД) | c:3394 | msgid "permission denied for foreign table %s" | msgstr "нет доступа к сторонней таблице %s" |
| (УПД) | c:3397 | msgid "permission denied for function %s" | msgstr "нет доступа к функции %s" |
| (УПД) | c:3400 | msgid "permission denied for index %s" | msgstr "нет доступа к индексу %s" |
| (УПД) | c:3403 | msgid "permission denied for language %s" | msgstr "нет доступа к языку %s" |
| (УПД) | c:3406 | msgid "permission denied for large object %s" | msgstr "нет доступа к большому объекту %s" |
| (УПД) | c:3409 | msgid "permission denied for materialized view %s" | msgstr "нет доступа к материализованному представлению %s" |
| (УПД) | c:3412 | msgid "permission denied for operator class %s" | msgstr "нет доступа к классу операторов %s" |
| (УПД) | c:3415 | msgid "permission denied for operator %s" | msgstr "нет доступа к оператору %s" |
| (УПД) | c:3418 | msgid "permission denied for operator family %s" | msgstr "нет доступа к семейству операторов %s" |
| (УПД) | c:3421 | msgid "permission denied for policy %s" | msgstr "нет доступа к политике %s" |
| (УПД) | c:3424 | msgid "permission denied for procedure %s" | msgstr "нет доступа к процедуре %s" |
| (УПД) | c:3427 | msgid "permission denied for publication %s" | msgstr "нет доступа к публикации %s" |
| (УПД) | c:3430 | msgid "permission denied for routine %s" | msgstr "нет доступа к подпрограмме %s" |
| (УПД) | c:3433 | msgid "permission denied for schema %s" | msgstr "нет доступа к схеме %s" |
| (УПД) | c:1852 | msgid "permission denied for sequence %s" | msgstr "нет доступа к последовательности %s" |
| (УПД) | c:3439 | msgid "permission denied for statistics object %s" | msgstr "нет доступа к объекту статистики %s" |
| (УПД) | c:3442 | msgid "permission denied for subscription %s" | msgstr "нет доступа к подписке %s" |
| (УПД) | c:3445 | msgid "permission denied for table %s" | msgstr "нет доступа к таблице %s" |
| (УПД) | c:3448 | msgid "permission denied for tablespace %s" | msgstr "нет доступа к табличному пространству %s" |

| | | |
|--------------------|--------------------------|--------------------------|
| № изменения: _____ | Подпись отв. лица: _____ | Дата внесения изм: _____ |
|--------------------|--------------------------|--------------------------|

| | | | |
|-------|-----------------|--|--|
| (УПД) | c:3451 | msgid "permission denied for text search configuration %s" | msgstr "нет доступа к конфигурации текстового поиска %s" |
| (УПД) | c:3454 | msgid "permission denied for text search dictionary %s" | msgstr "нет доступа к словарю текстового поиска %s" |
| (УПД) | c:3457 | msgid "permission denied for type %s" | msgstr "нет доступа к типу %s" |
| (УПД) | c:3460 | msgid "permission denied for view %s" | msgstr "нет доступа к представлению %s" |
| (УПД) | c:3643 | msgid "permission denied for column \"%s\" of relation \"%s\"" | msgstr "нет доступа к столбцу \"%s\" отношения \"%s\"" |
| (УПД) | c:58 | msgid "permission denied to create access method \"%s\"" | msgstr "нет прав на создание метода доступа \"%s\"" |
| (УПД) | c:60 | msgid "Must be superuser to create an access method." | msgstr "Для создания метода доступа нужно быть суперпользователем." |
| (УПД) | c:68 | msgid "access method \"%s\" already exists" | msgstr "метод доступа \"%s\" уже существует" |
| (УПД) | c:123 | msgid "must be superuser to drop access methods" | msgstr "для удаления методов доступа нужно быть суперпользователем" |
| (УПД) | c:824 | msgid "" "must be superuser or a member of the pg_write_server_files role to COPY to a ""file" | "для выполнения COPY с записью в файл нужно быть суперпользователем или ""членом роли pg_write_server_files" |
| (УПД) | c:311 | msgid "permission denied to create database" | msgstr "нет прав на создание базы данных" |
| (УПД) | c:346 | msgid "permission denied to copy database \"%s\"" | msgstr "нет прав на копирование базы данных \"%s\"" |
| (УПД) | c:480 c:1016 | msgid "database \"%s\" already exists" | msgstr "база данных \"%s\" уже существует" |
| (УПД) | c:839 | msgid "cannot drop a template database" | msgstr "удалить шаблон базы данных нельзя" |
| (УПД) | c:845 | msgid "cannot drop the currently open database" | msgstr "удалить базу данных, открытую в данный момент, нельзя" |
| (УПД) | c:1007 | msgid "permission denied to rename database" | msgstr "нет прав на переименование базы данных" |
| (УПД) | c:1667 | msgid "permission denied to change owner of database" | msgstr "нет прав на изменение владельца базы данных" |
| (УПД) | c:620 | msgid "permission denied to change owner of event trigger \"%s\"" | msgstr "нет прав на изменение владельца событийного триггера \"%s\"" |
| (УПД) | c:807 | msgid "permission denied to create extension \"%s\"" | msgstr "нет прав на создание расширения \"%s\"" |
| (УПД) | c:813 | msgid "permission denied to update extension \"%s\"" | msgstr "нет прав на изменение расширения \"%s\"" |
| (УПД) | c:696 | msgid "permission denied to alter foreign-data wrapper \"%s\"" | msgstr "нет прав на изменение обертки сторонних данных \"%s\"" |
| (УПД) | c:924 | msgid "permission denied: \"%s\" is a system catalog" | msgstr "доступ запрещен: \"%s\" - это системный каталог" |
| (УПД) | c:170 | msgid "ignoring specified roles other than PUBLIC" | msgstr "все указанные роли, кроме PUBLIC, игнорируются" |
| (УПД) | c:802 c:1247 | msgid "policy \"%s\" for table \"%s\" already exists" | msgstr "политика \"%s\" для таблицы \"%s\" уже существует" |

№ изменения: _____ Подпись отв. лица: _____ Дата внесения изм: _____

| | | | |
|-------|------------------|---|---|
| (УПД) | c:681 | msgid "permission denied to change owner of publication \"%s\"" | msgstr "нет прав на изменение владельца публикации \"%s\"" |
| (УПД) | c:590 | msgid "could not set permissions on directory \"%s\": %m" | msgstr "не удалось установить права для каталога \"%s\": %m" |
| (УПД) | c:295 | msgid "must be superuser to create superusers" | msgstr "для создания суперпользователей нужно быть суперпользователем" |
| (УПД) | c:302 | msgid "must be superuser to create replication users" | msgstr "для создания пользователей-репликаторов нужно быть суперпользователем" |
| (УПД) | c:309 c:707 | msgid "must be superuser to change bypassrls attribute" | msgstr "для изменения атрибута bypassrls нужно быть суперпользователем" |
| (УПД) | c:316 | msgid "permission denied to create role" | msgstr "нет прав для создания роли" |
| (УПД) | c:340 c:1210 | msgid "role \"%s\" already exists" | msgstr "роль \"%s\" уже существует" |
| (УПД) | c:406 c:816 | msgid "empty string is not a valid password, clearing password" | msgstr "пустая строка не является допустимым паролем; пароль сбрасывается" |
| (УПД) | c:1593 | msgid "must be superuser to alter superusers" | msgstr "для модификации суперпользователей нужно быть суперпользователем" |
| (УПД) | c:700 | msgid "must be superuser to alter replication users" | msgstr "для модификации пользователей-репликаторов нужно быть суперпользователем" |
| (УПД) | c:723 c:923 | msgid "permission denied" | msgstr "нет доступа" |
| (УПД) | c:975 | msgid "permission denied to drop role" | msgstr "нет прав для удаления роли" |
| (УПД) | c:1026 c:1030 | msgid "current user cannot be dropped" | msgstr "пользователь не может удалить сам себя" |
| (УПД) | c:1034 | msgid "session user cannot be dropped" | msgstr "пользователя текущего сеанса нельзя удалить" |
| (УПД) | c:1045 | msgid "must be superuser to drop superusers" | msgstr "для удаления суперпользователей нужно быть суперпользователем" |
| (УПД) | c:1182 | msgid "session user cannot be renamed" | msgstr "пользователя текущего сеанса нельзя переименовать" |
| (УПД) | c:1186 | msgid "current user cannot be renamed" | msgstr "пользователь не может переименовать сам себя" |
| (УПД) | c:1220 | msgid "must be superuser to rename superusers" | msgstr "для переименования суперпользователей нужно быть суперпользователем" |
| (УПД) | c:1227 | msgid "permission denied to rename role" | msgstr "нет прав на переименование роли" |
| (УПД) | c:1248 | msgid "MD5 password cleared because of role rename" | msgstr "в результате переименования роли очищен MD5-хеш пароля" |
| (УПД) | c:1346 | msgid "permission denied to drop objects" | msgstr "нет прав на удаление объектов" |

| | | | |
|-------|--------------------|--|--|
| (УПД) | c:1373 c:1382 | msgid "permission denied to reassign objects" | msgstr "нет прав для переназначения объектов" |
| (УПД) | c:1457 c:1601 | msgid "must have admin option on role \"%s\"" | msgstr "требуется право admin для роли \"%s\"" |
| (УПД) | c:1474 | msgid "must be superuser to set grantor" | msgstr "для назначения права управления правами нужно быть суперпользователем" |
| (УПД) | c:466 | msgid "could not access file \"%s\": %m" | msgstr "нет доступа к файлу \"%s\": %m" |
| (УПД) | c:847 c:296 | msgid "permission denied for large object %u" | msgstr "нет доступа к большому объекту %u" |
| (УПД) | c:696 | msgid "could not set permissions of file \"%s\": %m" | msgstr "не удалось установить права доступа для файла \"%s\": %m" |
| (УПД) | c:157 | msgid "data directory \"%s\" has invalid permissions" | msgstr "для каталога данных \"%s\" установлены неправильные права доступа" |
| (УПД) | c:645 | msgid "role \"%s\" is not permitted to log in" | msgstr "для роли \"%s\" вход запрещен" |
| (УПД) | c:663 | msgid "too many connections for role \"%s\"" | msgstr "слишком много подключений для роли \"%s\"" |
| (УПД) | c:723 | msgid "permission denied to set session authorization" | msgstr "нет прав для смены объекта авторизации в сеансе" |
| (УПД) | c:346 | msgid "User does not have CONNECT privilege." | msgstr "Пользователь не имеет привилегии CONNECT." |
| (УПД) | c:363 | msgid "too many connections for database \"%s\"" | msgstr "слишком много подключений к БД \"%s\"" |
| (УПД) | c:803 | msgid "must be superuser or replication role to start walsender" | msgstr "для запуска процесса walsender требуется роль репликации или права суперпользователя " |
| (УПД) | y:1089 | msgid "unrecognized role option \"%s\"" | msgstr "нераспознанный параметр роли \"%s\"" |
| (УПД) | y:14900 y:14907 | msgid "%s cannot be used as a role name here" | msgstr "%s нельзя использовать здесь как имя роли" |
| (ОЦЛ) | c:3003 | msgid "Cannot add header to table content: column count of %d exceeded.\n" | "Ошибка добавления заголовка таблицы: превышен предел числа столбцов (%d).\n" |
| (ОЦЛ) | c:3043 | msgid "Cannot add cell to table content: total cell count of %d exceeded.\n" | "Ошибка добавления ячейки в таблицу: превышен предел числа ячеек (%d).\n" |
| (ОЦЛ) | c:3292 | msgid "invalid output format (internal error): %d" | msgstr "неверный формат вывода (внутренняя ошибка): %d" |
| (ОЦЛ) | c:220 | msgid "Invalid command \\\%s. Try \\\? for help.\n" | msgstr "Неверная команда \\\%s. Справка по командам: \\\?\n" |
| (ОЦЛ) | c:222 | msgid "invalid command \\\%s\n" | msgstr "неверная команда \\\%s\n" |
| (ОЦЛ) | c:4496 | msgid "invalid field size" | msgstr "неверный размер поля" |
| (ОЦЛ) | c:4519 | msgid "incorrect binary data format" | msgstr "неверный двоичный формат данных" |
| (ОЦЛ) | c:3209 | msgid "invalid input string for \"%Y,YYY\"" | msgstr "ошибка синтаксиса в значении для шаблона \"%Y,YYY\"" |

| | | | |
|-------|-----------------------|---|--|
| (ОЦЛ) | c:3724 | msgid "hour \"%d\" is invalid for the 12-hour clock" | msgstr "час \"%d\" не соответствует 12-часовому формату времени" |
| (ОЦЛ) | c:2389 | msgid "The given value did not match any of the allowed values for this field." | msgstr "Данное значение не соответствует ни одному из допустимых значений для этого \"поля.\"" |
| (ОЦЛ) | c:2266 | msgid "Value must be in the range %d to %d." | msgstr "Значение должно быть в интервале %d..%d." |
| (ОЦЛ) | c:2259 | msgid "Value must be an integer." | msgstr "Значение должно быть целым числом." |
| (ОЦЛ) | c:2244 c:2257 | msgid "invalid value \"%s\" for \"%s\"" | msgstr "неверное значение \"%s\" для \"%s\"" |
| (ОЦЛ) | c:2229 | msgid "source string too short for \"%s\" formatting field" | msgstr "входная строка короче, чем требует поле форматирования \"%s\"" |
| (ОЦЛ) | c:1392 | msgid "\"%s\" is not a number" | msgstr "\"%s\" не является числом" |
| (ОЦЛ) | c:488 | msgid "invalid format specification for an interval value" | msgstr "неправильная спецификация формата для целого числа" |
| (ОЦЛ) | c:125 c:51 c:61 | msgid "invalid input syntax for integer: \"%s\"" | msgstr "неверное значение для целого числа: \"%s\"" |
| (ОЦЛ) | l:1556 | #~ msgid "access method name cannot be qualified" | #~ msgstr "имя метода доступа не может быть составным" |
| (ОЦЛ) | l:1556 | #~ msgid "database name cannot be qualified" | #~ msgstr "имя базы данных не может быть составным" |
| (ОЦЛ) | l:1556 | #~ msgid "extension name cannot be qualified" | #~ msgstr "имя расширения не может быть составным" |
| (ОЦЛ) | l:1556 | #~ msgid "tablespace name cannot be qualified" | #~ msgstr "имя табличного пространства не может быть составным" |
| (ОЦЛ) | l:1556 | #~ msgid "role name cannot be qualified" | #~ msgstr "имя роли не может быть составным" |
| (ОЦЛ) | l:1556 | #~ msgid "schema name cannot be qualified" | #~ msgstr "имя схемы не может быть составным" |
| (ОЦЛ) | l:1556 | #~ msgid "language name cannot be qualified" | #~ msgstr "имя языка не может быть составным" |
| (ОЦЛ) | l:1556 | #~ msgid "foreign-data wrapper name cannot be qualified" | #~ msgstr "имя обертки сторонних данных не может быть составным" |
| (ОЦЛ) | l:1556 | #~ msgid "server name cannot be qualified" | #~ msgstr "имя сервера не может быть составным" |
| (ОЦЛ) | l:1556 | #~ msgid "event trigger name cannot be qualified" | #~ msgstr "имя событийного триггера не может быть составным" |
| (ОЦЛ) | l:1556 | #~ msgid "invalid input syntax for type real: \"%s\"" | #~ msgstr "неверный синтаксис для типа real: \"%s\"" |
| (ОЦЛ) | l:1556 | #~ msgid "invalid value for parameter \"replication\"" | #~ msgstr "неверное значение параметра \"replication\"" |
| (ОЦЛ) | l:1556 | #~ msgid "invalid symbol" | #~ msgstr "неверный символ" |
| (РСБ) | c:179 | msgid "invalid data in history file \"%s\"" | msgstr "неверные данные в файле истории \"%s\"" |
| (РСБ) | c:915 | msgid "%s: invalid datetoken tables, please fix\n" | msgstr "%s: ошибка в таблицах маркеров времени, требуется исправление\n" |

| | | | |
|-------|----------------|---|---|
| (PCB) | c:565 c:579 | msgid "could not create pipe for syslog: %m" | msgstr "не удалось создать канал для syslog: %m" |
| (PCB) | c:1102 | msgid "could not write to log file: %s\n" | msgstr "не удалось записать в файл протокола: %s\n" |
| (PCB) | c:1219 | msgid "could not open log file \"%s\": %m" | msgstr "не удалось открыть файл протокола \"%s\": %m" |
| (PCB) | c:630 | msgid "could not fork system logger: %m" | msgstr "не удалось породить процесс системного протоколирования: %m" |
| (PCB) | c:484 | msgid "invalid input syntax for numeric time zone: \"%s\"" | msgstr "неверный синтаксис для числового часового пояса: \"%s\"" |
| (PCB) | c:301 | msgid "invalid time zone file name \"%s\"" | msgstr "неправильное имя файла часовых поясов: \"%s\"" |

10. ДЕЙСТВИЯ ПОСЛЕ СБОЕВ И ОШИБОК ЭКСПЛУАТАЦИИ СУБД «JATOBA»

При эксплуатации СУБД «Jatoba» возможно возникновение следующих ошибок:

- сбой активации лицензии (п. 10.1);
- сбой инициализация расширения «securityprofile» (п. 10.3);
- ошибки создания пользователя (п. 10.4);
- ошибки, возникающие при использовании профиля парольных политик (п. 10.5);
- ошибка авторизации (п. 10.6).

10.1. Сбой активации лицензии

Типичными причинами сбоя активации лицензии могут быть:

- отсутствие доступа в сеть Интернет при онлайн активации лицензии;
- окончание срока действия лицензии.

При сбое активации лицензии появится ошибка «FATAL: license is invalid» в журнале приложений Windows (см. рисунок 10.1).

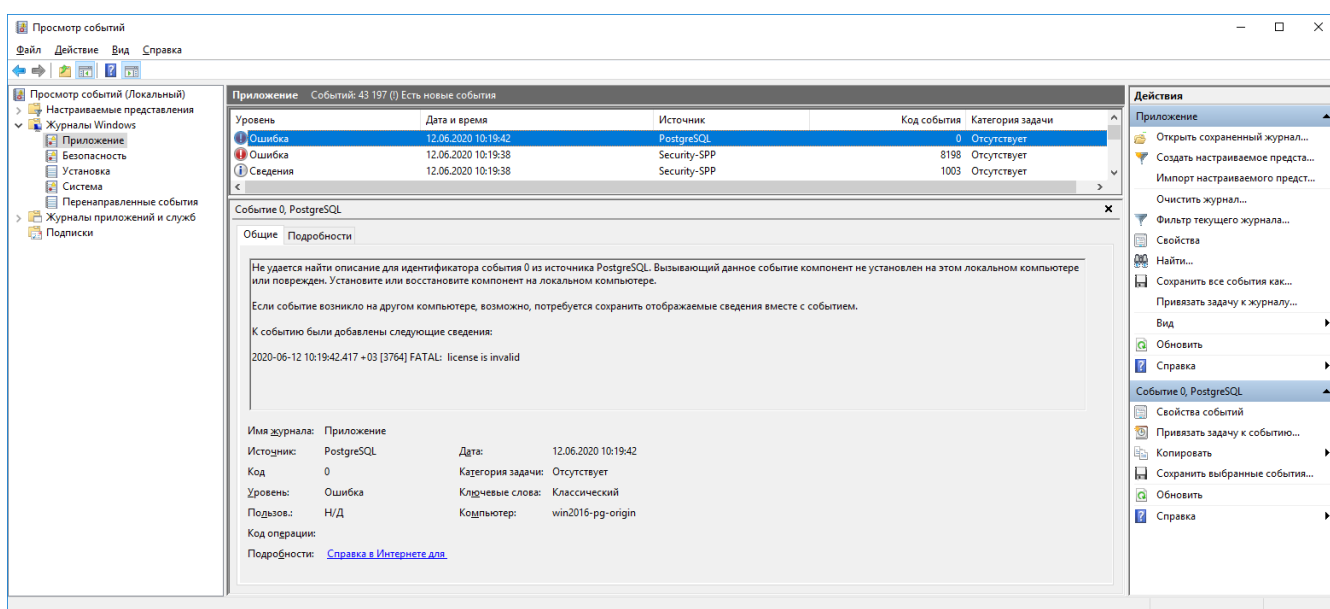


Рисунок 10.1 – Ошибка активации лицензии

При онлайн активации лицензии следует восстановить доступ сервера СУБД к сети Интернет, а также перезапустить службу JatobaServer (см. рисунок 10.2).

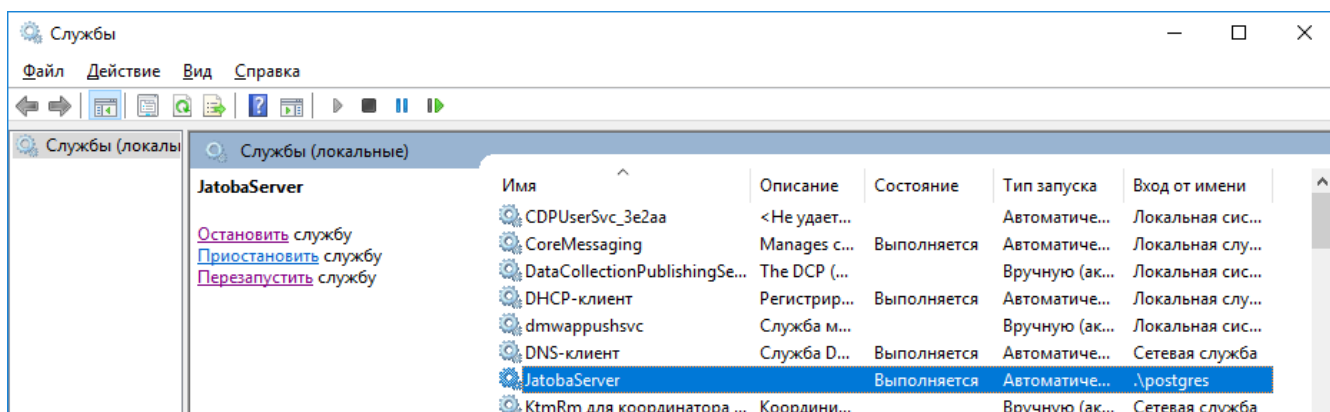


Рисунок 10.2 – Перезапуск службы JatobaServer

В случае окончания срока действия лицензии необходимо пройти повторную процедуру активации лицензии.

После чего перезапустить службу «JatobaServer» (см. рисунок 10.2).

10.2. Временная блокировка пользователей СУБД и суперпользователя

Ошибка может возникнуть если не были выполнены требования п. 6.1.2.2 настоящего документа.

```
Account must have password. Account locked temporary.
```

В случае когда временно заблокированы УЗ пользователей СУБД, следует выполнить действия описанные в п. 6.2.3.

Если же заблокирован пользователь «postgres», то порядок действий должен быть следующим:

- 1) Изменить метод аутентификации в конфигурационном файле «pg_hba.conf» на «TRUST»;
- 2) В файле конфигурационном файле «postgresql.conf» не отключать параметр:

```
shared_preload_libraries = 'securityprofile'
```

- 3) Перезапустить СУБД «Jatoba» командами:

- в ОС Windows:

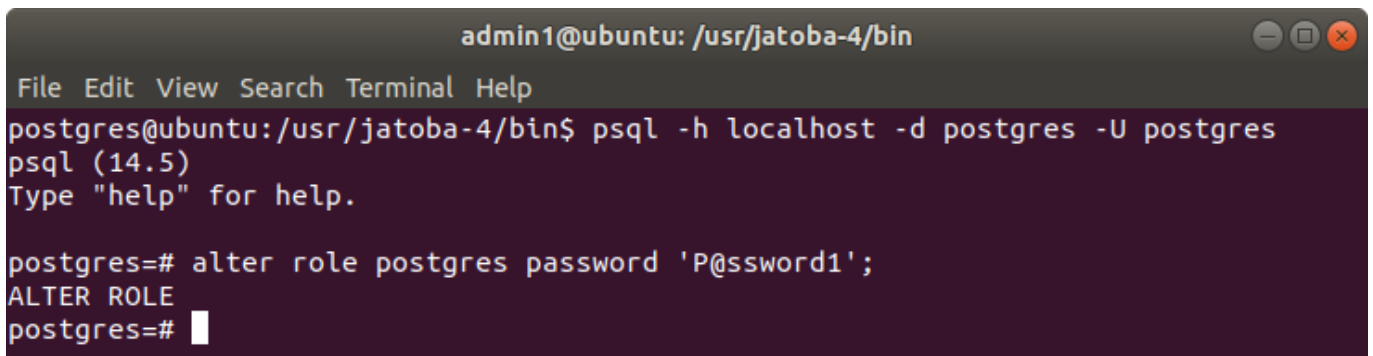
```
net stop JatobaServer  
net start JatobaServer
```

- в GNU Linux:

```
systemctl stop jatoba-4  
systemctl start jatoba-4  
systemctl status jatoba-4
```

4) Войти в СУБД от имени и с правами пользователя «postgres» и изменить пароль в СУБД при помощи команды:

```
alter role <имя учетной записи пользователя> password '<пароль  
пользователя>';
```



The screenshot shows a terminal window titled 'admin1@ubuntu: /usr/jatoba-4/bin'. The terminal output is as follows:

```
File Edit View Search Terminal Help  
postgres@ubuntu:/usr/jatoba-4/bin$ psql -h localhost -d postgres -U postgres  
psql (14.5)  
Type "help" for help.  
  
postgres=# alter role postgres password 'P@ssword1';  
ALTER ROLE  
postgres=#
```

Рисунок 10.3 – Смена пароля пользователя «postgres»

5) Изменить метод аутентификации в конфигурационном файле «pg_hba.conf» на «md5» или другой метод парольной аутентификации;

6) Перезапустить СУБД «Jatoba» командами:

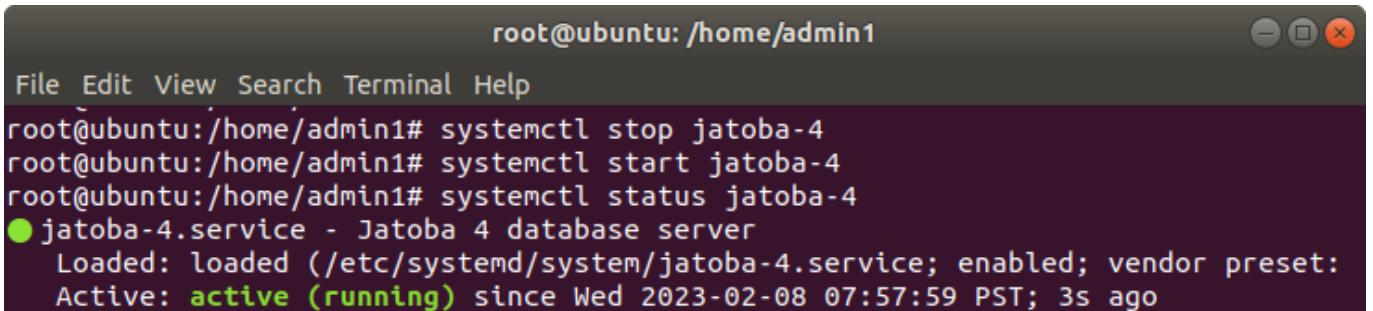
- в ОС Windows:

```
net stop JatobaServer  
net start JatobaServer
```

- в GNU Linux:

```
systemctl stop jatoba-4  
systemctl start jatoba-4
```

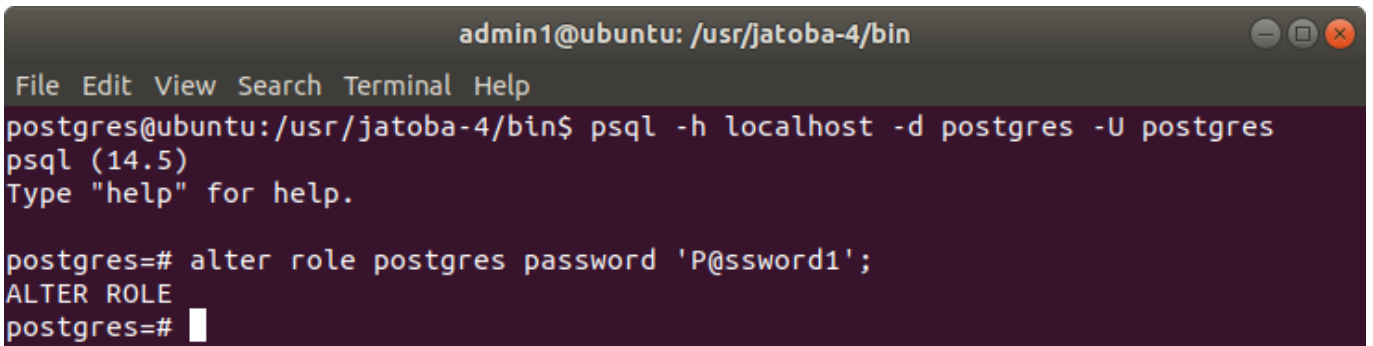
```
systemctl status jatoba-4
```



```
root@ubuntu: /home/admin1
File Edit View Search Terminal Help
root@ubuntu:/home/admin1# systemctl stop jatoba-4
root@ubuntu:/home/admin1# systemctl start jatoba-4
root@ubuntu:/home/admin1# systemctl status jatoba-4
● jatoba-4.service - Jatoba 4 database server
   Loaded: loaded (/etc/systemd/system/jatoba-4.service; enabled; vendor preset:
   Active: active (running) since Wed 2023-02-08 07:57:59 PST; 3s ago
```

Рисунок 10.4 – Перезапуск службы jatoba-4

- Проверить работоспособность СУБД, войдя от имени и с правами пользователя «postgres».



```
admin1@ubuntu: /usr/jatoba-4/bin
File Edit View Search Terminal Help
postgres@ubuntu:/usr/jatoba-4/bin$ psql -h localhost -d postgres -U postgres
psql (14.5)
Type "help" for help.

postgres=# alter role postgres password 'P@ssword1';
ALTER ROLE
postgres=#
```

Рисунок 10.5 – Аутентификация в СУБД пользователя «postgres»

10.3. Сбой инициализация расширения «securityprofile»

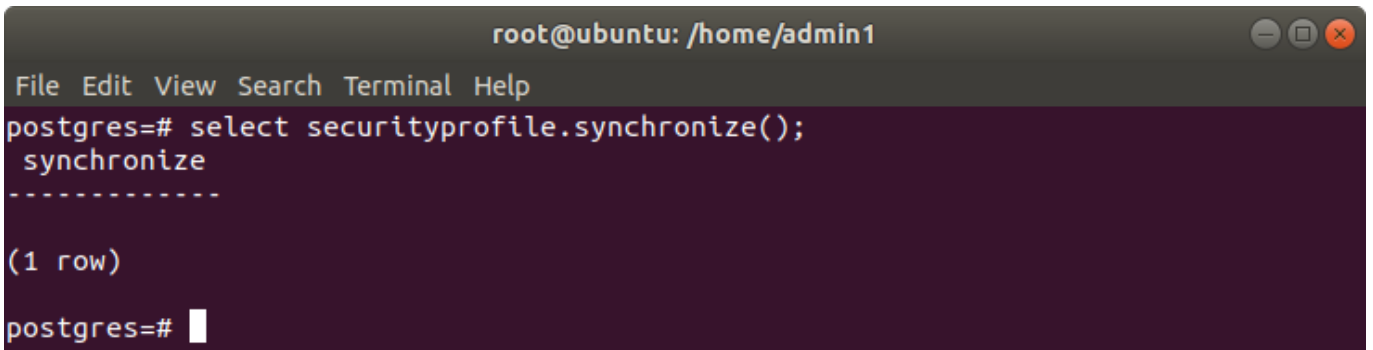
После перезагрузки сервера СУБД либо службы «JatobaServer» СУБД у пользователей, при авторизации может возникать ошибка:

```
«FATAL: Extension securityprofile need to be initialized by superuser.»
```

На процесс авторизации пользователей в СУБД данная ошибка не влияет.

Для устранения возникшей ошибки, следует повторно инициализировать расширение «SecurityProfile», выполнив команду:

```
select securityprofile.synchronize();
```



```
root@ubuntu: /home/admin1
File Edit View Search Terminal Help
postgres=# select securityprofile.synchronize();
synchronize
-----
(1 row)
postgres=#
```

Рисунок 10.6 – Команда выполнения инициализации расширения «SecurityProfile»

10.4. Ошибки создания пользователя

При попытке пользователя, обладающего привилегией создания ролей «Create roles», создать пользователя может возникнуть ошибка:

```
«permission denied for schema securityprofile»
```

Это означает, что у пользователя отсутствует доступ к схеме «securityprofile».

Для устранения ошибки следует предоставить права пользователю на использование схемы, выполнив команды:

```
GRANT CREATE ON SCHEMA securityprofile TO <имя пользователя>;
GRANT USAGE ON SCHEMA securityprofile TO <имя пользователя>;
```

После инициализации расширения «securityprofile» активируется парольная политика по умолчанию.

Пароль пользователя должен содержать:

- 1 символ в верхнем регистре;
- 1 символ в нижнем регистре;
- 1 спецсимвол.

10.5. Ошибки, возникающие при использовании профиля парольных политик «securityprofile»

Перечень ошибок, возникающих при использовании профиля парольных политик «securityprofile», приведен в таблице 10.1.

Таблица 10.1 – Перечень ошибок

| № | Текст ошибки | Перевод | Пути исправления |
|----|---|---|---|
| 1. | Schema (%s) does not exist. Probably extension (%s) is not created yet | Схема (<i>имя схемы</i>) не существует. Вероятно, расширение (<i>имя профиля</i>) еще не создано | Требуется установить расширение командой: <pre>create extension securityprofile;</pre> Подробно действия описаны в п.6.1.2 |
| 2. | Table (%s) does not exist. Probably extension (%s) is not created yet | Таблица (<i>имя таблицы</i>) не существует. Вероятно, расширение (<i>имя профиля</i>) еще не создано | Требуется установить расширение командой: <pre>create extension securityprofile;</pre> Подробно действия описаны в п.6.1.2 |
| 3. | Extension "securityprofile" has to be loaded using shared_preload_libraries | Расширение "securityprofile" должно быть загружено с помощью shared_preload_libraries | Для устранения ошибки в файле «postgresql.conf» прописать следующую строку: <pre>shared_preload_libraries = 'securityprofile'</pre> Подробно действия описаны в п.6.1.2 |
| 4. | You must be superuser to run this function | Вы должны быть суперпользователем, чтобы запустить эту функцию | Ошибка возникает при попытке с недостаточными привилегиями пользователя запустить функции управления расширениями, в том числе «securityprofile». Пользователю потребуется назначить дополнительные привилегии, в том числе на схему выполнив команды: <pre>GRANT CREATE ON SCHEMA securityprofile TO <имя пользователя>; GRANT USAGE ON SCHEMA securityprofile TO <имя пользователя>;</pre> |
| 5. | Failed login attempts limit exceeded | Превышен лимит неудачных попыток входа в систему | Пользователю следует подождать установленное |

| № | Текст ошибки | Перевод | Пути исправления |
|----|--|---|--|
| | | | время или обратиться к администратору |
| 6. | Password may not be reused. Try another | Пароль не может быть использован повторно. Попробовать другой | Сообщение возникает при нарушении парольной политики повторного использования пароля |
| 7. | Value of string's length should be between min_border and max_border | Значение длины строки должно быть между min_border и max_border | <p>Ошибка возникает, при:</p> <ul style="list-style-type: none"> • смене пароля пользователя; • создании или переименовании профиля и задании строки спецсимволов. <p>Длина введенной строки не удовлетворяет предустановленным границам расширения:</p> <ul style="list-style-type: none"> • имени от 1 до 32; • пароля от 6 до 256; • строки спецсимволов от 0 до 32 |
| 8. | New password must have at least (%d) changes. profile-> password_min_changes_count | Новый пароль должен иметь не менее (количество символов) изменений. profile -> password_min_changes_count | Сообщение возникает при нарушении политики количества изменений в пароле |
| 9. | User's password may not be changed right now. Password's minimim life time not expired yet | Пароль пользователя не может быть изменен прямо сейчас. Минимальное время жизни пароля еще не истекло | <p>В случае, когда инициализирован параметр «securityprofile.password_min_1 ife_time» и пользователю присвоен пароль начинается период в течение которого пароль должен использоваться и не может быть изменен.</p> <p>Соотношение временных параметров пароля подробно описано в п. 6.1.2.4.2, а параметры парольных политик приведены в таблице 6.1.</p> <p>В данном случае необходимо дождаться окончания минимального времени действия пароля, либо отключить параметр</p> |

| № | Текст ошибки | Перевод | Пути исправления |
|-----|---|--|---|
| | | | «securityprofile.password_min_l ife_time» |
| 10. | Password is too short | Пароль слишком короткий | Сообщение возникает при попытке установить пароль, который не соответствует значению минимального количества символов (securityprofile.minimum_length) |
| 11. | Password is too long | Пароль слишком длинный | Сообщение возникает при попытке установить пароль количество символов в котором превышает установленный параметр максимальной длины пароля (securityprofile.maximum_length) |
| 12. | Password must not contain user name | Пароль не должен содержать имя пользователя | Сообщение возникает при проверке содержания пароля. В теле пароля не должно быть указания имени пользователя |
| 13. | Password contains invalid characters | Пароль содержит недопустимые символы | Сообщение возникает, когда в пароле присутствуют специальные символы, не содержащиеся в справочнике специальных символов, заданных параметром «securityprofile.special_chars» |
| 14. | Extension (%)s need existent role to check it's new password. Call CREATE ROLE without PASSWORD part then use ALTER ROLE ... PASSWORD to set new password properly | Расширению требуется уже существующая роль, для проверки ее нового пароля. Выполните запрос CREATE ROLE без установки пароля. Затем выполните запрос ALTER ROLE для установки пароля | Ошибка возникает при создании пользователя с указанием пароля. Подробно создание пользователя в п.6.2.3 |
| 15. | Can not check password validity | Невозможно проверить валидность пароля | Ошибка связана с особенностью реализации парольных политик. Изменить |

| № | Текст ошибки | Перевод | Пути исправления |
|-----|--|--|---|
| | Password may be changed only by ALTER ROLE query | Пароль может быть изменен только запросом ALTER ROLE | пароль пользователя можно через команду ALTER ROLE |
| 16. | User must change password. Password grace time expired | Пользователь должен изменить пароль. Срок действия льготного пароля истек | Ошибка возникает при истечении срока действия пароля |
| 17. | User should change password. Password life time expired. Password still in use until grace time expired, so user may login on next try | Пользователь должен сменить пароль. Срок службы пароля истек. Пароль все еще используется до истечения льготного времени, поэтому пользователь может войти в систему при следующей попытке | Сообщение возникает при истечении срока действия пароля пользователя, если установлен параметр «securityprofile.password_grace_time» - время в секундах, в течение которого пользователь может использовать текущий пароль с напоминанием о необходимости его сменить до блокировки аккаунта. Время прибавляется к времени, установленному в securityprofile.password_life_time. Подробно взаимодействие параметров описано в пп. 6.1.2.4.1 |
| 18. | Account is locked forever | Учетная запись заблокирована навсегда | Учетную запись пользователя может разблокировать только Superuser. Ошибка возникает, если время блокировки установлено параметром «unlimited» (бесконечно) |
| 19. | Account is locked till. Try later unlock_date | Учетная запись пользователя заблокирована до «даты». Попробуйте позже «даты» | Учетную запись пользователя может разблокировать только Superuser. Ошибка возникает, если время блокировки установлено на определенный период времени |
| 20. | Extension "EXTENSION_NAME" need to be initialized by superuser | Расширение «securityprofile» должно быть инициализировано суперпользователем | Сообщение возникает при ошибке инициализации «securityprofile». Действия по |

| | | |
|--------------------|--------------------------|--------------------------|
| № изменения: _____ | Подпись отв. лица: _____ | Дата внесения изм: _____ |
|--------------------|--------------------------|--------------------------|

| № | Текст ошибки | Перевод | Пути исправления |
|-----|---|--|---|
| | Login as superuser and call "select securityprofile.synchronize() | Войдите в систему, как суперпользователь и вызовите команду select securityprofile.synchronize () | исправлению описаны в подразделе 10.3 |
| 21. | Value should be between min_border and max_border | Значение должно быть между min_border и max_border | Ошибка возникает при установке значений профиля. В данном случае устанавливаемые параметры выходят за предустановленные границы |
| 22. | Password minimum length can not be larger than maximum length, default_profile.password_max_len | Минимальная длина пароля не может быть больше максимальной длины, default_profile.password_max_len | Ошибка возникает при создании профиля для групп пользователей «securityprofile», если ошибочно были указаны противоречивые параметры, где минимальная длина пароля более максимальной длины |
| 23. | Password maximum length can not be lesser than minimum length, default_profile.password_min_len | Максимальная длина пароля не может быть меньше минимальной длины, default_profile.password_min_len | Ошибка возникает при создании профиля для групп пользователей «securityprofile», если ошибочно были указаны противоречивые параметры, где максимальная длина пароля менее минимальной длины |
| 24. | Default profile already exist. Specified name used by default profile | Профиль по умолчанию уже существует. Указанное имя используется профиль по умолчанию | Ошибка возникает при создании одноименного профиля существующему профилю securityprofile (default) |
| 25. | Profile already exist | Профиль (имя профиля) уже существует | Ошибка может возникать при указании имени нового профиля, совпадающего с уже существующим профилем securityprofile |
| 26. | Default profile can not be removed | Профиль по умолчанию не может быть удален | Поскольку securityprofile (default) является базовым |

| № | Текст ошибки | Перевод | Пути исправления |
|-----|--|---|--|
| | | | профилем, то его нельзя удалить |
| 27. | Profile have binded users | Профиль (имя профиля) имеет привязанных пользователей | Сообщение появляется при попытке удалить профайл с привязанными к нему пользователями. Для исправления ошибки необходимо перепривязать пользователей, выполнив команду select (имя схемы) bind_profile ('имя_профиля', 'имя_пользователя'). Команды управления профилями приведены в таблице 6.11 |
| 28. | Default profile can not be changed with function call | Профиль по умолчанию не может быть изменен с помощью вызова функции | Профиль по умолчанию не может быть изменен стандартными функциями. Изменения допустимы через редактирование конфигурационного файла postgresql.conf |
| 29. | Profile name already in use, new_profile_name | Имя профиля (имя профиля) уже используется | Используйте другое имя создаваемого профиля |
| 30. | Password minimum length can not be larger than maximum length, profile->password_max_len | Минимальная длина пароля не может быть больше максимальной длины, profile ->password_max_len) | Сообщение об ошибке возникает при формировании профиля для групп пользователей, при установлении длины пароля. Следует присвоить минимальной длине пароля (password_min_len) значение, которое не будет превышать ранее заданную максимальную длину пароля (password_max_len) |
| 31. | Password maximum length can not be lesser than minimum length, profile->password_min_len | Максимальная длина пароля не может быть меньше минимальной длины, profile ->password_min_len | Сообщение об ошибке возникает при формировании профиля для групп пользователей, при |

| № | Текст ошибки | Перевод | Пути исправления |
|-----|--|---|--|
| | | | установлении максимальной длины пароля. Следует присвоить максимальное значение длины пароля (password_max_len), превышающее ранее заданное значение минимальной длины пароля (password_min_len) |
| 32. | Shared buffer hash table corrupted(profiles) | Общая буферная хэш-таблица повреждена (<i>имя профиля</i>) | Ошибки связаны с системным сбоем. Для их устранения рекомендуется: <ul style="list-style-type: none"> • провести тестирование оперативной памяти; • перезагрузить СУБД; • восстановить БД из резервной копии |
| 33. | Password encryption failed | Ошибка шифрования пароля | |
| 34. | Cache entry does not exist | Запись в кэше не существует | |
| 35. | Cache synchronization failed for background worker of securityprofile. Extension not installed | Фоновый процесс не может выполнить синхронизацию, расширение не установлено | Указать в файле PostgreSQL.conf параметр securityprofile.db_name = 'dbname' и/или установить расширение securityprofile в БД dbname |

10.6. Ошибка авторизации

Ошибка авторизации в psql после установки СУБД «Jatoba» с настройками СУБД: "Язык и регион: English_USA" и "Кодировка: WIN1252" на английскую версию ОС Windows Server с выбранными при установке параметрами: "Time and currency format: Russian (Russia)" и "Keyboard or input method: Russian".

- 1) Запустить cmd.exe.
- 2) Выполнить:

```
psql -U postgres;
```

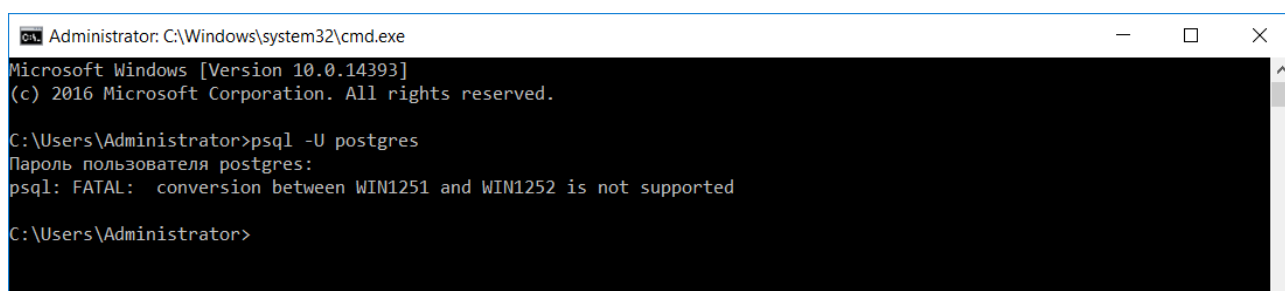
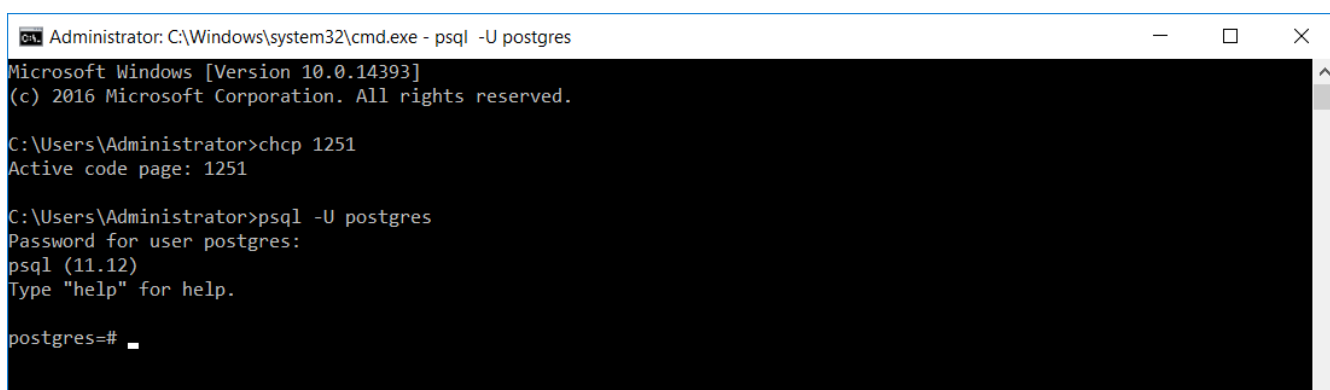


Рисунок 10.7 – Окно командной строки с ошибкой

| | | |
|--------------------|--------------------------|--------------------------|
| № изменения: _____ | Подпись отв. лица: _____ | Дата внесения изм: _____ |
|--------------------|--------------------------|--------------------------|

- 3) Решение ошибки:
- перейти в панель управления (control panel);
 - затем перейти в "Clock, Language, and Region/Language";
 - нажать "Advanced settings";
 - в секции "Override for Windows display language" выбрать "English (United Stated)";
 - нажать "Save";
 - снова запустить cmd.exe;
 - ввести: chcp 1251;
 - повторить вход в psql.



```
Administrator: C:\Windows\system32\cmd.exe - psql -U postgres
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>chcp 1251
Active code page: 1251

C:\Users\Administrator>psql -U postgres
Password for user postgres:
psql (11.12)
Type "help" for help.

postgres=#
```

Рисунок 10.8 – Окно командной строки без ошибок

10.7. Контактные данные службы технической поддержки

При невозможности самостоятельно решить возникшие трудности с СУБД «Jatoba» следует обратиться в службу технической поддержки ООО «Газинформсервис».

Таблица 10.2 – Контактные данные службы технической поддержки

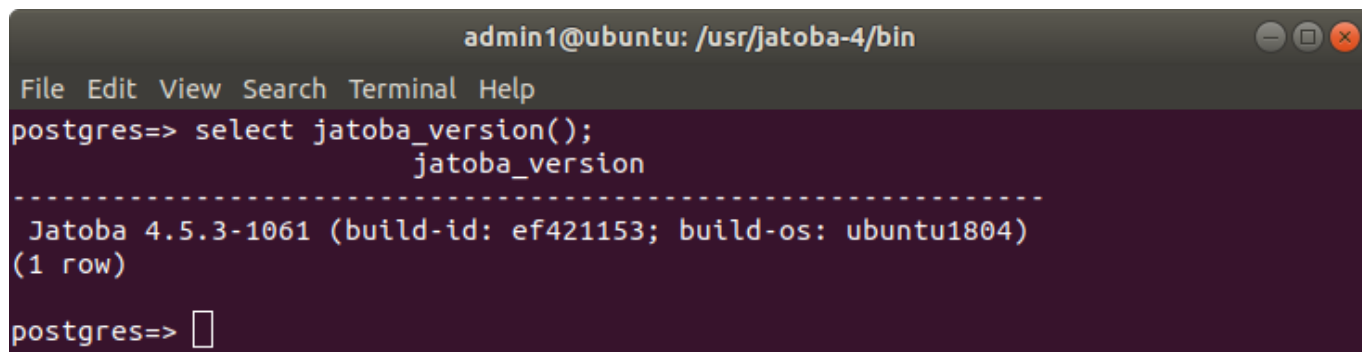
| | |
|----------|---|
| Телефон | 8 (800) 700-09-87 |
| Web-сайт | https://www.gaz-is.ru/poddergka/zajavka.html#produkty |
| E-mail | support@gaz-is.ru |

10.7.1. Версия изделия

Для скорейшего решения вопроса, рекомендуется сообщить в службу технической поддержки точную версию установленного экземпляра изделия.

Версию изделия можно узнать, выполнив команду:

```
select jatoba_version();
```



```
admin1@ubuntu: /usr/jatoba-4/bin
File Edit View Search Terminal Help
postgres=> select jatoba_version();
                jatoba_version
-----
Jatoba 4.5.3-1061 (build-id: ef421153; build-os: ubuntu1804)
(1 row)
postgres=> □
```

Рисунок 10.9 – Команда запроса версии изделия

ПРИЛОЖЕНИЕ 1

(обязательное)

Значение полей из файла pg_hba.conf

Значение поля «TYPE» представлены в таблице 1.1.

Таблица 1.1.1 – Значение поля «TYPE»

| Значение поля | Описание |
|--|--|
| local | Сопоставляет попытки подключения с использованием Unix-сокетов. Без данной записи все соединения через Unix-сокеты будут запрещены. Данное поле не работает в ОС Windows Server |
| host ¹⁾ | Соответствует попыткам подключения, выполненным с использованием TCP/IP. Записи хоста соответствуют попыткам подключения SSL или без SSL |
| hostssl | Соответствует попыткам подключения, выполненным с использованием TCP/IP и шифрованием SSL |
| hostnossl | Соответствует попыткам подключения, выполненным с использованием TCP/IP (без шифрования ssl) |
| ¹⁾ Удаленное соединение TCP/IP будут невозможны, если сервер не запущен с подходящим значением для параметра конфигурации listen_addresses, поскольку по умолчанию выполняется прослушивание соединений TCP/IP только на локальном кольцевом адресе localhost | |

Поле «DATABASE» указывает, какие имена баз данных соответствует данной строки. Значение поля «DATABASE» представлены в таблице 1.2.

Таблица 1.1.2 – Значение поля «DATABASE»

| Значение поля | Описание |
|---------------|--|
| all | Указывает, что данная строка относится ко всем базам данных |
| sameuser | Указывает, что данная строка соответствует тому, что запрашиваемая база имеет то же имя, что и запрашиваемый пользователь |
| samerole | Указывает, что данная строка соответствует тому, что запрашиваемый пользователь должен быть членом роли с тем же именем, что и запрошенная база данных. Суперпользователи не считаются членами роли для целей samerole, если они не являются явными членами роли, прямо или косвенно |
| replication | Значение replication указывает, что запрашивается подключение репликации (в этом случае конкретная база данных не указывается) |

Поле «USER» указывает, что данная строка соответствует конкретному имени пользователя. Значение all указывает, что оно соответствует всем пользователям. Можно указать несколько имен пользователей, разделяя их запятыми.

Поле «ADDRESS» указывает, что данная строка соответствует адресу клиентской машины. Данное поле может содержать имя хоста или диапазон IP-адресов, или одно из нижеупомянутых ключевых слов. Диапазон IP-адресов указывается с использованием стандартных числовых обозначений для начального адреса диапазона, затем косой черты (/)

| | | |
|--------------------|--------------------------|--------------------------|
| № изменения: _____ | Подпись отв. лица: _____ | Дата внесения изм: _____ |
|--------------------|--------------------------|--------------------------|

и длины маски CIDR. Длина маски указывает количество старших битов IP-адреса клиента, которые должны совпадать. Биты справа от этого должны быть равны нулю в данном IP-адресе. Между IP-адресом, / и длиной маски CIDR не должно быть пробелов. Запись в формате IPv4 будет соответствовать только соединениям IPv4, а запись в формате IPv6 будет соответствовать только соединениям IPv6, даже если представленный адрес находится в диапазоне IPv4-in-IPv6.

Поле «IP-адрес IP-маска» используется в качестве альтернативы IP-адрес / длина маски. Вместо указания длины маски фактическая маска указывается в отдельном столбце. Например, 255.0.0.0 представляет длину маски CIDR IPv4 8, а 255.255.255.255 представляет длину маски CIDR 32.

Поле «METHOD» определяет, что данная строка будет осуществлять соединение по этому методу аутентификации. Значение поля «METHOD» представлены в таблице 1.3.

Таблица 1.1.3 – Значение поля «METHOD»

| Значение поля | Описание |
|----------------------|---|
| md5 | Аутентификация осуществляется по паролю. По каналу связи передается пароль в виде хеша MD5. |
| password | Аутентификация осуществляется по паролю. Пароль передается в открытом виде. |

ПРИЛОЖЕНИЕ 2

Перечень событий СУБД с распределением по категориям безопасности

Таблица П.2.1 – Перечень событий СУБД с распределением по категориям безопасности

| Категория события/ Класс события | Код события | Название условия |
|--|--------------------------|---|
| Class 00 - Successful Completion | | |
| Управление данными | 00000 | ERRCODE SUCCESSFUL COMPLETION |
| Class 01 - Warning | | |
| Управление данными | 01000 | ERRCODE WARNING |
| Управление данными | 0100C | ERRCODE WARNING DYNAMIC RESULT SETS RETURNED |
| Управление данными | 01008 | ERRCODE WARNING IMPLICIT ZERO BIT PADDING |
| Управление данными | 01003 | ERRCODE WARNING NULL VALUE ELIMINATED IN SET FUNCTION |
| Управление доступом | 01007 | ERRCODE WARNING PRIVILEGE NOT GRANTED |
| Управление доступом | 01006 | ERRCODE WARNING PRIVILEGE NOT REVOKED |
| Управление данными | 01004 | ERRCODE WARNING STRING DATA RIGHT TRUNCATION |
| Управление данными | 01P01 | ERRCODE WARNING DEPRECATED FEATURE |
| Class 02 - No Data | | |
| Управление данными | 02000 | ERRCODE NO DATA |
| Управление данными | 02001 | ERRCODE NO ADDITIONAL DYNAMIC RESULT SETS RETURNED |
| Class 03 - SQL Statement Not Yet Complete | | |
| Управление данными | 03000 | ERRCODE SQL STATEMENT NOT YET COMPLETE |
| Class 08 - Connection Exception | | |
| Управление доступом | 08000 | ERRCODE CONNECTION EXCEPTION |
| Управление доступом | 08003 | ERRCODE CONNECTION DOES NOT EXIST |
| Управление доступом | 08006 | ERRCODE CONNECTION FAILURE |
| Управление доступом | 08001 | ERRCODE SQLCLIENT UNABLE TO ESTABLISH SQLCONNECTION |
| Управление доступом | 08004 | ERRCODE SQLSERVER REJECTED ESTABLISHMENT OF SQLCONNECTION |
| Управление доступом | 08007 | ERRCODE TRANSACTION RESOLUTION UNKNOWN |
| Управление доступом | 08P01 | ERRCODE PROTOCOL VIOLATION |
| Class 09 - Triggered Action Exception | | |
| Управление данными | 09000 | ERRCODE TRIGGERED ACTION EXCEPTION |
| Class 0A - Feature Not Supported | | |
| Управление данными | 0A000 | ERRCODE FEATURE NOT SUPPORTED |
| Class 0B - Invalid Transaction Initiation | | |
| Управление данными | 0B000 | ERRCODE INVALID TRANSACTION INITIATION |
| Class 0F - Locator Exception | | |
| Прочее | 0F000 | ERRCODE LOCATOR EXCEPTION |
| Прочее | 0F001 | ERRCODE L E INVALID SPECIFICATION |
| Class 0L - Invalid Grantor | | |
| Управление доступом | 0L000 | ERRCODE INVALID GRANTOR |
| Управление доступом | 0LP01 | ERRCODE INVALID GRANT OPERATION |
| Class 0P - Invalid Role Specification | | |
| Управление доступом | 0P000 | ERRCODE INVALID ROLE SPECIFICATION |
| Class 0Z - Diagnostics Exception | | |
| Управление данными | 0Z000 | ERRCODE DIAGNOSTICS EXCEPTION |
| № изменения: _____ | Подпись отв. лица: _____ | Дата внесения изм: _____ |

| Категория события/ Класс события | Код события | Название условия |
|---|----------------|---|
| Управление данными | 0Z002 | ERRCODE STACKED DIAGNOSTICS ACCESSED WITHOUT ACTIVE HANDLER |
| Class 20 - Case Not Found | | |
| Управление данными | 20000 | ERRCODE CASE NOT FOUND |
| Class 21 - Cardinality Violation | | |
| Прочее | 21000 | ERRCODE CARDINALITY VIOLATION |
| Class 22 - Data Exception | | |
| Управление данными | 22000 | ERRCODE DATA EXCEPTION |
| Управление данными | 2202E | ERRCODE ARRAY SUBSCRIPT ERROR |
| Управление данными | 22021 | ERRCODE CHARACTER NOT IN REPERTOIRE |
| Управление данными | 22008 | ERRCODE DATETIME FIELD OVERFLOW |
| Контроль целостности | 22008 | ERRCODE DATETIME VALUE OUT OF RANGE |
| Управление данными | 2202 | ERRCODE ARRAY ELEMENT ERROR |
| Управление данными | 22012 | ERRCODE DIVISION BY ZERO |
| Управление данными | 22005 | ERRCODE ERROR IN ASSIGNMENT |
| Управление данными | 2200B | ERRCODE ESCAPE CHARACTER CONFLICT |
| Управление данными | 22022 | ERRCODE INDICATOR OVERFLOW |
| Управление данными | 22015 | ERRCODE INTERVAL FIELD OVERFLOW |
| Управление данными | 2201E | ERRCODE INVALID ARGUMENT FOR LOG |
| Управление данными | 22013 | ERRCODE INVALID PRECEDING OR FOLLOWING SIZE |
| Управление данными | 22014 | ERRCODE INVALID ARGUMENT FOR NTILE |
| Управление данными | 22016 | ERRCODE INVALID ARGUMENT FOR NTH VALUE |
| Управление данными | 2201F | ERRCODE INVALID ARGUMENT FOR POWER FUNCTION |
| Управление данными | 2201G | ERRCODE INVALID ARGUMENT FOR WIDTH BUCKET FUNCTION |
| Управление данными | 22018 | ERRCODE INVALID CHARACTER VALUE FOR CAST |
| Управление данными | 22007 | ERRCODE INVALID DATETIME FORMAT |
| Управление данными | 22019 | ERRCODE INVALID ESCAPE CHARACTER |
| Управление данными | 2200D | ERRCODE INVALID ESCAPE OCTET |
| Управление данными | 22025 | ERRCODE INVALID ESCAPE SEQUENCE |
| Управление данными | 22P06 | ERRCODE NONSTANDARD USE OF ESCAPE CHARACTER |
| Управление данными | 22010 | ERRCODE INVALID INDICATOR PARAMETER VALUE |
| Управление данными | 22023 | ERRCODE INVALID PARAMETER VALUE |
| Управление данными | 2201B | ERRCODE INVALID REGULAR EXPRESSION |
| Управление данными | 2201W | ERRCODE INVALID ROW COUNT IN LIMIT CLAUSE |
| Управление данными | 2201X | ERRCODE INVALID ROW COUNT IN RESULT OFFSET CLAUSE |
| Управление данными | 2202H | ERRCODE INVALID TABLESAMPLE ARGUMENT |
| Управление данными | 2202G | ERRCODE INVALID TABLESAMPLE REPEAT |
| Управление данными | 22009 | ERRCODE INVALID TIME ZONE DISPLACEMENT VALUE |
| Управление данными | 2200C | ERRCODE INVALID USE OF ESCAPE CHARACTER |
| Управление данными | 2200G | ERRCODE MOST SPECIFIC TYPE MISMATCH |
| Управление данными | 22004 | ERRCODE NULL VALUE NOT ALLOWED |
| Управление данными | 22002 | ERRCODE NULL VALUE NO INDICATOR PARAMETER |
| Управление данными | 22003 | ERRCODE NUMERIC VALUE OUT OF RANGE |
| Управление данными | 22026 | ERRCODE STRING DATA LENGTH MISMATCH |
| Управление данными | 22001 | ERRCODE STRING DATA RIGHT TRUNCATION |
| Управление данными | 22011 | ERRCODE SUBSTRING ERROR |
| Управление данными | 22027 | ERRCODE TRIM ERROR |
| Управление данными | 22024 | ERRCODE UNTERMINATED C STRING |
| Управление данными | 2200F | ERRCODE ZERO LENGTH CHARACTER STRING |
| Управление данными | 22P01 | ERRCODE FLOATING POINT EXCEPTION |

№ изменения: _____ Подпись отв. лица: _____ Дата внесения изм: _____

| Категория события/ Класс события | Код события | Название условия |
|--|----------------|--|
| Управление данными | 22P02 | ERRCODE INVALID TEXT REPRESENTATION |
| Управление данными | 22P03 | ERRCODE INVALID BINARY REPRESENTATION |
| Управление данными | 22P04 | ERRCODE BAD COPY FILE FORMAT |
| Управление данными | 22P05 | ERRCODE UNTRANSLATABLE CHARACTER |
| Управление данными | 2200L | ERRCODE NOT AN XML DOCUMENT |
| Управление данными | 2200M | ERRCODE INVALID XML DOCUMENT |
| Управление данными | 2200N | ERRCODE INVALID XML CONTENT |
| Управление данными | 2200S | ERRCODE INVALID XML COMMENT |
| Управление данными | 2200T | ERRCODE INVALID XML PROCESSING INSTRUCTION |
| Управление данными | 2200H | ERRCODE SEQUENCE GENERATOR LIMIT EXCEEDED |
| Управление данными | 22030 | ERRCODE DUPLICATE JSON OBJECT KEY VALUE |
| Управление данными | 22031 | ERRCODE INVALID ARGUMENT FOR SQL JSON DATETIME FUNCTION |
| Управление данными | 22032 | ERRCODE INVALID JSON TEXT |
| Управление данными | 22033 | ERRCODE INVALID SQL JSON SUBSCRIPT |
| Управление данными | 22034 | ERRCODE MORE THAN ONE SQL JSON ITEM |
| Управление данными | 22035 | ERRCODE NO SQL JSON ITEM |
| Управление данными | 22036 | ERRCODE NON NUMERIC SQL JSON ITEM |
| Управление данными | 22037 | ERRCODE NON UNIQUE KEYS IN A JSON OBJECT |
| Управление данными | 22038 | ERRCODE SINGLETON SQL JSON ITEM REQUIRED |
| Управление данными | 22039 | ERRCODE SQL JSON ARRAY NOT FOUND |
| Управление данными | 2203A | ERRCODE SQL JSON MEMBER NOT FOUND |
| Управление данными | 2203B | ERRCODE SQL JSON NUMBER NOT FOUND |
| Управление данными | 2203C | ERRCODE SQL JSON OBJECT NOT FOUND |
| Управление данными | 2203D | ERRCODE TOO MANY JSON ARRAY ELEMENTS |
| Управление данными | 2203E | ERRCODE TOO MANY JSON OBJECT MEMBERS |
| Управление данными | 2203F | ERRCODE SQL JSON SCALAR REQUIRED |
| Class 23 - Integrity Constraint Violation | | |
| Контроль целостности | 23000 | ERRCODE INTEGRITY CONSTRAINT VIOLATION |
| Контроль целостности | 23001 | ERRCODE RESTRICT VIOLATION |
| Контроль целостности | 23502 | ERRCODE NOT NULL VIOLATION |
| Контроль целостности | 23503 | ERRCODE FOREIGN KEY VIOLATION |
| Контроль целостности | 23505 | ERRCODE UNIQUE VIOLATION |
| Контроль целостности | 23514 | ERRCODE CHECK VIOLATION |
| Контроль целостности | 23P01 | ERRCODE EXCLUSION VIOLATION |
| Class 24 - Invalid Cursor State | | |
| Прочее | 24000 | ERRCODE INVALID CURSOR STATE |
| Class 25 - Invalid Transaction State | | |
| Управление данными | 25000 | ERRCODE INVALID TRANSACTION STATE |
| Управление данными | 25001 | ERRCODE ACTIVE SQL TRANSACTION |
| Управление данными | 25002 | ERRCODE BRANCH TRANSACTION ALREADY ACTIVE |
| Управление данными | 25008 | ERRCODE HELD CURSOR REQUIRES SAME ISOLATION LEVEL |
| Управление данными | 25003 | ERRCODE INAPPROPRIATE ACCESS MODE FOR BRANCH TRANSACTION |
| Управление данными | 25004 | ERRCODE INAPPROPRIATE ISOLATION LEVEL FOR BRANCH TRANSACTION |
| Управление данными | 25005 | ERRCODE NO ACTIVE SQL TRANSACTION FOR BRANCH TRANSACTION |
| Управление данными | 25006 | ERRCODE READ ONLY SQL TRANSACTION |
| Управление данными | 25007 | ERRCODE SCHEMA AND DATA STATEMENT MIXING NOT SUPPORTED |

№ изменения: _____ Подпись отв. лица: _____ Дата внесения изм: _____

| Категория события/ Класс события | Код события | Название условия |
|---|----------------|---|
| Управление данными | 25P01 | ERRCODE NO ACTIVE SQL TRANSACTION |
| Управление данными | 25P02 | ERRCODE IN FAILED SQL TRANSACTION |
| Управление данными | 25P03 | ERRCODE IDLE IN TRANSACTION SESSION TIMEOUT |
| Class 26 - Invalid SQL Statement Name | | |
| Управление данными | 26000 | ERRCODE INVALID SQL STATEMENT NAME |
| Class 27 - Triggered Data Change Violation | | |
| Управление доступом | 27000 | ERRCODE TRIGGERED DATA CHANGE VIOLATION |
| Class 28 - Invalid Authorization Specification | | |
| Идентификация | 28000 | ERRCODE INVALID AUTHORIZATION SPECIFICATION |
| Идентификация | 28P01 | ERRCODE INVALID PASSWORD |
| Class 2B - Dependent Privilege Descriptors Still Exist | | |
| Управление доступом | 2B000 | ERRCODE DEPENDENT PRIVILEGE DESCRIPTORS STILL EXIST |
| Управление доступом | 2BP01 | ERRCODE DEPENDENT OBJECTS STILL EXIST |
| Class 2D - Invalid Transaction Termination | | |
| Управление данными | 2D000 | ERRCODE INVALID TRANSACTION TERMINATION |
| Class 2F - SQL Routine Exception | | |
| Управление доступом | 2F000 | ERRCODE SQL ROUTINE EXCEPTION |
| Управление доступом | 2F005 | ERRCODE S R E FUNCTION EXECUTED NO RETURN STATEMENT |
| Управление доступом | 2F002 | ERRCODE S R E MODIFYING SQL DATA NOT PERMITTED |
| Управление доступом | 2F003 | ERRCODE S R E PROHIBITED SQL STATEMENT ATTEMPTED |
| Управление доступом | 2F004 | ERRCODE S R E READING SQL DATA NOT PERMITTED |
| Class 34 - Invalid Cursor Name | | |
| Прочее | 34000 | ERRCODE INVALID CURSOR NAME |
| Class 38 - External Routine Exception | | |
| Управление доступом | 38000 | ERRCODE EXTERNAL ROUTINE EXCEPTION |
| Управление доступом | 38001 | ERRCODE E R E CONTAINING SQL NOT PERMITTED |
| Управление доступом | 38002 | ERRCODE E R E MODIFYING SQL DATA NOT PERMITTED |
| Управление доступом | 38003 | ERRCODE E R E PROHIBITED SQL STATEMENT ATTEMPTED |
| Управление доступом | 38004 | ERRCODE E R E READING SQL DATA NOT PERMITTED |
| Class 39 - External Routine Invocation Exception | | |
| Управление данными | 39000 | ERRCODE EXTERNAL ROUTINE INVOCATION EXCEPTION |
| Управление данными | 39001 | ERRCODE E R I E INVALID SQLSTATE RETURNED |
| Управление данными | 39004 | ERRCODE E R I E NULL VALUE NOT ALLOWED |
| Управление данными | 39P01 | ERRCODE E R I E TRIGGER PROTOCOL VIOLATED |
| Управление данными | 39P02 | ERRCODE E R I E SRF PROTOCOL VIOLATED |
| Управление данными | 39P03 | ERRCODE E R I E EVENT TRIGGER PROTOCOL VIOLATED |
| Class 3B - Savepoint Exception | | |
| Резервное копирование | 3B000 | ERRCODE SAVEPOINT EXCEPTION |
| Резервное копирование | 3B001 | ERRCODE S E INVALID SPECIFICATION |
| Class 3D - Invalid Catalog Name | | |
| Прочее | 3D000 | ERRCODE INVALID CATALOG NAME |
| Class 3F - Invalid Schema Name | | |
| Управление данными | 3F000 | ERRCODE INVALID SCHEMA NAME |
| Class 40 - Transaction Rollback | | |
| Управление данными | 40000 | ERRCODE TRANSACTION ROLLBACK |
| Управление данными | 40002 | ERRCODE T R INTEGRITY CONSTRAINT VIOLATION |
| Управление данными | 40001 | ERRCODE T R SERIALIZATION FAILURE |

№ изменения: _____ Подпись отв. лица: _____ Дата внесения изм: _____

| Категория события/ Класс события | Код события | Название условия |
|---|----------------|---|
| Управление данными | 40003 | ERRCODE T R STATEMENT COMPLETION UNKNOWN |
| Управление данными | 40P01 | ERRCODE T R DEADLOCK DETECTED |
| Class 42 - Syntax Error or Access Rule Violation | | |
| Управление доступом | 42000 | ERRCODE SYNTAX ERROR OR ACCESS RULE VIOLATION |
| Управление данными | 42601 | ERRCODE SYNTAX ERROR |
| Управление доступом | 42501 | ERRCODE INSUFFICIENT PRIVILEGE |
| Управление доступом | 42846 | ERRCODE CANNOT COERCE |
| Управление доступом | 42803 | ERRCODE GROUPING ERROR |
| Управление данными | 42P20 | ERRCODE WINDOWING ERROR |
| Управление данными | 42P19 | ERRCODE INVALID RECURSION |
| Идентификация | 42830 | ERRCODE INVALID FOREIGN KEY |
| Управление данными | 42602 | ERRCODE INVALID NAME |
| Управление данными | 42622 | ERRCODE NAME TOO LONG |
| Управление данными | 42939 | ERRCODE RESERVED NAME |
| Контроль целостности данных | 42804 | ERRCODE DATATYPE MISMATCH |
| Контроль целостности данных | 42P18 | ERRCODE INDETERMINATE DATATYPE |
| Управление данными | 42P21 | ERRCODE COLLATION MISMATCH |
| Управление данными | 42P22 | ERRCODE INDETERMINATE COLLATION |
| Контроль целостности данных | 42809 | ERRCODE WRONG OBJECT TYPE |
| Управление данными | 428C9 | ERRCODE GENERATED ALWAYS |
| Управление данными | 42703 | ERRCODE UNDEFINED COLUMN |
| Управление данными | 42883 | ERRCODE UNDEFINED FUNCTION |
| Управление данными | 42P01 | ERRCODE UNDEFINED TABLE |
| Управление данными | 42P02 | ERRCODE UNDEFINED PARAMETER |
| Управление данными | 42704 | ERRCODE UNDEFINED OBJECT |
| Управление данными | 42701 | ERRCODE DUPLICATE COLUMN |
| Управление данными | 42P03 | ERRCODE DUPLICATE CURSOR |
| Управление данными | 42P04 | ERRCODE DUPLICATE DATABASE |
| Управление данными | 42723 | ERRCODE DUPLICATE FUNCTION |
| Управление данными | 42P05 | ERRCODE DUPLICATE PSTATEMENT |
| Управление данными | 42P06 | ERRCODE DUPLICATE SCHEMA |
| Управление данными | 42P07 | ERRCODE DUPLICATE TABLE |
| Управление данными | 42712 | ERRCODE DUPLICATE ALIAS |
| Управление данными | 42710 | ERRCODE DUPLICATE OBJECT |
| Управление данными | 42702 | ERRCODE AMBIGUOUS COLUMN |
| Управление данными | 42725 | ERRCODE AMBIGUOUS FUNCTION |
| Управление данными | 42P08 | ERRCODE AMBIGUOUS PARAMETER |
| Управление данными | 42P09 | ERRCODE AMBIGUOUS ALIAS |
| Управление данными | 42P10 | ERRCODE INVALID COLUMN REFERENCE |
| Управление данными | 42611 | ERRCODE INVALID COLUMN DEFINITION |
| Управление данными | 42P11 | ERRCODE INVALID CURSOR DEFINITION |
| Управление данными | 42P12 | ERRCODE INVALID DATABASE DEFINITION |
| Управление данными | 42P13 | ERRCODE INVALID FUNCTION DEFINITION |
| Управление данными | 42P14 | ERRCODE INVALID PSTATEMENT DEFINITION |
| Управление данными | 42P15 | ERRCODE INVALID SCHEMA DEFINITION |
| Управление данными | 42P16 | ERRCODE INVALID TABLE DEFINITION |
| Управление данными | 42P17 | ERRCODE INVALID OBJECT DEFINITION |
| Class 44 - WITH CHECK OPTION Violation | | |
| Управление доступом | 44000 | ERRCODE WITH CHECK OPTION VIOLATION |

№ изменения: _____ Подпись отв. лица: _____ Дата внесения изм: _____

| Категория события/ Класс события | Код события | Название условия |
|--|----------------|---|
| Class 53 - Insufficient Resources | | |
| Прочее | 53000 | ERRCODE INSUFFICIENT RESOURCES |
| Прочее | 53100 | ERRCODE DISK FULL |
| Прочее | 53200 | ERRCODE OUT OF MEMORY |
| Прочее | 53300 | ERRCODE TOO MANY CONNECTIONS |
| Прочее | 53400 | ERRCODE CONFIGURATION LIMIT EXCEEDED |
| Class 54 - Program Limit Exceeded | | |
| Управление данными | 54000 | ERRCODE PROGRAM LIMIT EXCEEDED |
| Управление данными | 54001 | ERRCODE STATEMENT TOO COMPLEX |
| Управление данными | 54011 | ERRCODE TOO MANY COLUMNS |
| Управление данными | 54023 | ERRCODE TOO MANY ARGUMENTS |
| Class 55 - Object Not In Prerequisite State | | |
| Управление данными | 55000 | ERRCODE OBJECT NOT IN PREREQUISITE STATE |
| Управление данными | 55006 | ERRCODE OBJECT IN USE |
| Управление данными | 55P02 | ERRCODE CANT CHANGE RUNTIME PARAM |
| Управление данными | 55P03 | ERRCODE LOCK NOT AVAILABLE |
| Управление данными | 55P04 | ERRCODE UNSAFE NEW ENUM VALUE USAGE |
| Class 57 - Operator Intervention | | |
| Прочее | 57000 | ERRCODE OPERATOR INTERVENTION |
| Прочее | 57014 | ERRCODE QUERY CANCELED |
| Прочее | 57P01 | ERRCODE ADMIN SHUTDOWN |
| Прочее | 57P02 | ERRCODE CRASH SHUTDOWN |
| Прочее | 57P03 | ERRCODE CANNOT CONNECT NOW |
| Прочее | 57P04 | ERRCODE DATABASE DROPPED |
| Прочее | 57P05 | ERRCODE IDLE SESSION TIMEOUT |
| Class 58 - System Error | | |
| Прочее | 58000 | ERRCODE SYSTEM ERROR |
| Прочее | 58030 | ERRCODE IO ERROR |
| Управление данными | 58P01 | ERRCODE UNDEFINED FILE |
| Управление данными | 58P02 | ERRCODE DUPLICATE FILE |
| Class 72 - Snapshot Failure | | |
| Управление данными | 72000 | ERRCODE SNAPSHOT TOO OLD |
| Class F0 - Configuration File Error | | |
| Прочее | F0000 | ERRCODE CONFIG FILE ERROR |
| Прочее | F0001 | ERRCODE LOCK FILE EXISTS |
| Class HV - Foreign Data Wrapper Error (SQL/MED) | | |
| Управление данными | HV000 | ERRCODE FDW ERROR |
| Управление данными | HV005 | ERRCODE FDW COLUMN NAME NOT FOUND |
| Управление данными | HV002 | ERRCODE FDW DYNAMIC PARAMETER VALUE NEEDED |
| Управление данными | HV010 | ERRCODE FDW FUNCTION SEQUENCE ERROR |
| Управление данными | HV021 | ERRCODE FDW INCONSISTENT DESCRIPTOR INFORMATION |
| Управление данными | HV024 | ERRCODE FDW INVALID ATTRIBUTE VALUE |
| Управление данными | HV007 | ERRCODE FDW INVALID COLUMN NAME |
| Управление данными | HV008 | ERRCODE FDW INVALID COLUMN NUMBER |
| Управление данными | HV004 | ERRCODE FDW INVALID DATA TYPE |
| Управление данными | HV006 | ERRCODE FDW INVALID DATA TYPE DESCRIPTORS |
| Управление данными | HV091 | ERRCODE FDW INVALID DESCRIPTOR FIELD IDENTIFIER |
| Управление данными | HV00B | ERRCODE FDW INVALID HANDLE |
| Управление данными | HV00C | ERRCODE FDW INVALID OPTION INDEX |
| Управление данными | HV00D | ERRCODE FDW INVALID OPTION NAME |

№ изменения: _____ Подпись отв. лица: _____ Дата внесения изм: _____

| Категория события/ Класс события | Код события | Название условия |
|-------------------------------------|----------------|--|
| Управление данными | HV090 | ERRCODE FDW INVALID STRING LENGTH OR BUFFER LENGTH |
| Управление данными | HV00A | ERRCODE FDW INVALID STRING FORMAT |
| Управление данными | HV009 | ERRCODE FDW INVALID USE OF NULL POINTER |
| Управление данными | HV014 | ERRCODE FDW TOO MANY HANDLES |
| Управление данными | HV001 | ERRCODE FDW OUT OF MEMORY |
| Управление данными | HV00P | ERRCODE FDW NO SCHEMAS |
| Управление данными | HV00J | ERRCODE FDW OPTION NAME NOT FOUND |
| Управление данными | HV00K | ERRCODE FDW REPLY HANDLE |
| Управление данными | HV00Q | ERRCODE FDW SCHEMA NOT FOUND |
| Управление данными | HV00R | ERRCODE FDW TABLE NOT FOUND |
| Управление данными | HV00L | ERRCODE FDW UNABLE TO CREATE EXECUTION |
| Управление данными | HV00M | ERRCODE FDW UNABLE TO CREATE REPLY |
| Управление данными | HV00N | ERRCODE FDW UNABLE TO ESTABLISH CONNECTION |
| Class P0 - PL/pgSQL Error | | |
| Управление данными | P0000 | ERRCODE PLPGSQL ERROR |
| Управление данными | P0001 | ERRCODE RAISE EXCEPTION |
| Управление данными | P0002 | ERRCODE NO DATA FOUND |
| Управление данными | P0003 | ERRCODE TOO MANY ROWS |
| Управление данными | P0004 | ERRCODE ASSERT FAILURE |
| Class XX - Internal Error | | |
| Прочее | XX000 | ERRCODE INTERNAL ERROR |
| Управление данными | XX001 | ERRCODE DATA CORRUPTED |
| Управление данными | XX002 | ERRCODE INDEX CORRUPTED |

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

SMTP (Simple Mail Transfer Protocol) - протокол, используемый для передачи электронной почты.

ZULIP - веб-сервис для обмена сообщениями и организации обсуждений с использованием технологии real-time.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

| | | |
|-------|---|--|
| API | – | Application programming interface |
| CIDR | – | Classless Inter-Domain Routing |
| CIS | – | Center for Internet Security |
| CSV | – | Comma-Separated Values |
| DDL | – | Data Definition Language |
| DML | – | Data Manipulation Language |
| DNS | – | Domain Name System |
| HDD | – | Hard Disk Drive |
| HTTP | – | HyperText Transfer Protocol |
| HTTPS | – | HyperText Transfer Protocol Secure |
| IEC | – | International Electrotechnical Commission |
| IIS | – | Internet Information Services |
| IP | – | Internet Protocol |
| ISO | – | International Organization for Standardization |
| LDAP | – | Lightweight Directory Access Protocol |
| SQL | – | Structured Query Language |
| SSL | – | Secure Sockets Layer |
| SSPI | – | Security Support Provider Interface |
| TCP | – | Transmission Control Protocol |
| АРМ | – | Автоматизированное рабочее место |
| БД | – | База данных |
| ИАФ | – | Идентификация и аутентификация |
| ИС | – | Информационная система |
| ОДТ | – | Обеспечение доступности информации |
| ОЗУ | – | Оперативное запоминающее устройство |

| | | |
|-----------------|---|---|
| ООО | – | Общество с ограниченной ответственностью |
| ОС | – | Операционная система |
| ОЦЛ | – | Обеспечение целостности |
| РСБ | – | Регистрация событий безопасности |
| СВТ | – | Средство вычислительной техники |
| СУБД | – | Система управления базами данных |
| УЗ | – | Учетная запись |
| УПД | – | Управление доступом |
| ФБО | – | Функция безопасности объекта оценки |
| ФСТЭК России | – | Федеральная служба по техническому и экспортному контролю России |
| ЭВМ | – | Электронно-вычислительная машина |

