УТВЕРЖДЕН
643.72410666.00067-07 94 01-ЛУ

# ЗАЩИЩЕННАЯ СИСТЕМА УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ «JATOBA»

## Реализация функций безопасности

## 643.72410666.00067-07 94 01

Листов 180

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

2024

Литера $O_1$

# АННОТАЦИЯ

В настоящем документе приведено концептуальное описание защищенной системы управления базами данных «Jatoba» (далее по тексту – СУБД «Jatoba» или Изделие).

Документ содержит описание назначения и применения СУБД «Jatoba», архитектуру СУБД и функциональные возможности безопасности Изделия.

В разделе 3 «Меры защиты информации» приведены реализованные функциональные возможности безопасности Изделия в соответствии с Приказом ФСТЭК России от 11.02.2013 №17 (ред. от 28.08.2024) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

В разделе 4 «Требования по безопасности информации по Приказу ФСТЭК № 64» приведены требованиям по безопасности информации к СУБД на соответствие 4 классу защиты, установленные в документе «Требования по безопасности информации к системам управления базами данных» (утвержденный приказом ФСТЭК России от 14 апреля 2023 г. № 64).

В разделе 5 «Требования по безопасности информации по ГОСТ Р 57580.1-2017» приведен базовый состав технических мер защиты информации для информационных систем 1 уровня защиты информации финансовых организаций.

В Приложении 1 приведены парольные политики реализуемые компонентом SP

В Приложении 2 приведена аналитическая таблица подтверждающее соответствие состава и содержание регистрируемой информации СУБД «Jatoba» Приказам № 17 и № 64 ФСТЭК России.

В Приложении 3 приведено соответствие событий СУБД категориям мер защиты приказов ФСТЭК России.

В Приложении 4 приведена структура справочной таблицы с правилами кодирования событий безопасности для формирования JSON.

В Приложении 5 приведены идентификаторы событий СУБД «Jatoba».

Приложения 4 и 5 содержат описание событий безопасности для компонент СУБД «Jatoba» «ja_seceventlog» и «ja_Dog»

Степени важности примечаний, применяемые в документе:

**Важная информация** – указания, требующие особого внимания

**Дополнительная информация** – указания, позволяющие упростить работу с изделием

# СОДЕРЖАНИЕ

1. Назначение СУБД ... 7
2. Применение изделия ... 9
2.1. Среда функционирования ... 9
2.2. Параметры межсетевого взаимодействия ... 10
2.3. Компонент пользовательского веб-интерфейса для администраторов «Jatoba data safe» ... 14
2.3.1. Раздел JDS «Мониторинг» ... 15
2.3.2. Разделы JDS «User Risk» и «Access matrix» ... 15
2.3.3. Раздел JDS «Event List» (Список событий) ... 18
2.3.4. Раздел JDS «Snapshots & Reports» (Снимки и отчеты) ... 19
2.3.5. Раздел JDS «Проблемы и решения» (Problems & Solutions) ... 20
2.3.6. Раздел JDS «Активность БД» (DB Activity) ... 20
2.3.7. Раздел JDS «LDAP Sync» (LDAP синхронизация) ... 21
2.3.8. Раздел JDS «DB roles» (Администрирование ролей БД) ... 22
2.3.9. Раздел JDS «Notifications» (Уведомления) ... 23
2.3.10. Раздел «Ландшафт» (Landscape) ... 24
2.3.11. Раздел «Парольные политики» (Password policies) ... 24
2.3.12. Раздел «Резервное копирование» (BACKUP) ... 25
2.4. Разграничение доступа в компоненте «Jatoba data safe» ... 26
2.4.1. Актуальные угрозы безопасности и выполняемые меры защиты ... 26
2.4.2. Разделение полномочий в JDS ... 27
2.4.3. Двухкомпонентная ролевая модель ... 28
3. Меры защиты информации ... 30
3.1. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ) ... 39
3.1.1. Мера защиты ИАФ.1 ... 39
3.1.2. Мера защиты ИАФ.3 ... 40
3.1.3. Мера защиты ИАФ.4 ... 40
3.1.4. Мера защиты ИАФ.5 ... 46
3.2. Управление доступом субъектов доступа к объектам доступа (УПД) ... 48
3.2.1. Мера защиты УПД.1 ... 48
3.2.2. Мера защиты УПД.2 ... 53
3.2.3. Мера защиты УПД.4 ... 58
3.2.4. Мера защиты УПД.5 ... 60
3.2.5. Мера защиты УПД.6 ... 62
3.2.6. Мера защиты УПД.9 ... 64
3.3. Обеспечение целостности информационной системы информации и информации ... 68
3.3.1. Мера защиты ОЦЛ.1 ... 68
3.3.2. Мера защиты ОЦЛ.2 ... 68

3.3.3. Мера защиты ОЦЛ.7 ... 69
3.4. Регистрация событий безопасности (РСБ) ... 69
3.4.1. Мера защиты РСБ.2 ... 70
3.4.2. Мера защиты РСБ.3 ... 71
3.4.3. Мера защиты РСБ.6 ... 73
3.4.4. Мера защиты РСБ.7 ... 73
3.4.5. Мера защиты РСБ.8 ... 73
3.5. Обеспечение доступности информации (резервирование, кластеризация и восстановление информации) (ОДТ) ... 77
3.5.1. Мера защиты ОДТ.4 ... 77
3.5.2. Мера защиты ОДТ.5 ... 77
3.5.3. Мера защиты ОДТ.6 ... 79
4. Требования по безопасности информации по Приказу ФСТЭК № 64 ... 83
4.1. Ограничение программной среды в СУБД (ОПС) ... 84
4.2. Контроль целостности в системе управления базами данных ... 84
5. Требования по безопасности информации по ГОСТ Р 57580.1-2017 ... 87
5.1. Процесс 1 «Обеспечение защиты информации при управлении доступом» ... 91
5.1.1. Подпроцесс «Управление учетными записями и правами субъектов логического доступа» ... 91
5.1.2. Подпроцесс «Идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа» ... 96
5.2. Процесс 3 «Контроль целостности и защищенности информационной инфраструктуры» ... 101
5.2.1. Базовый состав мер по контролю отсутствия известных (описанных) уязвимостей защиты информации объектов информатизации ... 101
5.3. Процесс 6 «Управление инцидентами защиты информации» ... 102
5.3.1. Подпроцесс «Мониторинг и анализ событий защиты информации» ... 102
5.4. Описание реализации отдельных базовых мер защиты информации ... 103
5.4.1. Базовая мера МАС.4 «Организация мониторинга данных регистрации о событиях защиты информации, формируемых системным ПО, операционными системами, СУБД» ... 103
5.4.2. Базовая мера ЦЗИ.8 Контроль отсутствия известных (описанных) уязвимостей защиты информации объектов информатизации ... 109
Приложение 1 ... 110
Парольные политики ... 110
Параметры парольной политики по умолчанию ... 110
Параметры парольной политики FSTEC _1_Class ... 112
Параметры парольной политики FSTEC _2_Class ... 114
Параметры парольной политики CIS ... 116
Параметры парольной политики Corporate_1 ... 118
Параметры парольной политики Corporate_2 ... 120
Параметры парольной политики Corporate_3 ... 122
Приложение 2 ... 124

Соответствие требованиям приказов ФСТЭК к составу событий безопасности ..... 124
Приложение 3 .....127
Соответствие событий СУБД категориям мер защиты приказов ФСТЭК..... 127
Приложение 4 .....141
Соответствие требованиям приказов ФСТЭК к составу событий безопасности и структура справочной таблицы со всеми полями для формирования JSON ..... 141
Структура справочной таблицы с правилами кодирования событий безопасности для формирования JSON ..... 145
Структура справочной таблицы с компонентами для формирования JSON ..... 153
Приложение 5 .....154
Список ключей JSON для типа события безопасности «Идентификация и аутентификация субъекта доступа» ..... 154
Список ключей JSON для типа события безопасности «Управление учетными записями пользователей» ..... 156
Список ключей JSON для типа события безопасности «Управление атрибутами доступа» ..... 159
Список ключей JSON для типа события безопасности «Доступ к защищаемой информации» ..... 161
Список ключей JSON для типа события безопасности «Изменение параметров настроек средств защиты информации»..... 163
Список ключей JSON для типа события безопасности «Установка/удаление компонентов программного обеспечения»..... 166
Список ключей JSON для типа события безопасности «Управление запуском/остановкой компонентов программного обеспечения» ..... 169
Список ключей JSON для типа события безопасности «Управлением журналами регистрации событий безопасности» ..... 171
Идентификаторы событий для компонента «ja_Dog» ..... 175
Идентификаторы событий для компонента «ja_Log»..... 177
Термины и определения .....178
Перечень сокращений.....179

# 1. НАЗНАЧЕНИЕ СУБД

СУБД «Jatoba» при соблюдении условий эксплуатации, указанных в формуляре, предназначена для использования:

– в государственных информационных системах первого класса защищенности (ГИС) в соответствии с приказом ФСТЭК России от 11.02.2013 №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

– в информационных системах персональных данных 1 уровня защищенности (ИСПДн) в соответствии с приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды 1 класса защищенности (КВО) в соответствии с приказом ФСТЭК России от 14.03.2014 № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»;

– в значимых объектах значимых объектов критической информационной инфраструктуры 1 категории (КИИ) в соответствии с приказом ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;

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

– в информационных системах 1 уровня защиты информации финансовых организаций (ГОСТ Р 57580.1-2017. Национальный стандарт Российской Федерации.

Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер (утв. и введен в действие Приказом Росстандарта от 08.08.2017 № 822-ст)).

# 2. ПРИМЕНЕНИЕ ИЗДЕЛИЯ

## 2.1. Среда функционирования

СУБД «Jatoba» может функционировать в гетерогенных сетях и взаимодействовать с серверами различных функциональных возможностей:

1) MS Active Directory

С сервером каталогов MS Active Directory СУБД «Jatoba» взаимодействует, когда установлены методы аутентификации:

– LDAP;

– SSL;

– GSSAPI;

– SSPI.

Для синхронизации учетных записей пользователей используется компонент ja_Sync_LDAP.

2) Linux сервер

СУБД «Jatoba» адаптирована для работы на GNU/Linux. При этом СУБД «Jatoba» может использовать Linux сервер для применения метода аутентификации PAM.

3) RADIUS сервер

RADIUS сервер используется СУБД «Jatoba» при применении метода аутентификации RADIUS.

4) Сервер центра сертификации (удостоверяющий центр)

Центр сертификации используется для проверки валидности сертификата, выданного пользователю при методе аутентификации SSL, и сертификатов серверов кластера при использовании компонента jaDog.

Для организации центра сертификации могут использоваться решения Microsoft Corporation, отечественные решения, например, продукты компании ООО «Крипто-Про», и другие центры сертификации.

В сетях с контроллером домена роль сервера контроллера домена может совпадать с ролью центра сертификации.

5) BackUp server

BackUp server используется для хранения резервных копий СУБД «Jatoba» и последующего восстановления информации. Резервное копирование и восстановление информации осуществляется компонентом pg_ProBackup.

6) File – server

Файловый сервер используется для кластеризации БД при использовании компонента «ja_Dog».

7) Сервер СЗИ от НСД

СУБД «Jatoba» может функционировать в сети непосредственно на серверах, защищенных средствами защиты информации от несанкционированного доступа.

8) Jatoba data safe сервер

Компонента «Jatoba data safe» (JDS) рекомендуется использовать на отдельном сервере с установленной СУБД «Jatoba». Поскольку функциональная возможность сбора событий безопасности с целевых СУБД требует дополнительного дискового пространства сервера

Функциональные возможности компонента JDS описаны в разделе 2.2 «Компонент пользовательского веб-интерфейса для администраторов «Jatoba data safe».

Требуется установка СУБД «Jatoba» в защищаемой локальной вычислительной сети, в помещениях (сооружениях) с контролируемым и управляемым физическим доступом.

## 2.2. 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 2.1.

Таблица 2.1 – Параметры протоколов используемых СУБД

| Компонент | Наименование протокола | Протокол | Порты |
|---|---|---|---|
| **СУБД** | Database port (db_port) | Libpq | 5432 |
| | Аутентификации LDAP | LDAP | 389 (AD, ALD Pro, FreeIPA) по умолчанию |
| | | LDAPS | 636 (SAMBA) по умолчанию |
| | Аутентификации GSSAPI | NTLM/Kerberos | 88, 445 |
| | Аутентификации SSPI | NTLM/Kerberos | 88, 445 |
| | Аутентификации Radius | Radius | 1812, 1813 |
| | Аутентификации TLS/SSL (сертификаты) | TLS/SSL | 5432 |
| **jaDog** | Jadog TCP port (user_interface) | TCP | 54321, 54322 |
| | Jadog PORT number (port) | Jadog | 12345, (Custom) |
| | Jadog searching protocol port (jadog_search_port) | Jadog | 12346 |
| | REST API | REST API | 54443 |
| **ja__Hipe_Cluster** | Database port (db_port) | Libpq | 5432 |
| | Протокол аутентификации SSL | SSL | 5432, 443 |
| **ja_Inventory** | Database port (db_port) | Libpq | 5432 |
| **ja_Log** | Database port (db_port) | Libpq | 5432 |
| | Протокол аутентификации SSL | SSL | 443, 10051 |

| Компонент | Наименование протокола | Протокол | Порты |
|---|---|---|---|
| **ja_Sync_Ldap** | Протокол аутентификации LDAP | LDAP | 389 (AD, ALD Pro, FreeIPA) по умолчанию |
| | | LDAPS | 636 (SAMBA) по умолчанию |
| **JDS** | Database port (db_port) | Libpq | 5432 |
| | Протокол передачи данных HTTPS | HTTPS | 443, 5000 |
| | Протокол передачи данных HTTP | HTTP | 9000 |
| | Протокол электронной почты | SMTP | 25, 587 |
| | Протокол аутентификации SSL | SSL | 464 |
| | Протокол передачи сообщений на веб-сервер ZULIP | ZULIP | 443 |
| | Протокол удалённого управления операционной системой | SSH | 22 |
| | Jadog PORT number (port) | Jadog | 12345, (Custom) |
| | Протокол аутентификации LDAP | LDAP | 389 (AD, ALD Pro, FreeIPA), 636 (SAMBA) |
| | Database port (db_port) | Libpq | 5433 |
| **Prometheus** | Протокол передачи данных HTTP | HTTP | 9090 |
| | Протокол удалённого управления операционной системой | SSH | 22 |
| **Alert manager** | Протокол передачи данных HTTP | HTTPS | 9093 |
| | Протокол удалённого управления операционной системой | SSH | 22 |
| | Протокол электронной почты | SMTP | 25 |
| **node_exporter** | Протокол передачи данных HTTP | HTTP | 9100 |
| **postgres_exporter** | Протокол передачи данных HTTP | HTTP | 9187 |
| | Database port (db_port) | Libpq | 5432 |
| **sql_exporter** | Протокол передачи данных HTTP | HTTP | 9399 |
| | Database port (db_port) | Libpq | 5432 |
| **pg_ProBackup** | Database port (db_port) | Libpq | 5433 |
| | Протокол удалённого управления операционной системой | SSH | 22 |

| Компонент | Наименование протокола | Протокол | Порты |
|---|---|---|---|
| **pgSQL-HTTP** | Протокол передачи данных HTTP | HTTP | 80, 443, Custom proxy port |

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

Пользователи БД используют протокол Libpq 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 Libpq на порт 5432.

Схема подключения представлена на рисунке 2.1.

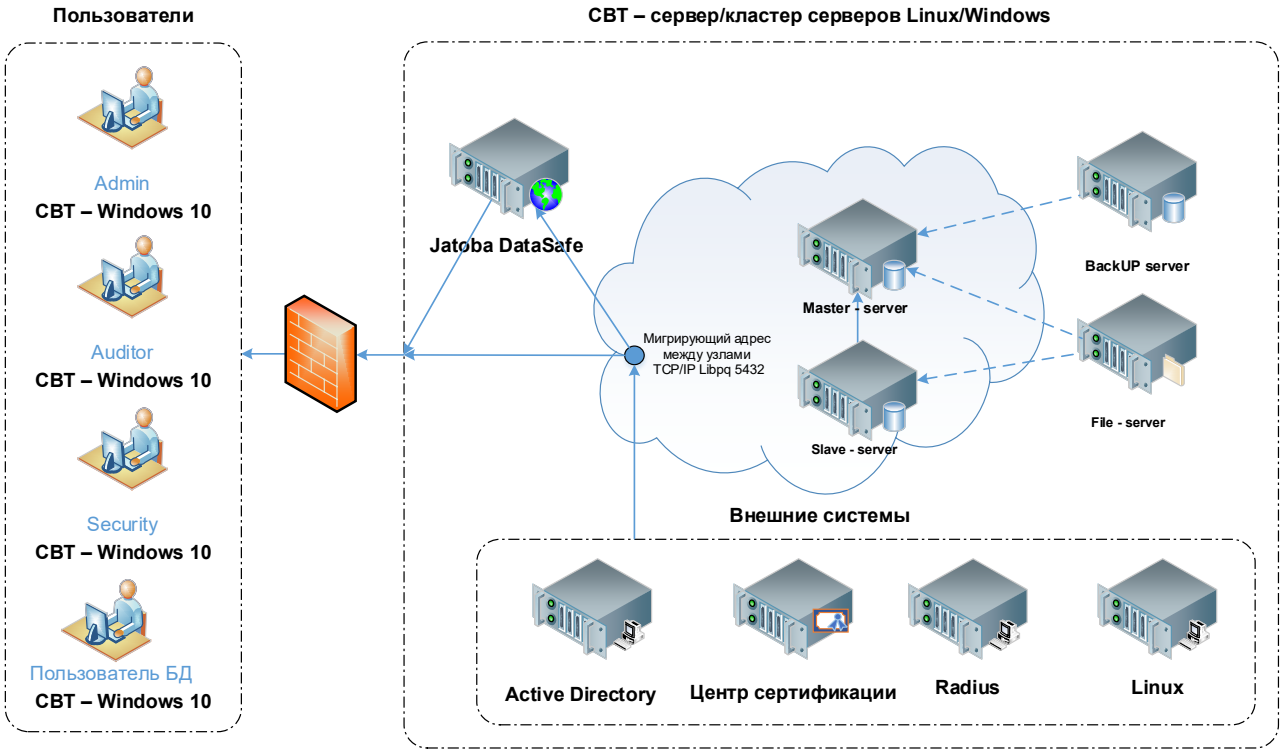


Рисунок 2.1 – Интерфейсы подключения СУБД

Протокол HTTPS по порту 443 используется для взаимодействия:

– СУБД с сервером лицензирования;

– компонента «Jatoba Data Safe» и служебной СУБД.

## 2.3. Компонент пользовательского веб-интерфейса для администраторов «Jatoba data safe»

Компонент JDS разработан с учетом требований ГОСТ Р 59547-2021 «Национальный стандарт Российской Федерации. Защита информации. Мониторинг информационной безопасности. Общие положения» (утв. и введен в действие Приказом Росстандарта от 27.07.2021 № 656-ст).

Компонент JDS является частью СУБД «Jatoba» и позволяет осуществлять:

– мониторинг состояния хоста и СУБД;

– формирование матрицы привилегий пользователей;

– формирование матрицы системных привилегий пользователей;

– управление кластером;

– просмотр событий безопасности;

– выявление проблем в целевой СУБД и разрешать их;

– формирование отчетов о СУБД;

– контроль за подключениями к целевой СУБД и JDS;

– управление синхронизацией учетных записей пользователей с активным каталогом;

– управление ролями СУБД;

– оповещение администраторов о событиях целевой СУБД и компонента JDS;

– управление и конфигурирование хоста СУБД и самой СУБД;

– управление парольными политиками целевой СУБД и самого компонента JDS

– управление резервными копиями.

Компонент предназначен для постоянного и периодического контроля и мониторинга состояния целевых СУБД, уровня их безопасности, управления кластером.

Каждая инсталляция СУБД подразумевает отдельный сервер и (или) кластер СУБД, на котором установлена СУБД «Jatoba».

### 2.3.1. Раздел JDS «Мониторинг»

Раздел «Мониторинг» не выполняет функций безопасности и предназначен для отображения оперативной информации в форме графических и цифровых панелей (виджетов) о целевой СУБД и ОС, на которой она установлена.

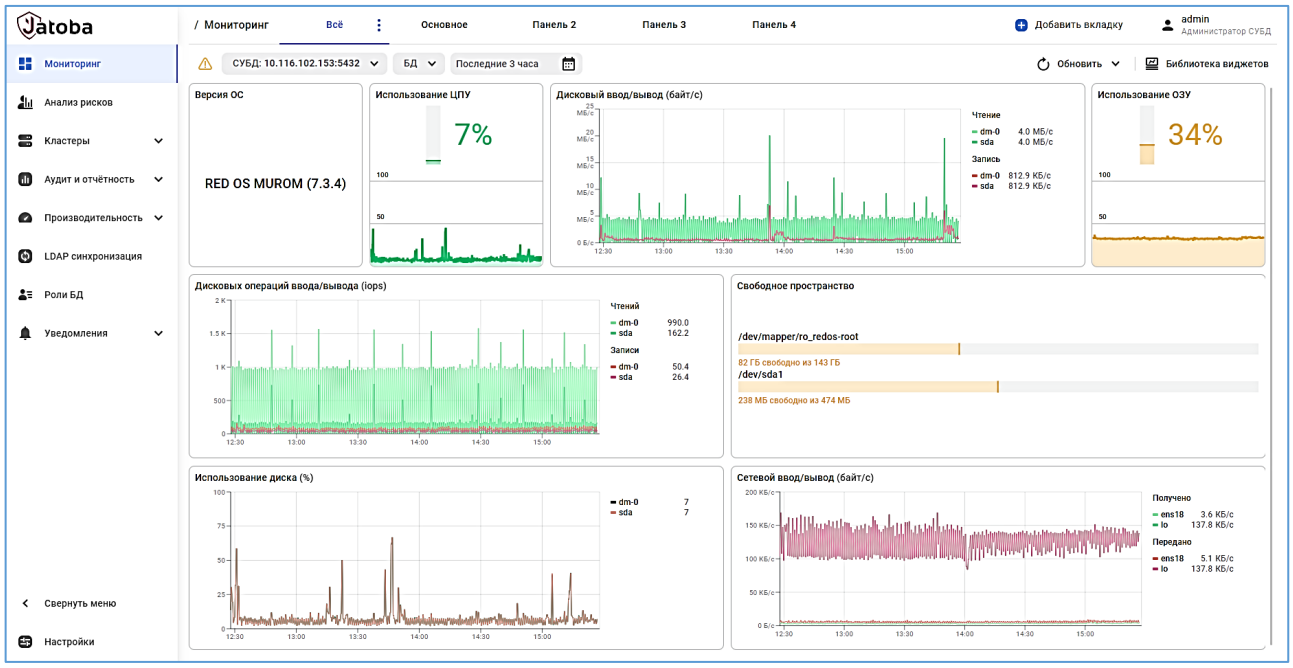


Рисунок 2.2 – Предустановленные виджеты

Виджеты имеют функциональную возможность контроль над пороговыми значениями и рассылку уведомлений

### 2.3.2. Разделы JDS «User Risk» и «Access matrix»

Разделы JDS «User Risk» (Анализ рисков) и «Access Matrix» (Матрица доступа) являются инструментами аудита безопасности и используются при:

– проведении оперативного контроля назначенных прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы;

– расследовании инцидентов безопасности;

– формировании сертификационной документации Системы менеджмента информационной безопасности (СМИБ);

– прохождении ежегодного аудита органом по сертификации по СМИБ.

Раздел «User Risk» предоставляет количественные показатели системных привилегий и атрибутов ролей относительно схемы данных в БД, функционирующей на выбранном сервере.

Рисунок 2.3 – Раздел «User Risk» (Анализ рисков)

Для полноты представления о дискреционной модели доступа разработан раздел JDS «Access matrix» (Матрица доступа). Раздел отражает назначенные атрибуты пользователей, объекты доступа и имеющиеся привилегии пользователей относительно этих объектов.

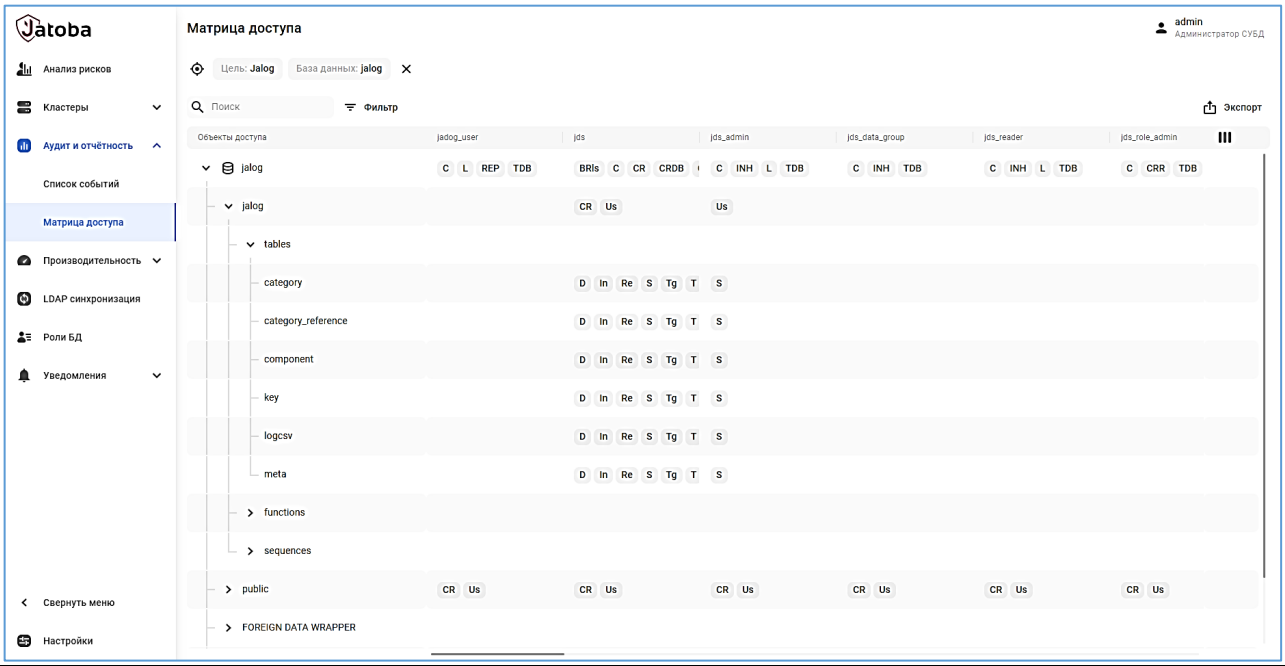

Рисунок 2.4 – Раздел «Access matrix» (Матрица доступа)

### 2.3.3. Раздел JDS «Event List» (Список событий)

Раздел JDS «Event List» разработан с учетом требований ГОСТ Р 59548-2022 «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации» (утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 13 января 2022 г. № 2-ст).

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

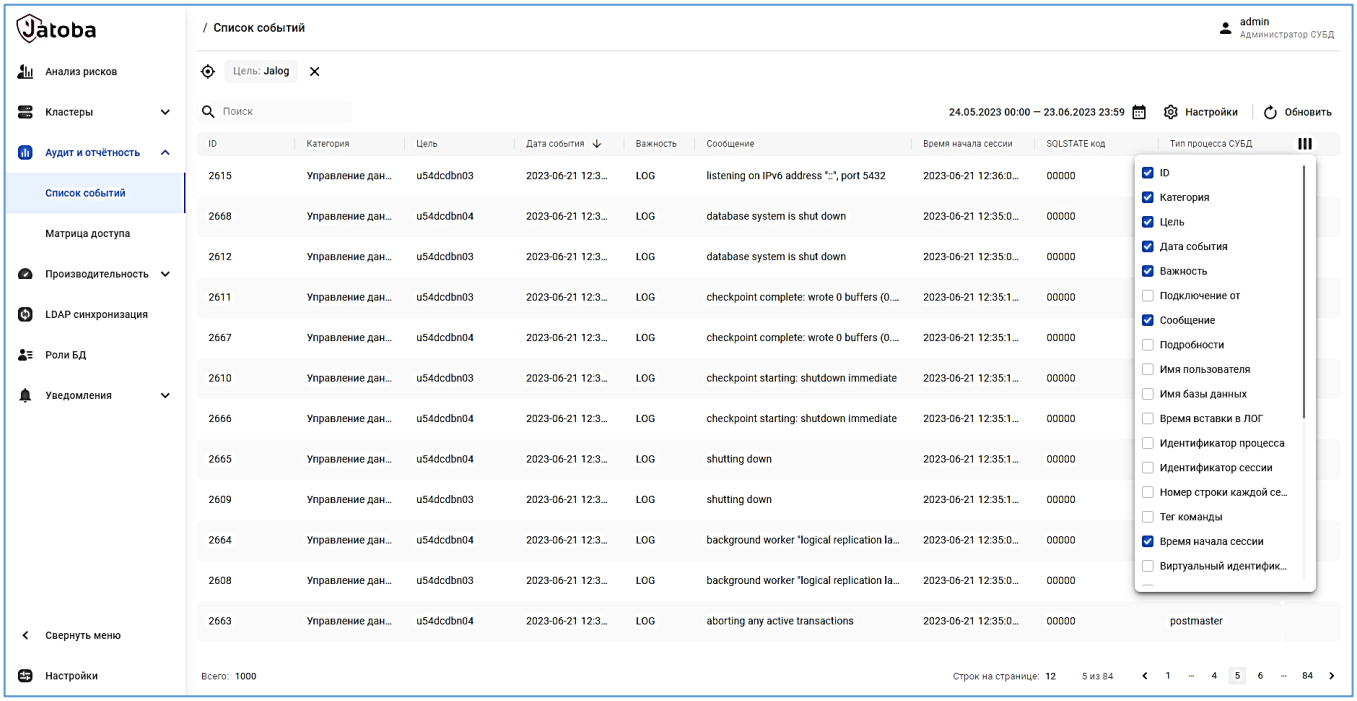


Рисунок 2.5 – Раздел «Event List» (Список событий)

Применение компонента «pgAudit» расширяет поле «Error message», как описано в разделе 3.4.1 документа.

Состав и содержание регистрируемой информации приведен в Приложении 2.

Сбор данных о событиях безопасности осуществляется при помощи агентов сбора данных в автоматическом режиме с каждой инсталляции (с сервера СУБД, кластера СУБД) и аккумулируются в служебной БД Data Safe, как описано в п. 3.4.2.1 документа.

Выводимые события СУБД дополняются категориями событий безопасности, приведенными в Приложении 3, определенных методом «Делфи».

### 2.3.4. Раздел JDS «Snapshots & Reports» (Снимки и отчеты)

Раздел «Snapshots & Reports» предназначен для создания снимков состояния БД (снапшотов) и получения отчетов. Формирование статической информации выполняется компонентом «pg_Profile». Сбор информации доступен только с СУБД, на которых установлено расширение «pg_Profile».

«pg_Profile» – компонент, позволяющий собирать и просматривать параметры и метрики функционирования различных БД в различное время, а также строить отчеты по этим данным и сравнивать их между собой для выявления проблемных мест.

Анализ снимков состояния позволяет выявить проблемные участки путем просмотра или сравнения данных из разных снапшотов.

Перечень отчетов полностью описан в документе 643.72410666.00067-07 98 01-06 «Руководство по настройке. Часть 6. Формирование отчетов производительности СУБД. Компонент «pg_Profile».

Снимки и отчеты представлены на рисунках 2.6 и 2.7 соответственно.

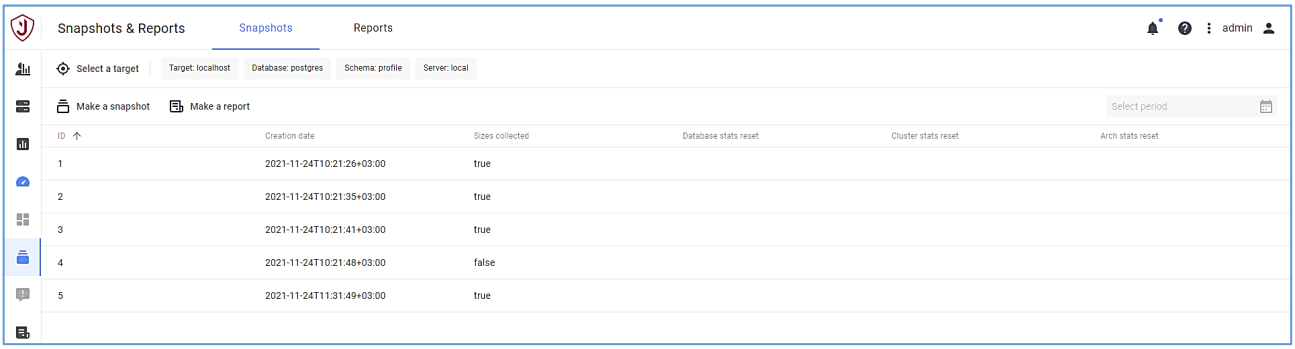


Рисунок 2.6 – Вкладка «Snapshots» (Снимки)

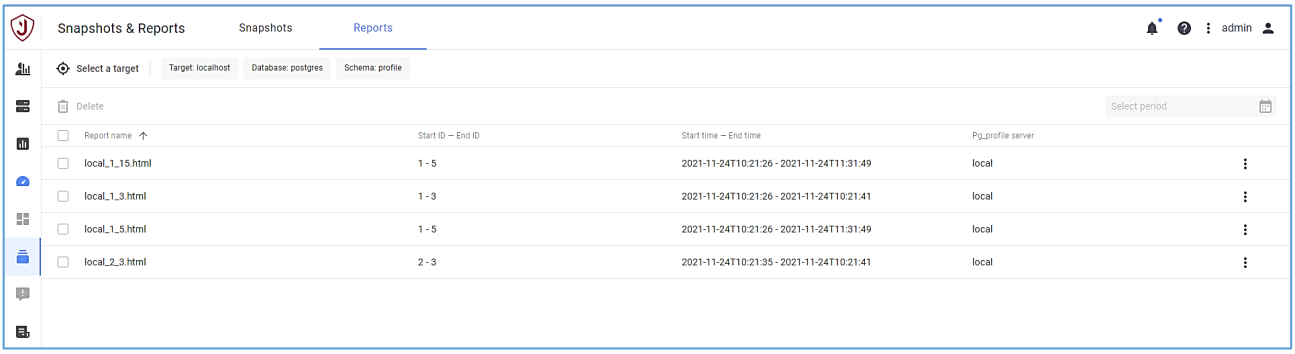


Рисунок 2.7 – Вкладка «Reports» (Отчеты)

### 2.3.5. Раздел JDS «Проблемы и решения» (Problems & Solutions)

Раздел JDS «Problems & Solutions» позволяет определять ряд проблем, существующих в целевой СУБД. Для определения проблемы созданы скрипт обнаружения и для исправления проблемы – динамические скрипты (шаблон таблетки).

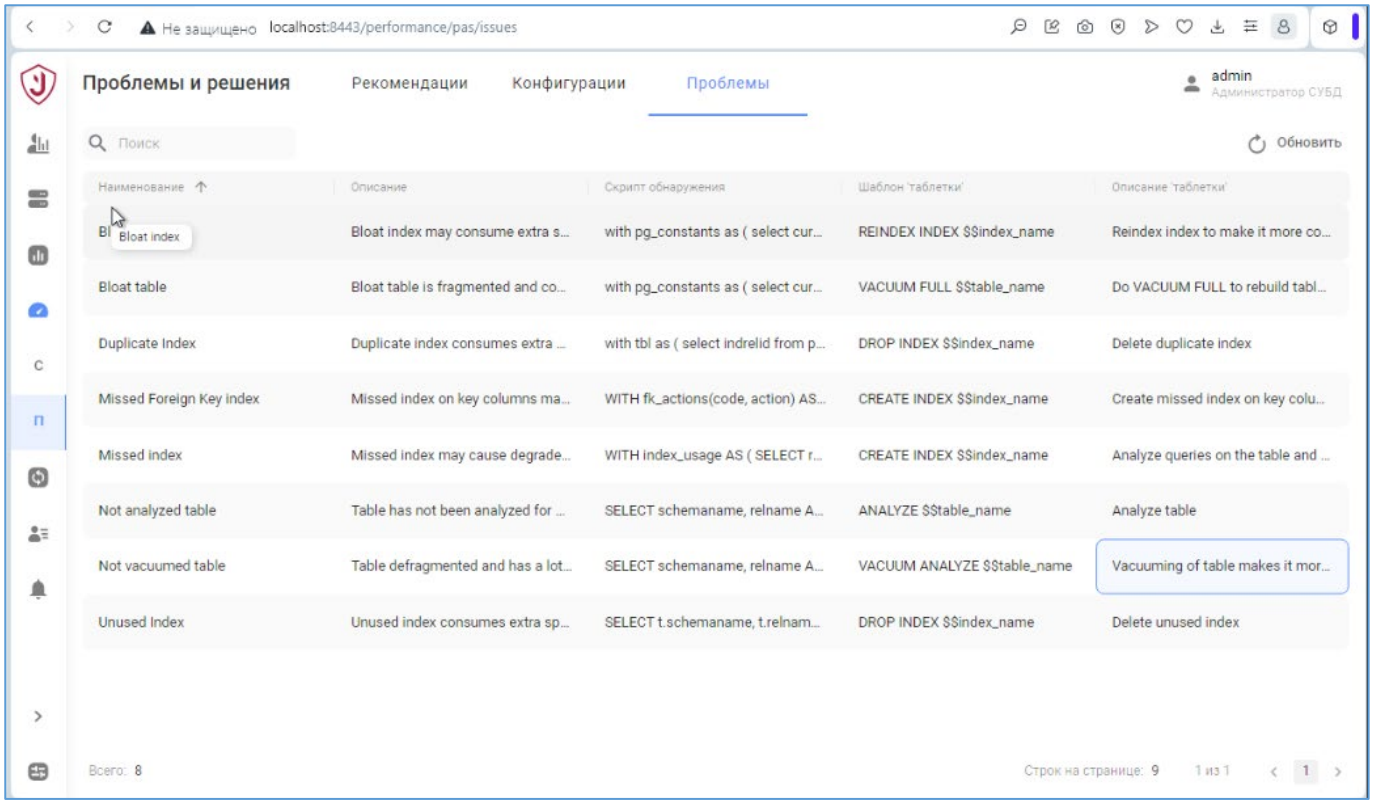


Рисунок 2.8 – Вкладка «Проблемы»

### 2.3.6. Раздел JDS «Активность БД» (DB Activity)

Раздел «Активность БД» (DB Activity) предназначен для:

– мониторинга активности в СУБД;

– получения информации о выполняющихся сессиях/процессах, существующих блокировках;

– завершения сессий;

– выявления подозрительной активности пользователей.

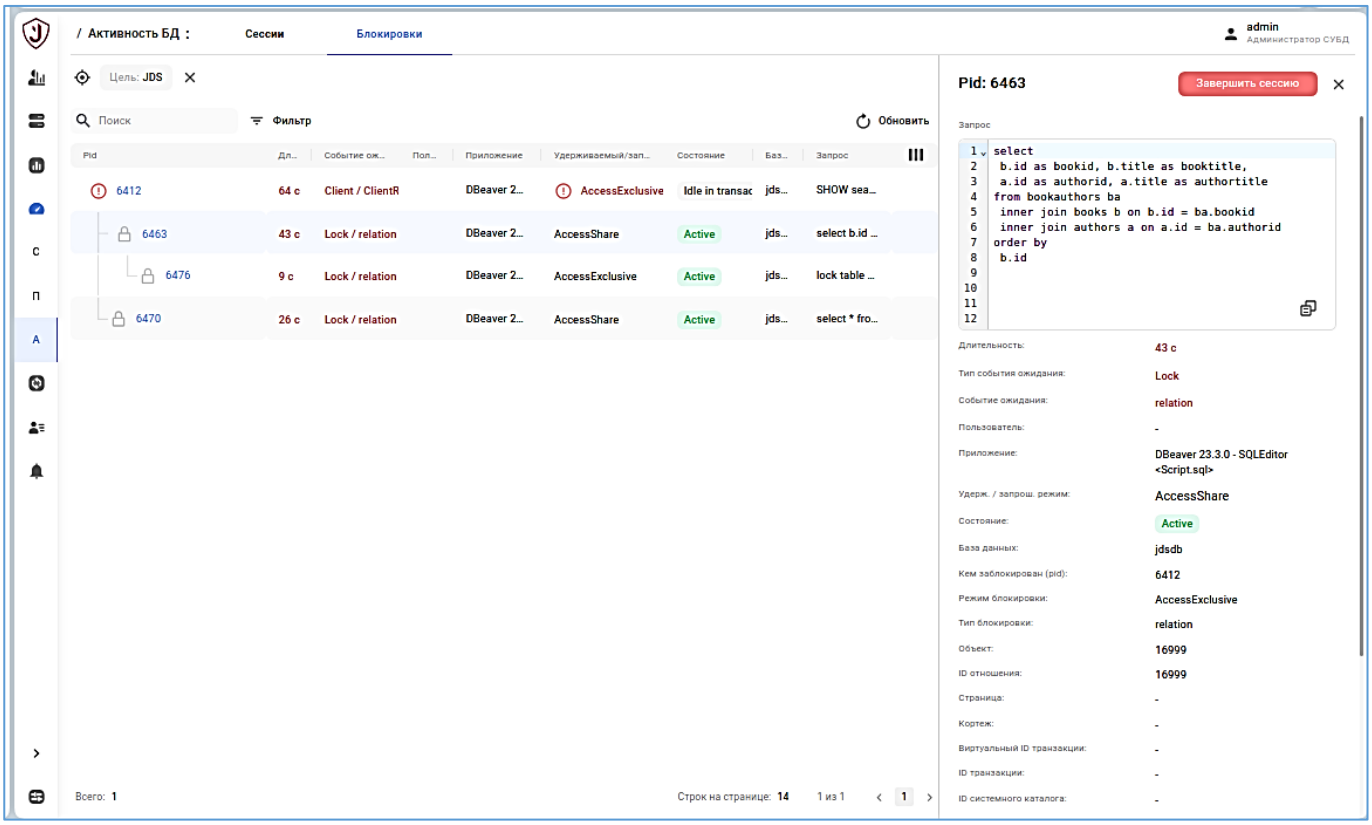


Рисунок 2.9 – Окно «Завершение сессии» на вкладке «Блокировки»

### 2.3.7. Раздел JDS «LDAP Sync» (LDAP синхронизация)

Раздел JDS «LDAP Sync» предназначен для графического отображения операций по синхронизации учетных записей Microsoft Active Directory и учетных записей целевой СУБД.

Для выполнения синхронизации требуется, чтобы расширение компонента «ja_Sync_LDAP» было установлено на целевой СУБД.

Вид списка профилей синхронизации УЗ и журнал событий представлен на рисунке 2.10.

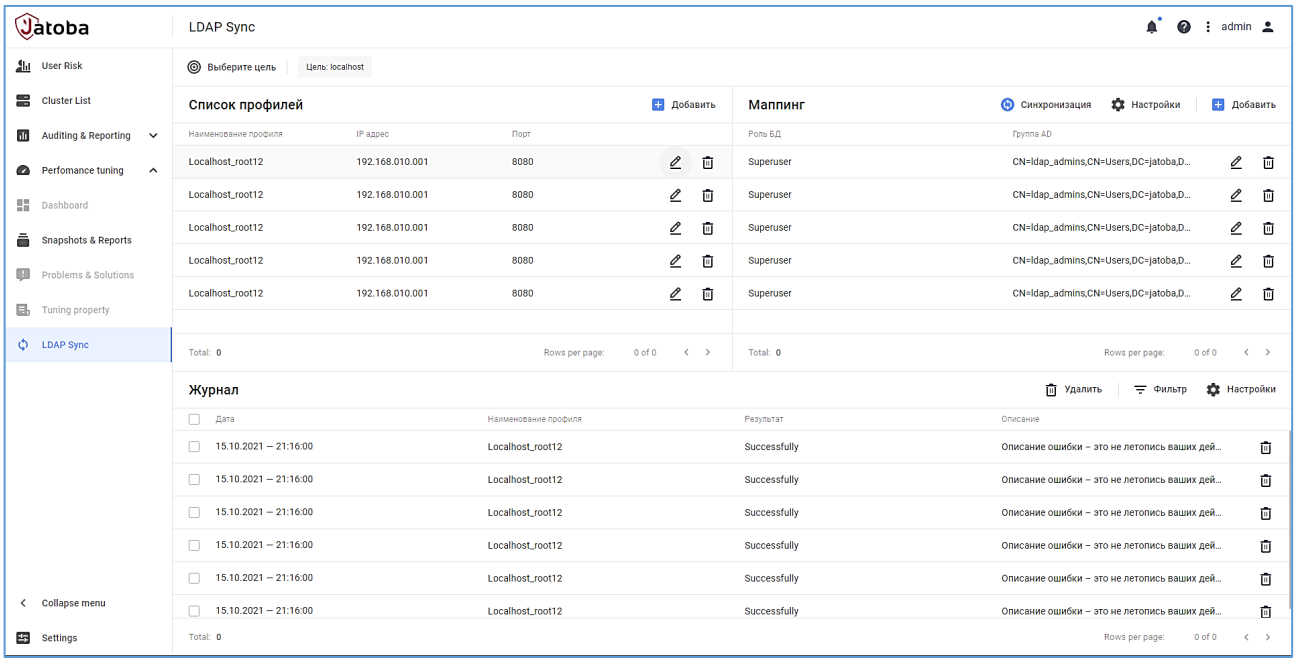


Рисунок 2.10 – LDAP Sync (LDAP синхронизация)

### 2.3.8. Раздел JDS «DB roles» (Администрирование ролей БД)

Раздел «Роли БД» предназначен для:

– создания ролей;

– редактирования ролей;

– назначения атрибутов и привилегий ролей.

Раздел доступен пользователю «JDS» с назначенной функциональной ролью:

1) Администратор (Administrator).

2) Администратор ИБ (Security).

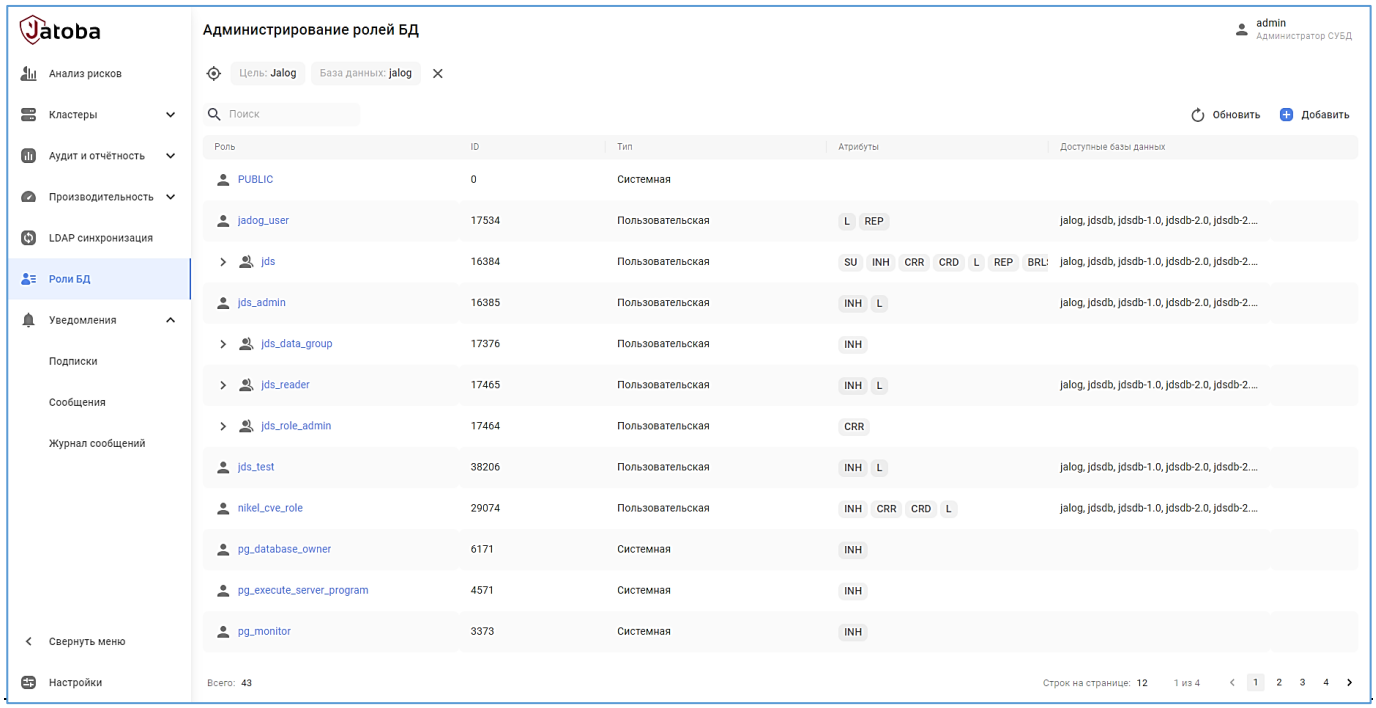


Рисунок 2.11 – Раздел Администрирование ролей БД

### 2.3.9. Раздел JDS «Notifications» (Уведомления)

Раздел «Уведомления» предназначен для оповещения администраторов о событиях целевой СУБД и компонента JDS.

Механизм уведомлений содержит в себе три типа поиска сообщений:

1) Ошибки БД.

Поиск выполняется по классу события или по коду события.

2) События учетных записей.

Поиск выполняется по ключевым фразам для выполнения мер безопасности УПД.1 (5) и УПД.9 (4) в соответствии с Приказом № 17 ФСТЭК России.

3) Произвольный текст.

Поиск выполняется по ключевым словам, задаваемым пользователем JDS.

Оповещение производится по сервисам E-mail и /или Zulip.

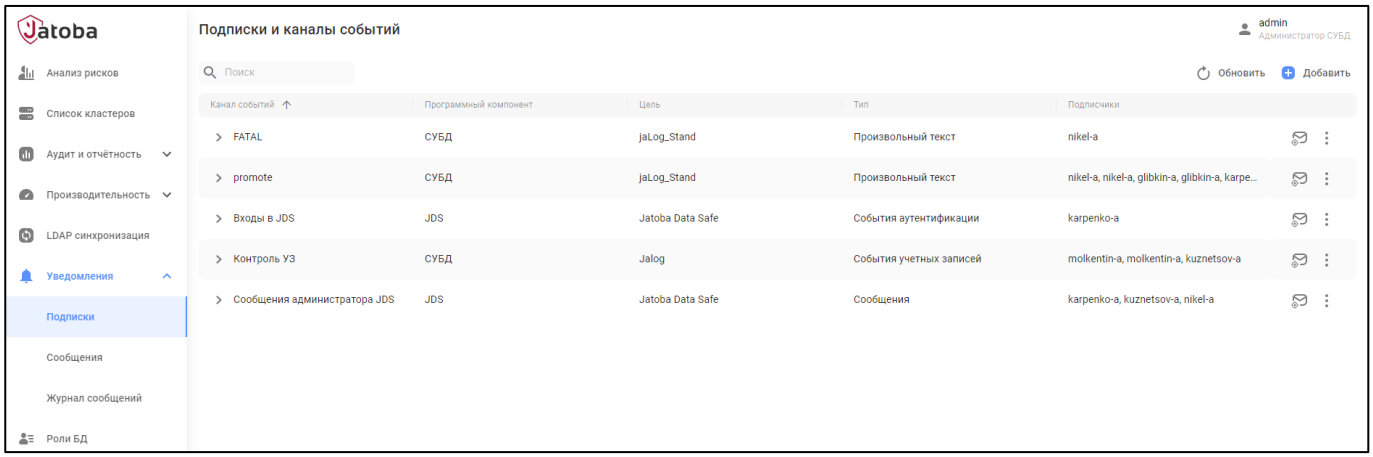


Рисунок 2.12 – Список каналов событий

### 2.3.10. Раздел «Ландшафт» (Landscape)

Раздел «Ландшафт» предназначен для:

- получения общей информации о хосте СУБД;
- получения общей информации о СУБД;
- управления конфигурационными файлами СУБД;
- установки и управления расширениями СУБД.
- управление кластером на основе компонента jaDog

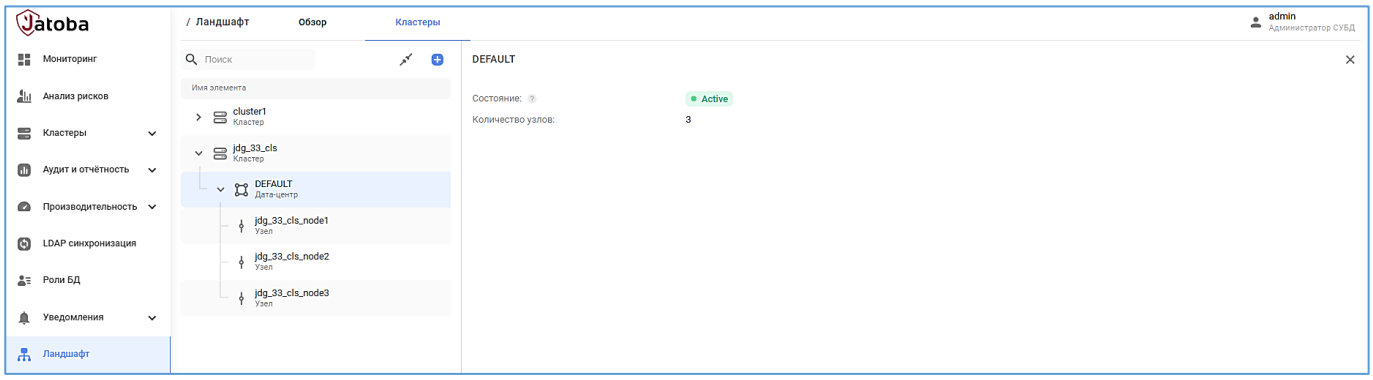


Рисунок 2.13 - Вкладка «Параметры СУБД»

### 2.3.11. Раздел «Парольные политики» (Password policies)

Раздел «Уведомления» предназначен для оповещения администраторов о событиях целевой СУБД и компонента JDS.

В комплект поставки СУБД «Jatoba» с версией ядра «5» и выше в компонент JDS включен раздел «Парольные политики».

Раздел «Парольные политики» предназначен для автоматизации и упрощения работы с парольными политиками и блокировками пользователей целевой СУБД.

Раздел включает в себя подразделы:

- Управление политиками (Policy management);
- Привязка ролей (Role Binding);
- Работа с блокировками.

Корректная работа раздела обеспечивается установленными и настроенными на целевой СУБД компонент:

SecurityProfile, описанного в документе «Руководство администратора»;

ja_CSum, описанного в документе «Руководство по настройке. Часть 14. Контроль целостности. Компонент «ja_CSum».

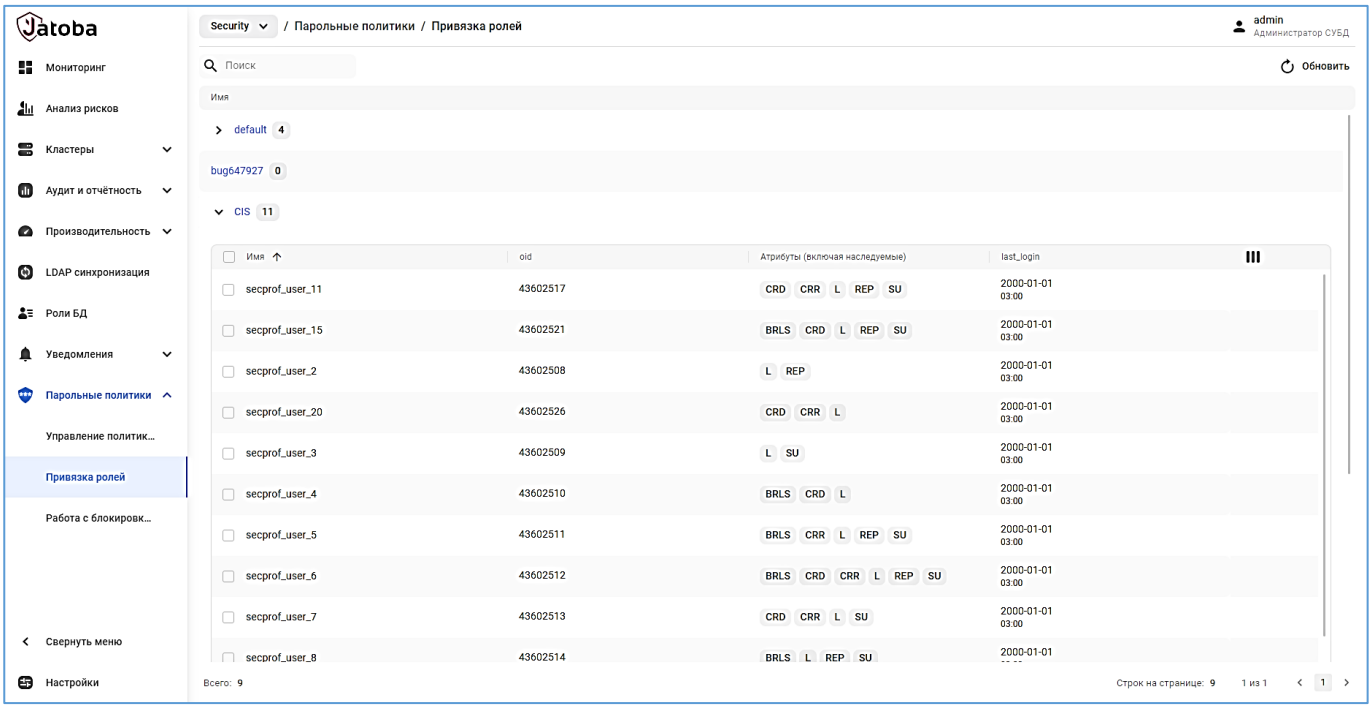


Рисунок 2.14 – Список пользователей привязанных к парольной политике

### 2.3.12. Раздел «Резервное копирование» (BACKUP)

Раздел выполняет функцию безопасности и предназначен для:

- настройки и управления компонентом «probackup»;

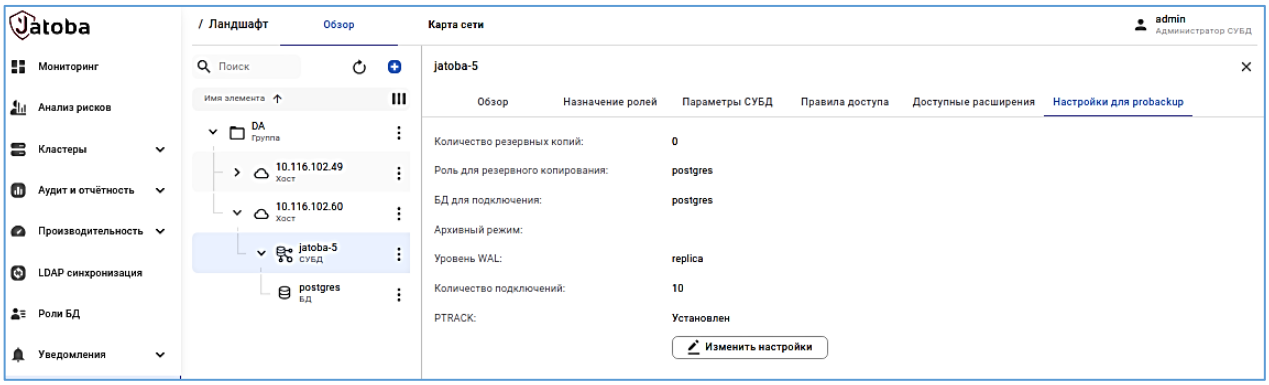


Рисунок 2.15 - Вкладка «Настройки для probackup»

– управления хранилищем резервных копий;
– создания резервных копий.

## 2.4. Разграничение доступа в компоненте «Jatoba data safe»

### 2.4.1. Актуальные угрозы безопасности и выполняемые меры защиты

Компонент «Jatoba data safe» является частью СУБД «Jatoba» и несет в себе часть административных функциональных возможностей и функций безопасности.

JDS и СУБД «Jatoba» при совместном функционировании рассматриваются как единый объект оценки (ОО).

При оценке реальной архитектуры Изделия выявляются актуальные угрозы безопасности информации список которых приводится ниже, но не ограничивается им:

– УБИ. 122 «Угроза повышения привилегий»;

– УБИ. 090 «Угроза несанкционированного создания учетной записи пользователя»;

– УБИ. 037 «Угроза исследования приложения через отчеты об ошибках».

Реализация (возникновение) приведенных угроз может привести к:

– нарушению безопасности, обрабатываемой в целевой и служебной СУБД информации, выражающейся в нарушении:

а) конфиденциальности;

б) целостности;

в) доступности;

г) неотказуемости;

д) подотчетности, аутентичности и достоверности информации.

– нарушению или прекращению функционирования целевой СУБД.

Служебная СУБД компонента «Jatoba data safe», как и целевая СУБД «Jatoba», реализует меры защиты информации, описанные в разделе 3 «Меры защиты информации» для нейтрализации угроз безопасности. Например, следующих угроз:

1) Через вкладку «Clusters» JDS возможна реализация УБИ. 122 «Угроза повышения привилегий», т.е. нарушение работы кластера или приведение его в состояние отказа в обслуживании умышленными или не умышленными действиями.

2) Через раздел JDS «LdapSync» возможна реализация угрозы УБИ. 090 «Угроза несанкционированного создания учетной записи пользователя», т.е. создание учетной записи в целевой СУБД пользователю AD, у которого такого доступа быть не должно.

3) Через разделы JDS «Event List» и «Snapshots & Reports» возможна реализация УБИ. 037 «Угроза исследования приложения через отчеты об ошибках». Так как «Event List» предоставляет информацию о событиях безопасности, «Snapshots & Reports» предоставляет комбинированные и расширенные отчеты о состоянии целевой СУБД, то получив доступ к этим разделам, злоумышленник получит данные об алгоритме работы СУБД и о ее предполагаемой структуре.

Компонент JDS реализует меру защиты информации Усиление РСБ.3(1). Раздел JDS «Event List» в совокупности мер безопасности выполняет меру защиты информации РСБ.7. Раздел JDS «LDAP Sync» вызывая одноименное расширение на целевой СУБД выполняет меру защиты информации УПД.1.

### 2.4.2. Разделение полномочий в JDS

Для нейтрализации угроз безопасности в компоненте JDS, реализовано разделение доступа пользователей к функциональным возможностям компонента.

Разделение полномочий осуществляется на основе предустановленной ролевой модели, предусматривающей следующие роли:

1) Auditor – оператор мониторинга, выполняющий функции, связанные с анализом результатов мониторинга (событий безопасности) и подготовкой аналитической информации.

2) Security – администратор безопасности, выполняющий функции, связанные с настройкой программных и аппаратных компонентов, применяемых для мониторинга.

3) Admin – системный администратор, выполняющий функции, связанные с установкой и обеспечением работоспособности программных и аппаратных компонентов, применяемых для мониторинга.

Доступность разделов компонента должна соответствовать матрице, представленной в таблице 2.2.

Таблица 2.2 – Матрица доступности разделов

| **Разделы JDS** | | **Роли в JDS** | | |
|---|---|---|---|---|
| | **Подраздел JDS** | **Admin** | **Security** | **Auditor** |
| | | **Администратор СУБД** | **Администратор ИБ** | **Аудитор** |
| **Анализ рисков (User Risk)** | | + | + | + |
| **Список кластеров (Cluster List)** | | + | | |
| **Аудит и отчетность (Auditing & Reporting)** | | | | |
| | События безопасности (Event List) | + | + | + |
| | Матрица доступа (Access Matrix) | + | + | + |
| **Производительность (Performance tuning)** | | | | |
| | Снимки и отчеты (Snapshots & Reports) | + | + | |
| | Проблемы и решения (Problems & Solutions) | + | | |
| **LDAP синхронизация (LDAP Sync)** | | + | | |
| **Уведомления (Notifications)** | | + | + | |
| **Роли БД (DB roles)** | | + | + | |
| **Настройки (Settings)** | | + | | |

### 2.4.3. Двухкомпонентная ролевая модель

Предустановленные роли в компоненте должны ассоциироваться с одноименными групповыми ролями в целевой или целевых СУБД, как представлено на схеме 2.16.

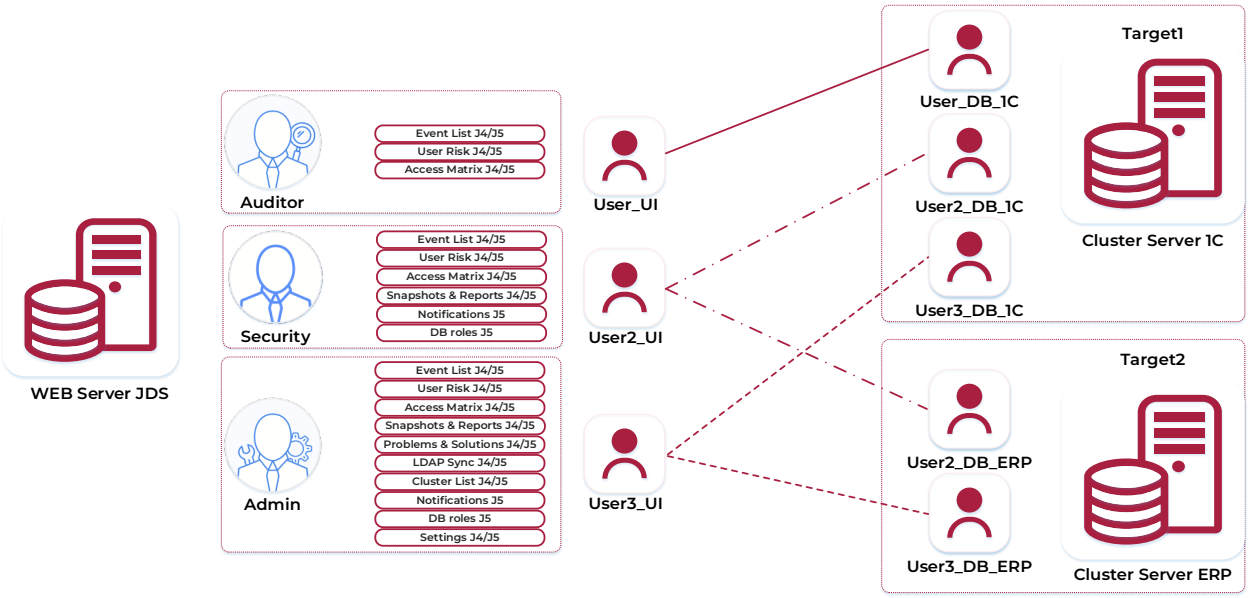


Рисунок 2.16 – Схема двухкомпонентной ролевой модели

На практике, как правило, возникают трудности с предоставлением доступа к «чувствительным» данным.

Использование двухкомпонентной ролевой модели дает безопасное преимущество при доступе сотрудников предприятия и внешних аудиторов к оценке состояния безопасности СУБД.

По представленной модели сотрудник (субъект доступа) не знает учетных записей, созданных для него в целевых СУБД, что исключает утечку, компрометацию или потерю данных в результате ошибочных действий.

Доступ к целевой СУБД осуществляется через ассоциированную учетную запись, которая неизвестна сотруднику, т.е. через функциональные возможности компонента возможно оценить целевую СУБД без прямого доступа к таковой.

Такой подход не только реализует ролевую модель управления доступом внутри компонента «Jatoba data safe», но и выполняет меру защиты информации РСБ.7, описанную в п. 3.4.4.

# 3. МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ

Состав и содержание организационных и технических мер защиты информации определяют следующие нормативные акты:

– Приказ ФСТЭК России № 17 от 11.02.2013 (ред. от 28.08.2024) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

– Приказ ФСТЭК России № 21 от 18.02.2013 (ред. от 14.05.2020) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (Зарегистрировано в Минюсте России 14.05.2013 № 28375);

– Приказ ФСТЭК России № 31 от 14.03.2014 (ред. от 15.03.2021) «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»;

– Приказ ФСТЭК России № 239 от 25.12.2017 (ред. от 28.08.2024) «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;

– ГОСТ Р 57580.1-2017. Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер" (утв. и введен в действие Приказом Росстандарта от 08.08.2017 № 822-ст).

В таблице 3.1 приведены выполняемые меры защиты информации в соответствии с Приказами ФСТЭК России № 17 от 11.02.2013 (ред. от 28.08.2024), № 21 от 18.02.2013 (ред. от 04.05.2020), № 31 от 14.03.2014 (ред. от 15.03.2021), № 239 от 25.12.2017 (ред. от 28.08.2024) и ГОСТ Р 57580.1-2017 от 08.08.2017.

Таблица 3.1 – Реализуемые меры защиты информации

| Наименование | J4 | | J5 | | J6 | | ГОСТ Р 57580.1-2017 | Приказы ФСТЭК | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | ГИС | ИСПДн | КИИ и КВО |
| | Дист.[1] | Обр.к.[2] | Дист.[1] | Обр.к.[2] | Дист.[1] | Обр.к.[2] | | №17 | №21 | №239, №31 |
| Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ) | X | X | X | X | X | X | УЗП.1<br>РД.1<br>РД.3<br>РД.30 | ИАФ.1 | ИАФ.1 | ИАФ.1 |
| | X | X | X | X | X | X | — | ИАФ.3 | ИАФ.3 | ИАФ.3 |
| | X | X | X | X | X | X | РД.11<br>РД.23 | ИАФ.4 | ИАФ.4 | ИАФ.4 |
| | X | X | X | X | X | X | РД.19<br>РД.20<br>РД.21<br>РД.22 | ИАФ.4(1г) | — | — |
| | — | — | X | X | X | X | — | ИАФ.4(2) | | |
| | X | X | X | X | X | X | РД.8 | ИАФ.5 | ИАФ.5 | — |
| Управление доступом субъектов доступа к объектам доступа (УПД) | X | — | X | — | X | — | УЗП.8<br>УЗП.18 | — | — | |
| | X | X | X | X | X | X | УЗП.3 | УПД.1 | УПД.1 | УПД.1 |
| | X | X | X | X | X | X | — | УПД.1(1) | — | — |
| | X | X | X | X | X | X | УЗП.3<br>УЗП.13 | УПД.1(2) | — | — |
| | X | X | X | X | X | X | УЗП.15 | УПД.1(3б) | — | — |
| | — | — | X | — | X | — | — | УПД.1 (5) | — | — |
| | X | X | X | X | X | X | УЗП.10<br>УЗП.11<br>РД.31<br>РД.32<br>РД.33<br>МАС.4 | УПД.2 | УПД.2 | УПД.2 |
| | X | X | X | X | X | X | — | УПД.2(1) | — | — |
| | X | — | X | — | X | — | — | УПД.4 | УПД.4 | УПД.4 |
| | X | X | X | X | X | X | — | УПД.5 | УПД.5 | УПД.5 |
| | X | X | X | X | X | X | РД.11 | УПД.6 | УПД.6 | УПД.6 |
| | | | | | | | — | УПД.6(1) | — | — |
| | X | X | X | X | X | X | РД.12 | УПД.9 | УПД.9 | УПД.9 |
| | X | X | X | X | X | X | — | УПД.9(3) | — | — |
| | — | — | X | — | X | — | — | УПД.9(4) | — | — |
| Регистрация событий безопасности (РСБ) | X | X | X | X | X | X | УЗП.22 | РСБ.2(1а) | — | — |
| | X | X | X | X | X | X | УЗП.23<br>УЗП.24<br>УЗП.25<br>РД.39 | РСБ.3 | РСБ.3 | АУД.4 |

| Наименование | J4 | | J5 | | J6 | | ГОСТ Р 57580.1-2017 | Приказы ФСТЭК | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | ГИС | ИСПДн | КИИ и КВО |
| | Дист.[1] | Обр.к.[2] | Дист.[1] | Обр.к.[2] | Дист.[1] | Обр.к.[2] | | №17 | №21 | №239, №31 |
| | | | | | | | РД.40<br>РД.41<br>РД.42<br>РД.43 | | | |
| | X | — | X | — | X | — | МАС.4 | РСБ.3(1) | — | — |
| | X | X | X | X | X | X | — | РСБ.6 | РСБ.6 | АУД.3 |
| | X | X | X | X | X | X | — | РСБ.7 | РСБ.7 | АУД.6 |
| | X | X | X | X | X | X | — | РСБ.8 | — | АУД.9 |
| | X | — | X | — | X | — | — | РСБ.8(1) | — | — |
| Обеспечение целостности информационной системы и информации (ОЦЛ) | X | X | X | X | X | X | УЗП.11 | ОЦЛ.1 | ОЦЛ.1 | ОЦЛ.1 |
| | X | X | X | X | X | X | — | ОЦЛ.2 | ОЦЛ.2 | ОЦЛ.2 |
| | X | X | X | X | X | X | — | ОЦЛ.7 | ОЦЛ.7 | ОЦЛ.4 |
| Обеспечение доступности информации (ОДТ) | X | — | X | — | X | — | — | ОДТ.4 | ОДТ.4 | ОДТ.4 |
| | X | — | X | — | X | — | — | ОДТ.5 | ОДТ.5 | ОДТ.5 |
| | X | — | X | — | X | — | — | ОДТ.6 (2) | — | ОДТ.7 |
| Контроль отсутствия известных (описанных) уязвимостей защиты информации объектов информатизации | X | X | X | X | X | X | ЦЗИ.8 | — | — | — |

Примечание:

1) Дистрибутив

2) Образ контейнера.

В таблице 3.2 приведены компоненты Изделия выполняющие меры защиты информации.

Таблица 3.2 – Компоненты реализующие меры защиты информации

| Наименование | J4 | | J5 | | J6 | | ГОСТ Р 57580.1-2017 | Приказы ФСТЭК | | | | Диспозиция меры | Компонент |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | СУБД | ГИС | ИСПДн | КИИ и КВО | | |
| | Дист.[1] | Обр.к.[2] | Дист.[1] | Обр.к.[2] | Дист.[1] | Обр.к.[2] | | №64 | №17 | №21 | №239, №31 | | |
| Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ) | X | X | X | X | X | X | УЗП.1<br>РД.1<br>РД.3<br>РД.30 | X | ИАФ.1 | ИАФ.1 | ИАФ.1 | Идентификация и аутентификация пользователей | СУБД |
| | | | | | | | | | | | | | jaDog |
| | X | — | X | — | X | — | | | | | | | JDS |
| | X | X | X | X | X | X | — | — | ИАФ.3 | ИАФ.3 | ИАФ.3 | Управление идентификаторами | СУБД |
| | | | | | | | | | | | | | jaDog |
| | X | X | X | X | X | X | РД.11<br>РД.23 | — | ИАФ.4 | ИАФ.4 | ИАФ.4 | Управление средствами аутентификации | СУБД |
| | X | X | X | X | X | X | РД.19<br>РД.20<br>РД.21<br>РД.22 | X | ИАФ.4(1г) | — | — | Парольные политики | СУБД/ SecurityProfile |
| | X | — | X | — | X | — | | | | | | | JDS |
| | X | — | X | — | X | — | | | | | | | СУБД/ SecurityProfile/JDS |
| | — | — | X | X | X | X | — | — | ИАФ.4(2) | — | — | Генерации паролей | СУБД/pwgen |
| | X | — | X | — | X | — | | | | | | | JDS |
| | X | X | X | X | X | X | РД.8 | X | ИАФ.5 | ИАФ.5 | — | Защита обратной связи | СУБД |
| | X | — | X | — | X | — | | | | | | | JDS |
| | X | X | X | X | X | X | | | | | | | jaDog |
| Управление доступом | X | — | X | — | X | — | УЗП.8<br>УЗП.18 | — | — | — | — | Определение матрицы доступа | JDS |

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

| Наименование | J4 | | J5 | | J6 | | ГОСТ Р 57580.1-2017 | Приказы ФСТЭК | | | | Диспозиция меры | Компонент |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | СУБД | ГИС | ИСПДн | КИИ и КВО | | |
| | Дист.[1] | Обр.к.[2] | Дист.[1] | Обр.к.[2] | Дист.[1] | Обр.к.[2] | | №64 | №17 | №21 | №239, №31 | | |
| субъектов доступа к объектам доступа (УПД) | X | X | X | X | X | X | УЗП.3 | X | УПД.1 | УПД.1 | УПД.1 | Управление пользователями | СУБД |
| | X | — | X | — | X | — | | | | | | | JDS |
| | X | X | X | X | X | X | | | | | | | jaDog |
| | X | X | X | X | X | X | — | — | УПД.1(1) | — | — | Автоматизированного управления УЗ | СУБД/ja_Sync_Ldap |
| | X | — | X | — | X | — | | | | | | | СУБД/ja_Sync_Ldap/ JDS |
| | X | X | X | X | X | X | УЗП.3<br>УЗП.13 | — | УПД.1(2) | — | — | Автоматическое блокирование временных УЗ | СУБД |
| | X | X | X | X | X | X | УЗП.15 | — | УПД.1(3б) | — | — | Автоматическое блокирование неактивных УЗ | СУБД/ SecurityProfile |
| | X | — | X | — | X | — | | | | | | | JDS |
| | — | — | X | — | X | — | — | — | УПД.1(5) | — | — | Автоматический контроль УЗ | СУБД - ja_Log - JDS |
| | X | X | X | X | X | X | УЗП.10<br>УЗП.11<br>РД.31<br>РД.32<br>РД.33<br>МАС.4 | X | УПД.2 | УПД.2 | УПД.2 | Реализация методов, типов и правил разграничения доступа (ролевой / дискреционный) | СУБД |
| | X | — | X | — | X | — | | | | | | | JDS |
| | X | X | X | X | X | X | — | X | УПД.2(1) | — | — | Разграничения доступа при входе | СУБД |
| | X | — | X | — | X | — | — | — | УПД.4 | УПД.4 | УПД.4 | Разделение полномочий пользователей, администраторов | СУБД |
| | X | — | X | — | X | — | | | | | | | JDS |

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

| Наименование | J4 | | J5 | | J6 | | ГОСТ Р 57580.1-2017 | Приказы ФСТЭК | | | | Диспозиция меры | Компонент |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | СУБД | ГИС | ИСПДн | КИИ и КВО | | |
| | Дист.[1] | Обр.к.[2] | Дист.[1] | Обр.к.[2] | Дист.[1] | Обр.к.[2] | | №64 | №17 | №21 | №239, №31 | | |
| | X | X | X | X | X | X | — | — | УПД.5 | УПД.5 | УПД.5 | Минимально необходимые права | СУБД |
| | X | — | X | — | X | — | | | | | | | JDV |
| | | | | | | | | | | | | | JDS |
| | X | X | X | X | X | X | РД.11 | X | УПД.6 | УПД.6 | УПД.6 | Ограничение неуспешных попыток входа | СУБД/ SecurityProfile |
| | X | — | X | — | X | — | | | | | | | JDS |
| | X | X | X | X | X | X | — | X | УПД.6(1) | — | — | Блокирование УЗ при неуспешных попытках входа | СУБД |
| | X | — | X | — | X | — | | | | | | | JDS |
| | X | X | X | X | X | X | РД.12 | X | УПД.9 | УПД.9 | УПД.9 | Ограничение числа параллельных сеансов | СУБД |
| | X | — | X | — | X | — | | | | | | | JDS |
| | X | X | X | X | X | X | — | — | УПД.9(3) | — | — | Контроль и отображение администратору число активных параллельных (одновременных) сеансов | СУБД |
| | X | — | X | — | X | — | | | | | | | JDS |
| | X | — | X | — | X | — | — | — | УПД.9(4) | — | — | Оповещение администратора о превышении числа параллельных сеансов | JDS |
| Регистрация событий безопасности (РСБ) | — | — | X | X | X | X | — | X | РСБ.1 | РСБ.1 | — | Определение событий безопасности, подлежащих | СУБД/ ja_seceventlog |

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

| Наименование | J4 | | J5 | | J6 | | ГОСТ Р 57580.1-2017 | Приказы ФСТЭК | | | | Диспозиция меры | Компонент |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | СУБД | ГИС | ИСПДн | КИИ и КВО | | |
| | Дист.[1] | Обр.к.[2] | Дист.[1] | Обр.к.[2] | Дист.[1] | Обр.к.[2] | | №64 | №17 | №21 | №239, №31 | | |
| | | | | | | | | | | | | регистрации, и сроков их хранения | |
| | — | — | X | X | X | X | — | — | РСБ.1(4а) | — | — | Хранение только записей о выявленных событиях безопасности | СУБД/ ja_seceventlog |
| | X | X | X | X | X | X | УЗП.22 | — | РСБ.2(1а) | — | — | Запись дополнительной информации | pgAudit<br>СУБД/ ja_seceventlog |
| | X | — | X | — | X | — | УЗП.23<br>УЗП.24<br>УЗП.25<br>РД.39<br>РД.40<br>РД.41<br>РД.42<br>РД.43 | X | РСБ.3 | РСБ.3 | АУД.4 | Хранение информации о событиях безопасности в течение установленного времени хранения | СУБД / ja_Log / JDS |
| | X | — | X | — | X | — | МАС.4 | — | РСБ.3(1) | — | — | Централизованное хранение событий безопасности | СУБД / ja_Log/ JDS |
| | X | X | X | X | X | X | — | X | РСБ.6 | РСБ.6 | АУД.3 | Генерирование временных меток | СУБД |
| | X | X | X | X | X | X | — | X | РСБ.7 | РСБ.7 | АУД.6 | Защита информации о событиях безопасности | СУБД |
| | X | — | X | — | X | — | | | | | | | СУБД / ja_Log/ JDS |
| | X | — | X | — | X | — | — | — | РСБ.8 | — | АУД.9 | Просмотра и анализа информации о | СУБД / ja_Log/ JDS |

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

| Наименование | J4 | | J5 | | J6 | | ГОСТ Р 57580.1-2017 | Приказы ФСТЭК | | | | Диспозиция меры | Компонент |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | СУБД | ГИС | ИСПДн | КИИ и КВО | | |
| | Дист.[1] | Обр.к.[2] | Дист.[1] | Обр.к.[2] | Дист.[1] | Обр.к.[2] | | №64 | №17 | №21 | №239, №31 | | |
| | | | | | | | | | | | | действиях отдельных пользователей | |
| | X | — | X | — | X | — | — | — | РСБ.8(1) | — | — | Автоматизированная обработка записей событий безопасности на основе критериев избирательности | СУБД / ja_Log/ JDS |
| Обеспечение целостности информационной системы и информации (ОЦЛ) | X | X | X | X | X | X | УЗП.11 | X | ОЦЛ.1 | ОЦЛ.1 | ОЦЛ.1 | Контроль целостности компонентов | ja_Csum/ SecurityProfile |
| | X | X | X | X | X | X | — | — | ОЦЛ.2 | ОЦЛ.2 | ОЦЛ.2 | Контроль целостности информации | СУБД |
| | X | X | X | X | X | X | — | — | ОЦЛ.7 | ОЦЛ.7 | ОЦЛ.4 | Контроль точности, полноты и правильности данных | СУБД |
| Обеспечение доступности информации (ОДТ) | X | — | X | — | X | — | — | X | ОДТ.4 | ОДТ.4 | ОДТ.4 | Периодическое резервное копирование | pg_proBackup |
| | X | — | X | — | X | — | | | | | | | pg_proBackup/JDS |
| | X | — | X | — | X | — | — | X | ОДТ.5 | ОДТ.5 | ОДТ.5 | Восстановления информации | pg_proBackup |
| | X | — | X | — | X | — | | | | | | | pg_proBackup/JDS |
| | X | X | X | X | X | X | — | X | ОДТ.6 (2) | — | ОДТ.7 | Кластеризация | ja_Dog |
| Ограничение программной среды | X | X | X | X | X | X | — | X | — | — | — | Блокировать загрузку ПО, не включенного в перечень ПО | СУБД/ ja_CSum |

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

| Наименование | J4 | | J5 | | J6 | | ГОСТ Р 57580.1-2017 | Приказы ФСТЭК | | | | Диспозиция меры | Компонент |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | СУБД | ГИС | ИСПДн | КИИ и КВО | | |
| | Дист.[1] | Обр.к.[2] | Дист.[1] | Обр.к.[2] | Дист.[1] | Обр.к.[2] | | №64 | №17 | №21 | №239, №31 | | |
| Контроль отсутствия известных (описанных) уязвимостей защиты информации объектов информатизации | X | X | X | X | X | X | ЦЗИ.8 | — | — | — | — | | |

Примечание:

1) Дистрибутив

2) Образ контейнера.

## 3.1. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)

### 3.1.1. Мера защиты ИАФ.1

СУБД «Jatoba» реализует меру безопасности ИАФ.1 «Идентификация и аутентификация пользователей, являющихся работниками оператора» в части следующих требований:

- идентификация и аутентификация пользователей, являющихся работником оператора;
- аутентификация пользователя осуществляется с использованием паролей.

СУБД поддерживает методы аутентификации:

- PASSWORD;
- GSSAPI;
- LDAP;
- PAM;
- RADIUS;
- SSL;
- SSPI.

Собственным механизмом аутентификации СУБД является метод аутентификации «Password». Данный метод согласно «ГОСТ Р 58833-2020. Национальный стандарт Российской Федерации. Защита информации. Идентификация и аутентификация. Общие положения» осуществляет простую однофакторную аутентификацию с низким уровнем доверия.

Остальные методы аутентификации предполагают установление доверительных отношений между объектом доступа и субъектом доступа на стороне внешних серверов, которые не являются ОО. В свою очередь СУБД доверяет внешнему серверу, которым проведена аутентификация.

Для использования методов аутентификации, использующих механизмы операционной системы (третьей стороны), операционная система должна быть сертифицирована на соответствие уровню доверия не ниже уровню доверия изделия.

Методы аутентификации, использующие доверенную третью сторону, рассматриваются как функциональные возможности СУБД, но не как функциональные возможности безопасности.

Идентификацию и аутентификацию субъектов доступа выполняют:

– СУБД «Jatoba»;

– JDS;

– jaDog.

### 3.1.2. Мера защиты ИАФ.3

СУБД «Jatoba» реализует меру безопасности ИАФ.3 «Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов» в части следующих требований:

– формирование идентификатора, который однозначно идентифицирует пользователя;

– присвоение идентификатора пользователю.

При первичной идентификации пользователя СУБД, т.е. при формировании информации о субъекте доступа и регистрации информации о субъекте доступа в СУБД, ему присваивается уникальный идентификатор.

Идентификатором служит имя пользователя в СУБД и уникальный OID генерируемый автоматически на уровне ядра СУБД. Использование одноименных учетных записей и OID в перечне идентификаторов невозможно.

### 3.1.3. Мера защиты ИАФ.4

СУБД «Jatoba» реализует меру безопасности ИАФ.4 «Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации» в части следующих требований:

– установление характеристик пароля (при использовании в информационной системе механизмов аутентификации на основе пароля):

а) задание минимальной сложности пароля с определяемыми оператором требованиями к регистру, количеству символов, сочетанию букв верхнего и нижнего регистра, цифр и специальных символов;

Алфавит пароля должен задаваться элементами согласно приведенному перечню в таблице 3.3.

Таблица 3.3 – Алфавит пароля

| № | Наименование | Допустимые символы | Количество символов, шт. |
|---|---|---|---|
| 1 | Заглавные буквы | A…Z | 26 |
| 2 | Строчные буквы | a…z | 26 |
| 3 | Цифры | 0…9 | 10 |
| 4 | Специальные символы | \!"#$%&()*+,-./:;<=>?@[]^_`{\|}~ | 25 |
| **Итого:** | | | **93** |

б) задание минимального количества измененных символов при создании новых паролей;

в) задание максимального времени действия пароля;

г) задание минимального времени действия пароля;

д) запрет на использование пользователями определенного оператором числа последних использованных паролей при создании новых паролей;

– защита аутентификационной информации от неправомерного доступа к ней и модифицирования.

Данная функция безопасности реализована в интерфейсе компонента JDS.

**3.1.3.1 Усиление ИАФ.4 (1г)**

СУБД «Jatoba» реализует усиление меры защиты ИАФ.4 (1г) в части следующих требований:

– СУБД обеспечивает (в парольной политике FSTEC _1_Class) длину 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.

СУБД управляет средствами аутентификации используя внутренние собственные механизмы, но для установления парольных политик использует расширение SecurityProfile (подробное применение расширения SecurityProfile описано в документе «Руководство администратора» 643.72410666.00067-07 95 01). Расширение имеет профиль парольной политики по умолчанию и позволяет создавать собственные профили. К профилям привязываются различные группы пользователей и технические учетные записи.

При использовании сертифицированных СЗИ более высокого уровня доверия, чем требует класс или категория информационной системы, для разных типов учетных записей, для разных типов информационных систем в зависимости от класса защищенности, с использованием рекомендаций и т.п., были созданы преднастроенные профили парольных политик:

- FSTEC_1_class – профиль для ИС первого класса защищенности (Приложение 1. Параметры парольной политики FSTEC _1_Class. Таблица П1.2);
- FSTEC_2_class – профиль для ИС второго класса защищенности (Приложение 1. Параметры парольной политики FSTEC _2_Class. Таблица П1.3);
- CIS – профиль, основанный на рекомендациях Center for Internet Security (Приложение 1. Параметры парольной политики CIS. Таблица П1.4);
- Corporate_1 – корпоративный профиль первого уровня для учетных записей пользователей (Приложение 1. Параметры парольной политики Corporate_1. Таблица П1.5);
- Corporate_2 – корпоративный профиль второго уровня для учетных записей администраторов программных (программно-аппаратных) средств (Приложение 1. Параметры парольной политики Corporate_2. Таблица П1.6);
- 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 (Приложение 1. Параметры парольной политики Corporate_3. Таблица П1.7).

Усиления меры защиты ИАФ.4 (1) требуют использование в алфавите пароля от 30 до 70 символов, что ограничивает конечного пользователя Изделия в формировании парольных политик, поэтому алфавит пароля увеличен до 93 символов, как приведено в таблице 3.3.

Защита аутентификационной информации от неправомерного доступа к ней и модифицирования обеспечивается организационными мерами безопасности на уровне операционной системы, установлением прав на каталог журнала аудита.

Данная функция безопасности реализована в интерфейсе компонента JDS.

Компонент JDS управляет парольными политиками:

— СУБД;

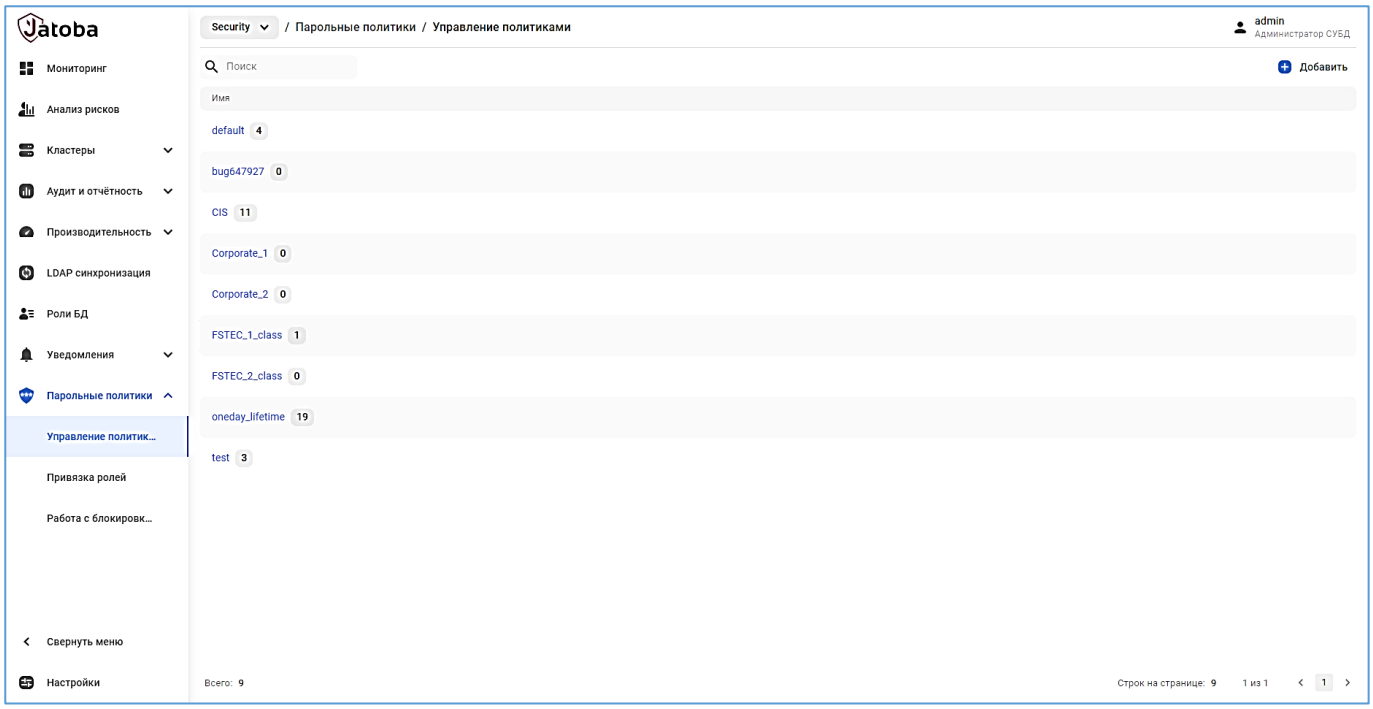


Рисунок 3.1 – Вкладка «Редактирование политик»

— парольными политиками самого компонента.

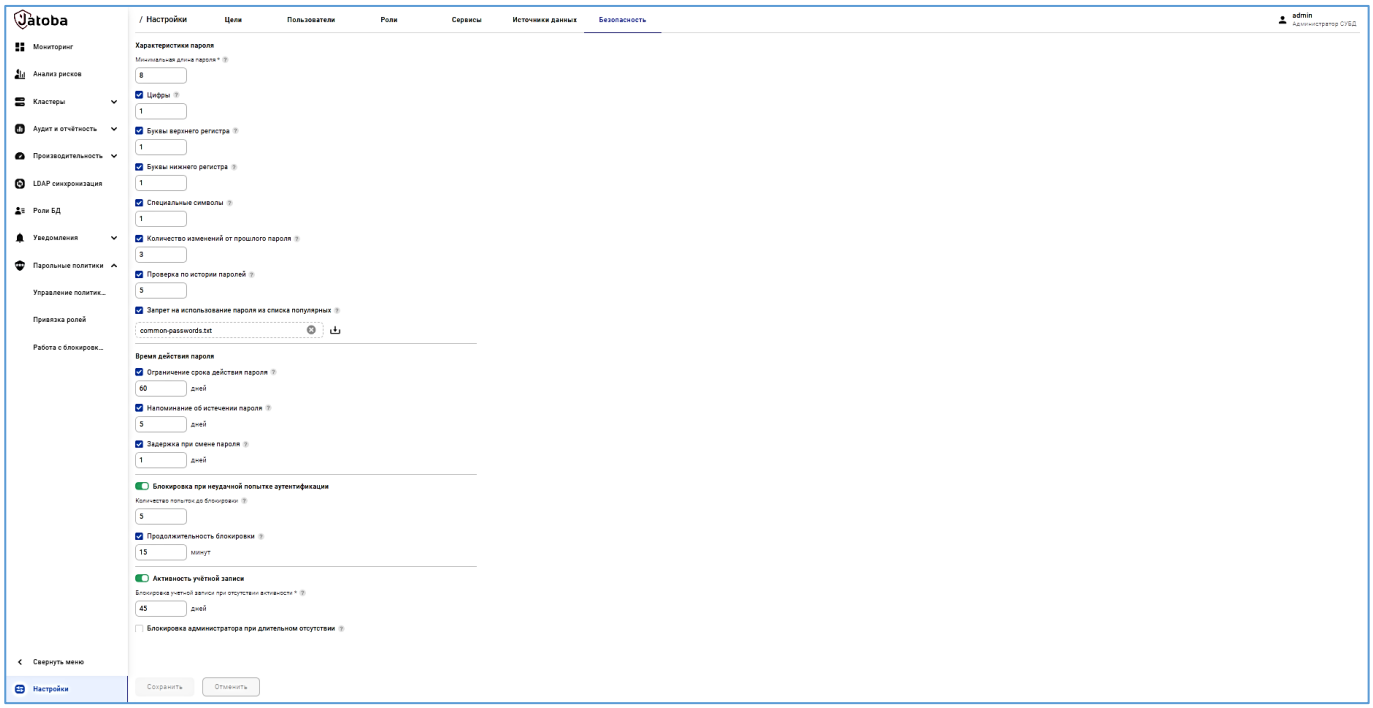


Рисунок 3.2 - Вкладка «Безопасность»

Дополнительно, на уровне СУБД, реализована функциональная возможность маскирования паролей в журнале аудита СУБД. Режим маскирования паролей в журнале аудита устанавливается в конфигурационном файле postgresql.conf параметром:

```
log_mask_password=1
```

Рисунок 3.3 – Параметры postgresql.conf обязательные для маскирования паролей

Отключить режим маскирования паролей SQL-командой невозможно.

В результате каждая SQL-команда, связанная с установкой паролей, в журнале аудита будет отражаться с маскированным паролем.

**Например**

Создается пользователь СУБД с паролем SQL-командой:

```
CREATE USER user1 with password 'n123456';
```

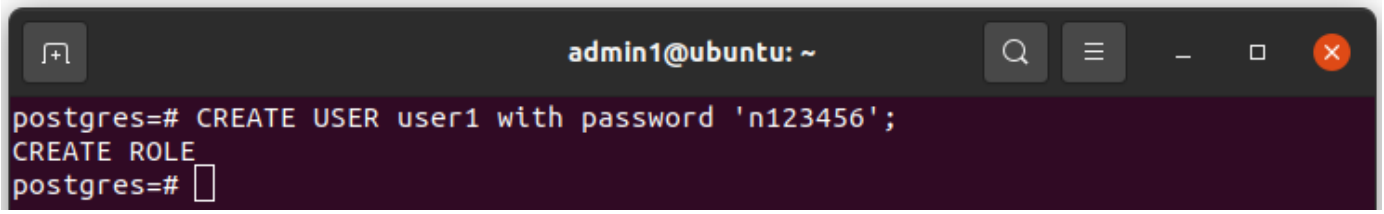


Рисунок 3.4 – SQL-команда создания пользователя

В журнале аудита СУБД установленный пароль будет маскирован.

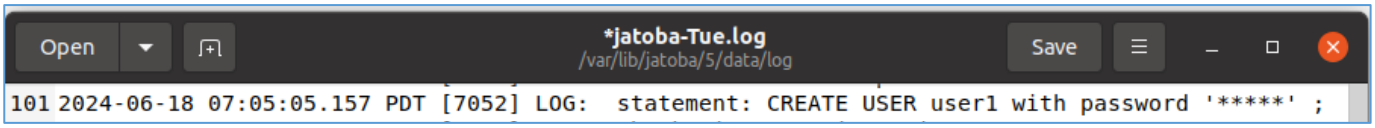


Рисунок 3.5 – Журнал аудита СУБД с записью создания пользователя

**3.1.3.2 Усиление ИАФ.4 (2)**

СУБД «Jatoba» реализует усиление меры защиты ИАФ.4 (2) в части следующего требования:

– использование автоматизированных средств формирования аутентификационной информации (генерации паролей) с требуемыми характеристиками стойкости (силы) механизма аутентификации.

В СУБД «Jatoba» реализована встроенная функция «pwgen», предназначенная для генерации пароля либо множества паролей по заданным параметрам.

**Например**

Генерация пароля выполняется SQL-командой:

```
# SELECT pwgen(10,2,2,1,1,'abcde','ABCDE','@!');
```

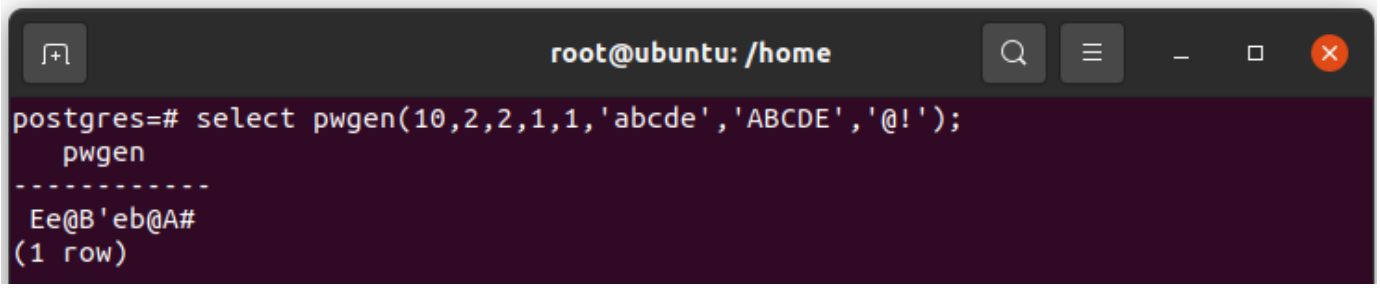


Рисунок 3.6 – SQL-команда генерации пароля по последовательности параметров

Генерация множества паролей выполняется SQL-командой:

```
SELECT pwgen() from generate_series(1, 10);
```

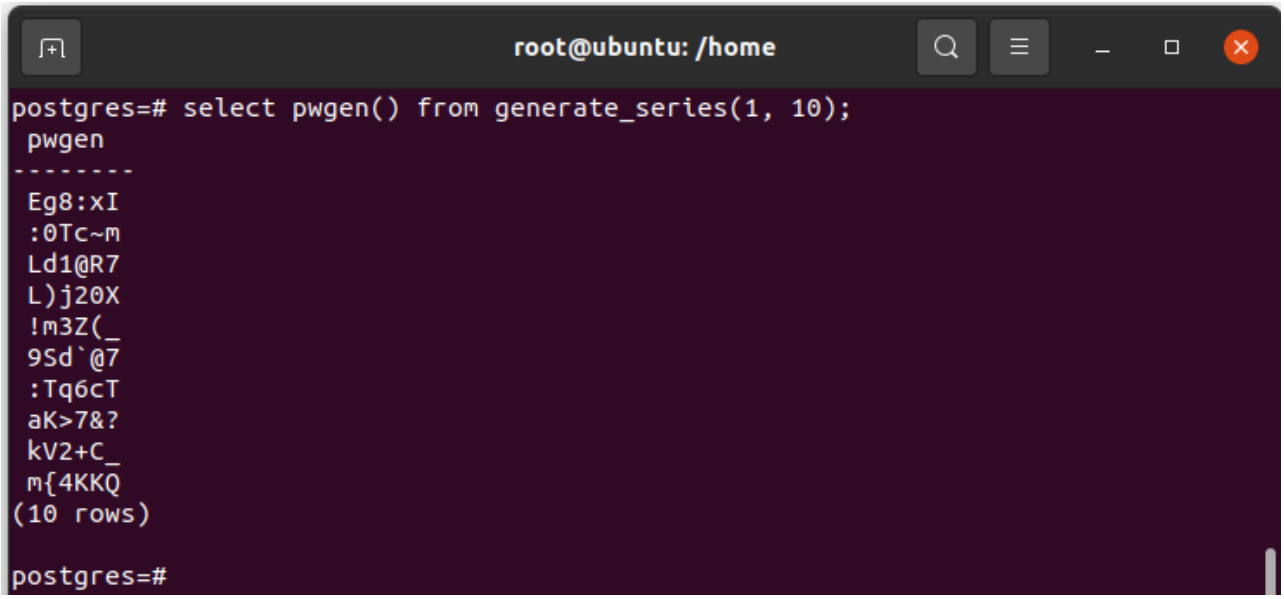


Рисунок 3.7 – Генерация множества паролей

Генерация пароля в соответствии с установленными параметрами, в JDS выполняется для пользователей компонента:

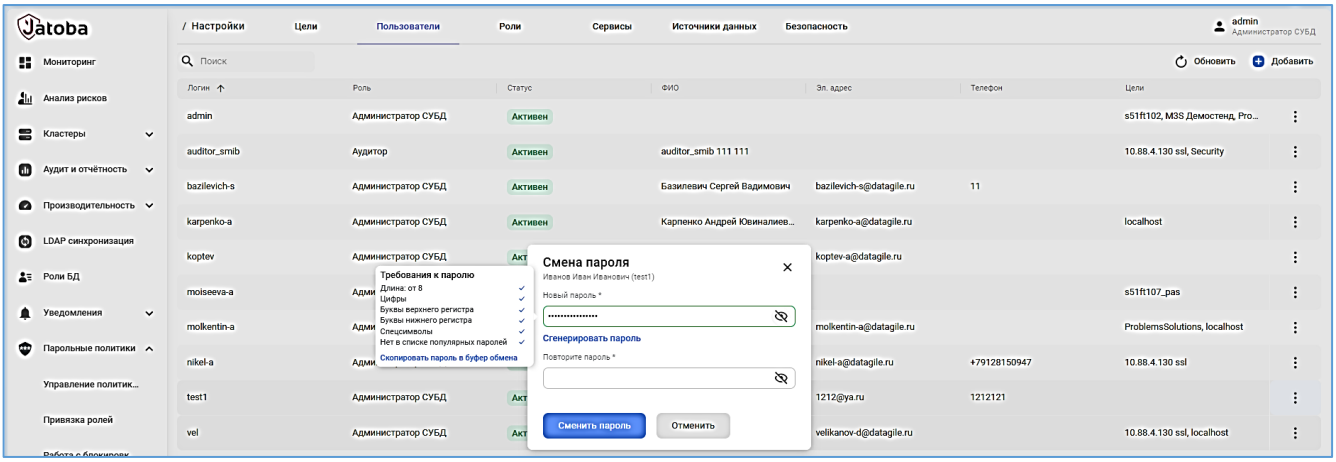


Рисунок 3.8 – Окно смены пароля

### 3.1.4. Мера защиты ИАФ.5

СУБД «Jatoba» реализует меру безопасности (ИАФ.5) «Защита обратной связи при вводе аутентификационной информации» в части следующего требования:

– защита обратной связи при вводе аутентификационной информации путем исключения отображения для пользователя действительного значения аутентификационной информации с заменой вводимых символов пароля условным знаком «•».

В стандартном компоненте CLI пароль, вводимый пользователем, не отображается. В приложении JDS используется только метод аутентификации password и при аутентификации пользователей вводимый пароль не отображается. В разделах настройки приложения пароль также не отображается.

Аналогично пароль, вводимый пользователем, не отображается в компонентах:

— JDS;

— jaDog;

## 3.2. Управление доступом субъектов доступа к объектам доступа (УПД)

### 3.2.1. Мера защиты УПД.1

СУБД «Jatoba» реализует меру безопасности УПД.1 «Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей» в части следующих требований:

– объединение учетных записей в группы;

– заведение, активацию, блокирование и уничтожение учетных записей пользователей;

– уничтожение временных учетных записей пользователей, предоставленных для однократного (ограниченного по времени) выполнения задач в информационной системе.

Заведение, блокирование и уничтожение УЗ доступно в компоненте jaDog.

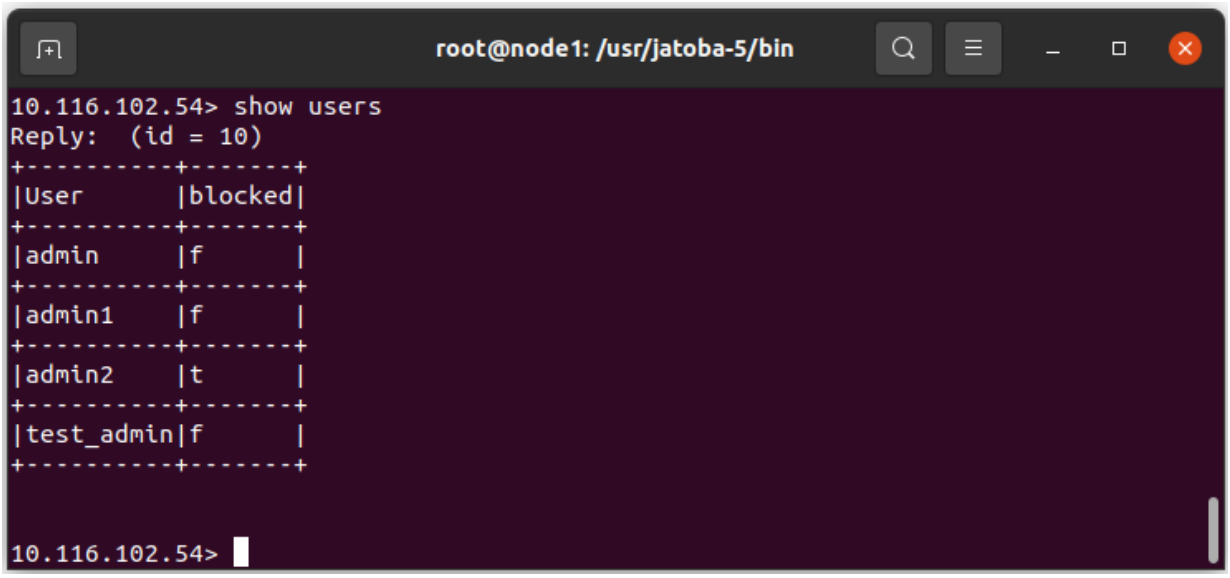


Рисунок 3.9 – Просмотр учетных записей в кластере

Компонент JDS, для собственных пользователей, выполняет меру защиты информации УПД.1 в части требований по

– заведение, активацию, блокирование и уничтожение учетных записей пользователей.

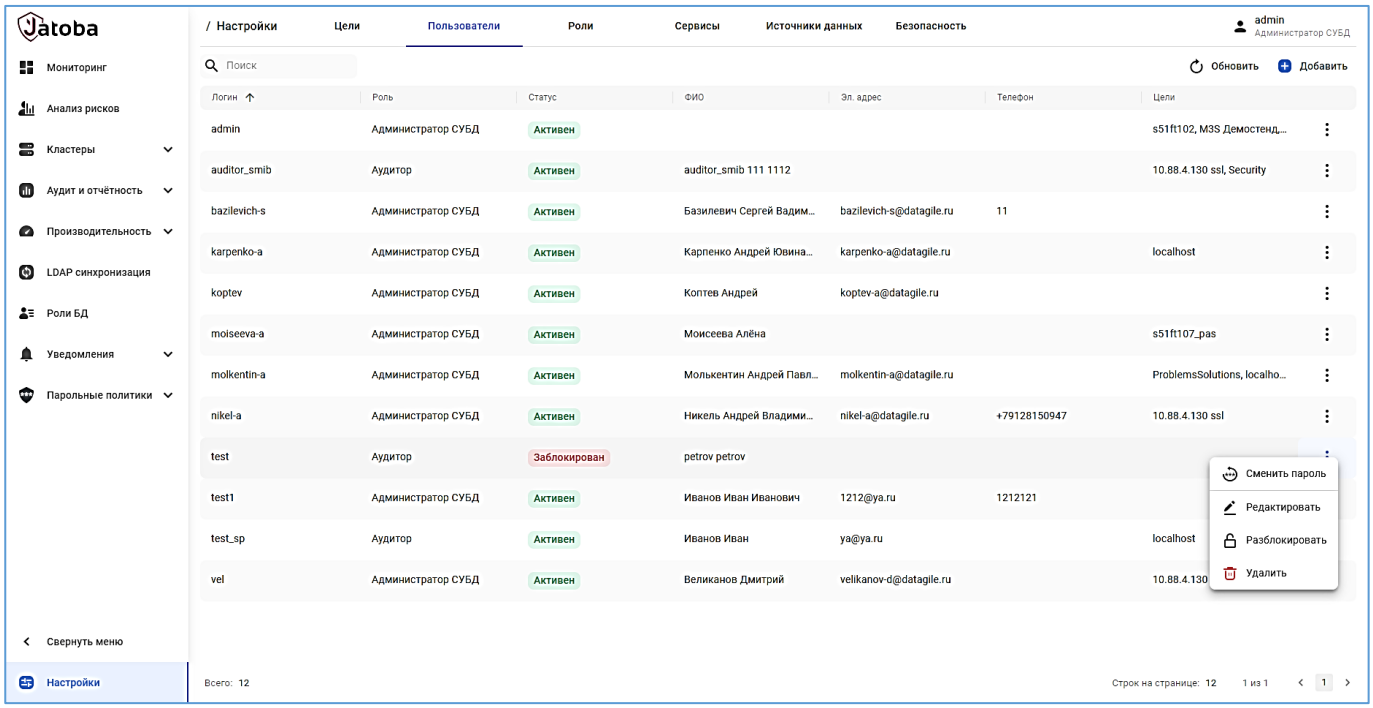


Рисунок 3.10 – Управление пользователями JDS

В разделе «Роли БД» (DB ROLES) JDS выполняет все вышеперечисленные функциональные возможности безопасности, за исключением блокирования/разблокирования УЗ целевой СУБД.

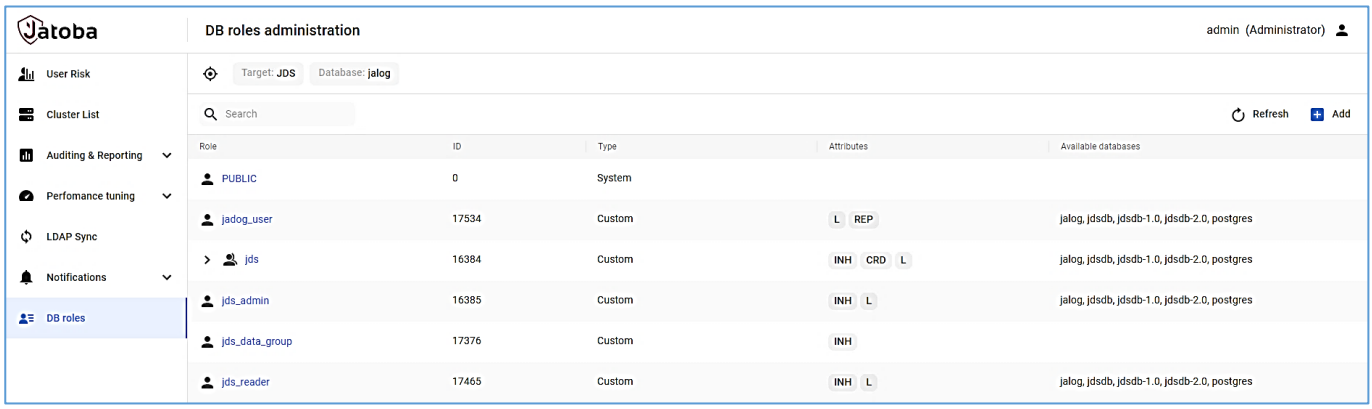


Рисунок 3.11 – Окно списка пользователей

#### 3.2.1.1. Усиление УПД.1(1)

СУБД «Jatoba» реализует усиление меры защиты УПД.1(1) в части следующего требования:

– автоматизированное управление учетными записями пользователей имеющих роль «Право входа».

Для функциональных возможностей безопасности, таких как заведение, активация, блокирование и уничтожение учетных записей пользователей СУБД использует встроенные механизмы и специальные расширения. К такому расширению относится ja_Sync_LDAP, которое позволяет:

- создавать профили синхронизации;
- создавать и привязывать профили маппинга к профилям синхронизации;
- синхронизировать учетные записи пользователей.

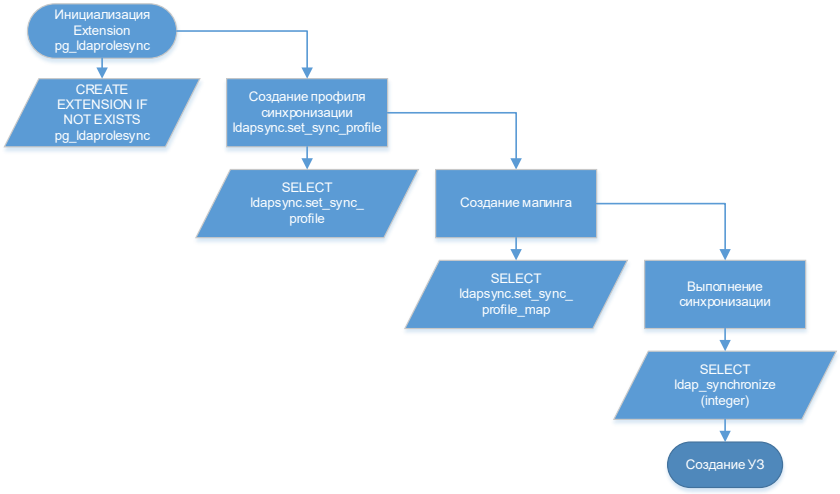


Рисунок 3.12 – Блок-схема формирования пользователей

Синхронизация учетных записей возможна если пользователи в активном каталоге внесены в специальную группу, и со стороны СУБД создан профиль синхронизации и профиль маппинга. В процессе синхронизации учетным записям могут быть назначены атрибуты ролей напрямую или созданные учетные записи буду включены в групповую роль и наследовать атрибуты ролей от нее.

Компонент ja_Sync_LDAP может функционировать вместе с компонентом JDV. При этом пользователь от имени и с правами которого синхронизируются учетные записи должен входить в группу «dv_acctmgr».

Полностью работа компонента ja_Sync_LDAP описана в документе 643.72410666.00067-07 98 01-08 «Руководство по настройке. Часть 8. Синхронизация учетных записей служб каталогов и СУБД. Компонент «ja_Sync_LDAP».

Выполнение синхронизации пользователей также доступно из приложения JDS, работа которого описана в документе 643.72410666.00067-07 98 01-07 «Руководство по

настройке. Часть 7. Пользовательский веб-интерфейс для администраторов. Компонент «Jatoba data safe».

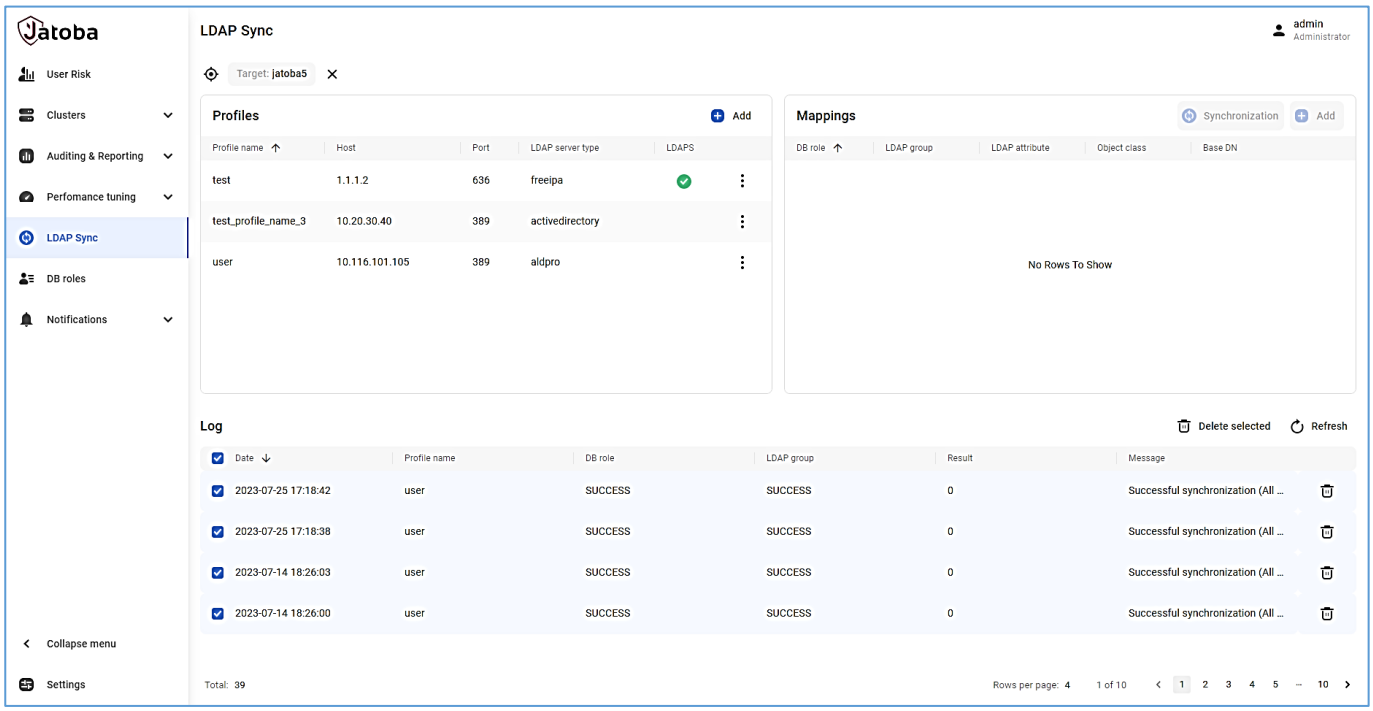


Рисунок 3.13 –Раздел «LDAP синхронизация» (LDAP SYNC)

#### 3.2.1.2. Усиление УПД.1(2)

СУБД «Jatoba» реализует усиление меры защиты УПД.1(2) в части следующего требования:

– СУБД автоматически блокирует учетные записи пользователей имеющих роль «Право входа» по окончании установленного периода для их использования.

СУБД автоматически блокирует учетные записи пользователей, для которых установлен параметр «VALID UNTIL».

#### 3.2.1.3. Усиление УПД.1(3б)

СУБД «Jatoba» реализует усиление меры защиты УПД.1(3б) в части следующего требования:

3) в информационной системе должно осуществляться автоматическое блокирование неактивных (неиспользуемых) учетных записей пользователей после периода времени неиспользования:

б) более 45 дней.

Данное требование выполняется установкой параметра ser_idle_days_max в компоненте парольных политик «securityprofile»:

```
set_profile_user_idle_days_max(profile, кол-во_дней);
```

Компонент JDS для собственных пользователей в разделе «Безопасность», в параметре парольной политики «Активность учётной записи» устанавливает период неактивности 45 дней с последующим блокированием.

#### 3.2.1.4. Усиление УПД.1(5)

Компонент JDS СУБД «Jatoba» реализует усиление меры защиты УПД.1(5) в части следующего требования:

– оповещение администратора, об изменении сведений о пользователях, их ролях, обязанностях, полномочиях, ограничениях.

Для реализации потребуется создать канал событий в разделе «Уведомления» в компоненте JDS.

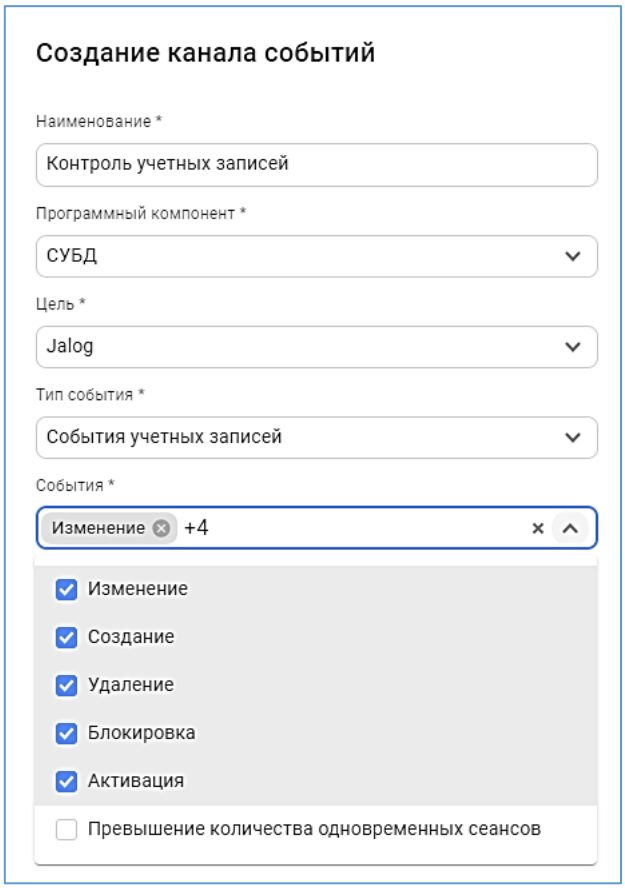


Рисунок 3.14 – Настройка канала событий для контроля УЗ

При создании канала событий должны быть выбраны параметры:

— Программный компонент – «СУБД»;

— Цель – служебная БД «ja_Log»;

— Тип события – «События учетных записей»;

— События – «Изменение», «Создание», «Удаление», «Блокировка» и «Активация».

На контролируемой СУБД должен быть установлен агент компонента «ja_Log» который будет передавать журнал событий в служебная БД «ja_log».

Компонент JDS периодически будет просматривать служебную БД «ja_log» выбирать события безопасности и при их нахождении перешлет сообщение через сервисы E-mail и/или Zulip.

### 3.2.2. Мера защиты УПД.2

СУБД «Jatoba» выполняет меру безопасности УПД.2 «Реализация необходимых методов (дискреционный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа в части следующих требований:

– СУБД обеспечивает дискреционный метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе идентификационной информации субъекта и для каждого объекта доступа - списка, содержащего набор субъектов доступа (групп субъектов) и ассоциированных с ними типов доступа, поддерживая права субъекта доступа, указанных в таблице 3.5, к объектам доступа указанных в таблице 3.4.

СУБД имеет встроенный механизм дискреционного разграничения доступа. Объекты доступа представлены в таблице 3.4.

Таблица 3.4 – Объекты доступа

| № | Наименование | Описание |
|---|---|---|
| 1 | СУБД | Система управления базами данных |
| 2 | БД | Базы данных |

| № | Наименование | Описание |
|---|---|---|
| 3 | Системные привилегии в СУБД и БД | Право на выполнения общесистемных действий на уровне СУБД |
| 4 | Схемы | Пространство имен образующее логическую структуру БД из именованных объектов |
| 5 | Таблицы | Объект БД, представляющий собой именованный набор строк и столбцов с назначенным для столбцов типом данных |
| 6 | Представления | Представления – это способ отображения данных одной или множества таблиц, генерирующийся в момент выполнения запроса |
| 7 | Материализованные представления | Объект БД содержащий результаты выполнения запроса хранящийся на диске, данные в котором наполняются либо изменяются с помощью запроса |
| 8 | Функции | Набор операторов и выражений на SQL реализующий законченное действие по обработке данных |
| 9 | Последовательности | Последовательностью (sequence) называется объект базы данных использующийся для автоматического присвоения уникальных значений в таблицах |

Дискреционный метод управления доступом реализован на уровне БД: пользователи, т.е. субъекты доступа, могут получить доступ в зависимости от назначенных им привилегий.

Таблица 3.5 – Привилегии пользователей на вложенные объекты уровня БД

| Привилегия | Назначение | Описание | Объект распространения |
|---|---|---|---|
| Select | Чтение | Отображает данные объекта хранения | Таблица, представление, материализованное представление, последовательность |
| Insert | Создание | Вносит данные в объект хранения | Таблица, представление, материализованное представление |

| Привилегия | Назначение | Описание | Объект распространения |
|---|---|---|---|
| Update | Изменение | Изменяет данные в объекте хранения | Таблица, представление, последовательность |
| Delete | Удаление | Удаляет строку из объекта хранения | Таблица, представление, материализованное представление |
| Truncate | Удаление всех строк | Удаляет все строки объекта хранения | Таблица |
| Execute | Выполнение | Выполнение функции | Функция |
| USAGE | Чтение текущего значения или его инкремент | Счетчик | Последовательность |

– СУБД обеспечивает ролевой метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе ролей субъектов доступа.

Ролевой метод управления доступом основан на присвоении ролям атрибутов, приведенных в таблице 3.6. Ролевая модель может меняться в зависимости от применяемых расширений (как описано в разделах 3.2.3, 3.2.4) и приложений СУБД.

При эксплуатации приложения «Jatoba data safe» используется двухкомпонентная ролевая модель.

Таблица 3.6 – 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 |

| Атрибут | Условный перевод | Описание |
|---|---|---|
| SUPERUSER | Суперпользователь | Роль «Суперпользователь» обладает полными правами доступа к СУБД |
| 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 обеспечивает разграничение доступа к системным привилегиям в самой СУБД и в БД в соответствии с таблицей 3.7.

Реализация ролевой модели доступа не ограничивается назначением атрибутов ролей. СУБД позволяет разграничивать доступ к объектам доступа на уровне системных привилегий. Администратор БД, при наличии достаточных полномочий, может назначить пользователю или технической учетной записи системные привилегии.

Таблица 3.7 – Системные привилегии для ролей с атрибутом «LOGIN»

| № | Наименование | Описание |
|---|---|---|
| 1 | SELECT LARGE OBJECT | Получение больших объектов |
| 2 | SELECT SEQUENCE | Получение значения счетчиков |
| 3 | UPDATE LARGE OBJECT | Изменение данных в больших объектах |

| № | Наименование | Описание |
|---|---|---|
| 4 | UPDATE SEQUENCE | Обновление значения счетчиков |
| 5 | TRIGGER TABLE | Установка триггеров на таблицы |
| 6 | REFERENCES TABLE | Использование зависимых таблиц |
| 7 | REFERENCES TABLE COLUMN | Использование колонок зависимых таблиц |
| 8 | CREATE DATABASE | Создание базы данных |
| 9 | CREATE SCHEMA | Создание схемы |
| 10 | CREATE TABLESPACE | Создание табличного пространства |
| 11 | CONNECT DATABASE | Подключение к базе данных |
| 12 | TEMPORARY DATABASE | Использование временных таблиц |
| 13 | EXECUTE FUNCTION | Выполнение функций |
| 14 | EXECUTE PROCEDURE | Выполнение процедур |
| 15 | USAGE DOMAIN | Использование домена |
| 16 | USAGE FOREIGN DATA WRAPPER | Использование внешних источников данных |
| 17 | USAGE FOREIGN SERVER | Использование внешних серверов |
| 18 | USAGE LANGUAGE | Использования языка программирования |
| 19 | USAGE SCHEMA | Использование схемы |
| 20 | USAGE SEQUENCE | Использование счетчика |
| 21 | USAGE TYPE | Использование тип |

#### 3.2.2.1. Усиление УПД.2(1)

СУБД «Jatoba» реализует усиление меры защиты УПД.2(1) в части следующего требования:

– СУБД обеспечивает правила разграничения доступа субъектов при входе в информационную систему.

Методы разграничения доступа реализуются встроенными средствами СУБД, которые применяются при входе субъекта доступа в СУБД.

Для реализации усиления меры УПД.2(1) имеются эксплуатационные ограничения, к которым относится запрет на использование метода аутентификации «Trust».

### 3.2.3. Мера защиты УПД.4

СУБД «Jatoba» выполняет меру безопасности УПД.4 «Разделение обязанностей полномочий (ролей), администраторов и лиц, обеспечивающих функционирование информационной системы» в части следующего требования:

– СУБД обеспечивает разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы и санкционирование доступа к объектам доступа в соответствии с разделением полномочий (ролей).

Выполнение меры защиты обусловлено встроенной ролевой моделью, в которой:

– пользователями являются роли с атрибутом «Login»;

– администраторами БД – роли с атрибутами «CreateRole» и «Replication»;

– администраторами СУБД – роли с атрибутом «Superuser».

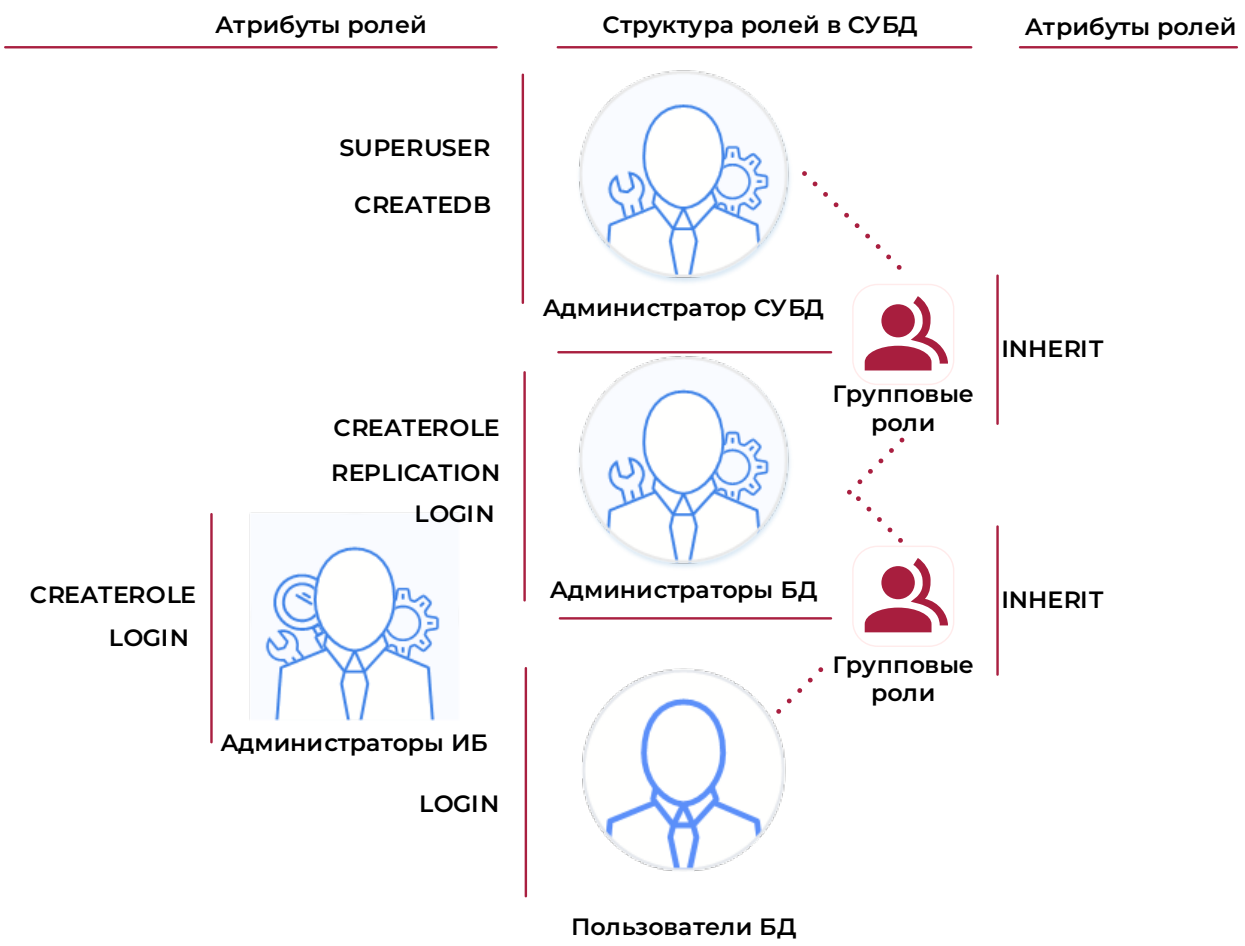


Рисунок 3.15 – Схема структуры атрибутов ролей

Дополнительно к условиям выполнения меры можно отнести назначение пользователям системных привилегий.

В компоненте JDS встроенной ролевой моделью разделена доступность разделов компонента и соответственно доступ к их функциональным возможностям.

Предусмотрены роли:

— Admin (Администратор СУБД);

— Security (Администратор ИБ);

— Auditor (Аудитор);

— DB developer (Разработчик БД).

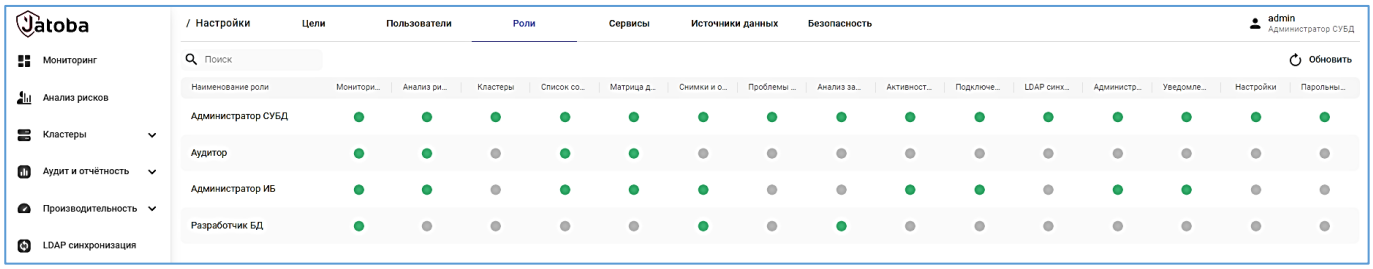


Рисунок 3.16– Вкладка «Роли» JDS

### 3.2.4. Мера защиты УПД.5

СУБД «Jatoba» выполняет меру безопасности УПД.5 «Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы» в части следующего требования:

– СУБД обеспечивает назначение прав и привилегий пользователям и запускаемым от их имени процессам, администраторам и лицам, обеспечивающим функционирование информационной системы, минимально необходимых для выполнения ими своих должностных обязанностей (функций), и санкционирование доступа к объектам доступа в соответствии с минимально необходимыми правами и привилегиями.

Меры УПД.4 и УПД.5 логически связаны между собой, т.к. требуют разделения полномочий. Ролевая модель СУБД разграничивает роли на пользователей, администраторов и лиц, обеспечивающих функционирование ИС.

Для назначения минимально необходимых прав и привилегий вышеописанным лицам применяется расширение JDV. Расширение описано в документе 643.72410666.00067-07 98 01-02 «Руководство по настройке. Часть 2. Контроль субъектов доступа. Компонент «Jatoba data vault».

Типовая ролевая модель СУБД, представленная на рисунке 3.17, при использовании расширения JDV изменяется.

Условная группа «Администраторы БД» разделяется на дополнительные роли с переходом функциональных возможностей по:

– администрированию защищаемых таблиц и пользователей;

– мониторингу ролей, объектов и схем;

– администрированию пользователей.

Ролевая модель состоит из:

- Администраторов баз данных (Database administrator);
- Администраторов безопасности (Security administrator);
- Аудиторов (Auditor);
- Администраторов пользователей (User administrator);
- Защищаемых и обычных пользователей (Protected users & users).

Для администрирования защищаемых таблиц и пользователей администратор безопасности (Security administrator) имеет роль «dv_owner», при этом он не имеет функциональных возможностей по администрированию пользователей.

Аудитор (Auditor) отнесен к групповой роли «dv_secanalyst» и его функциональные возможности ограничены просмотром событий безопасности, генерируемых компонентом JDV.

Администратор пользователей (User administrator) отнесен к роли «dv_acctmgr» и имеет эксклюзивную функциональную возможность по администрированию пользователей, включающую в том числе смену паролей пользователей.

Защищаемые пользователи (Protected users), являющиеся владельцами таблиц(ы) и (или) имеющие специальное разрешение на доступ к защищаемому объекту, относятся к групповой роли «dv_group».

Остальные пользователи (users) могут относится к любым другим групповым ролям.

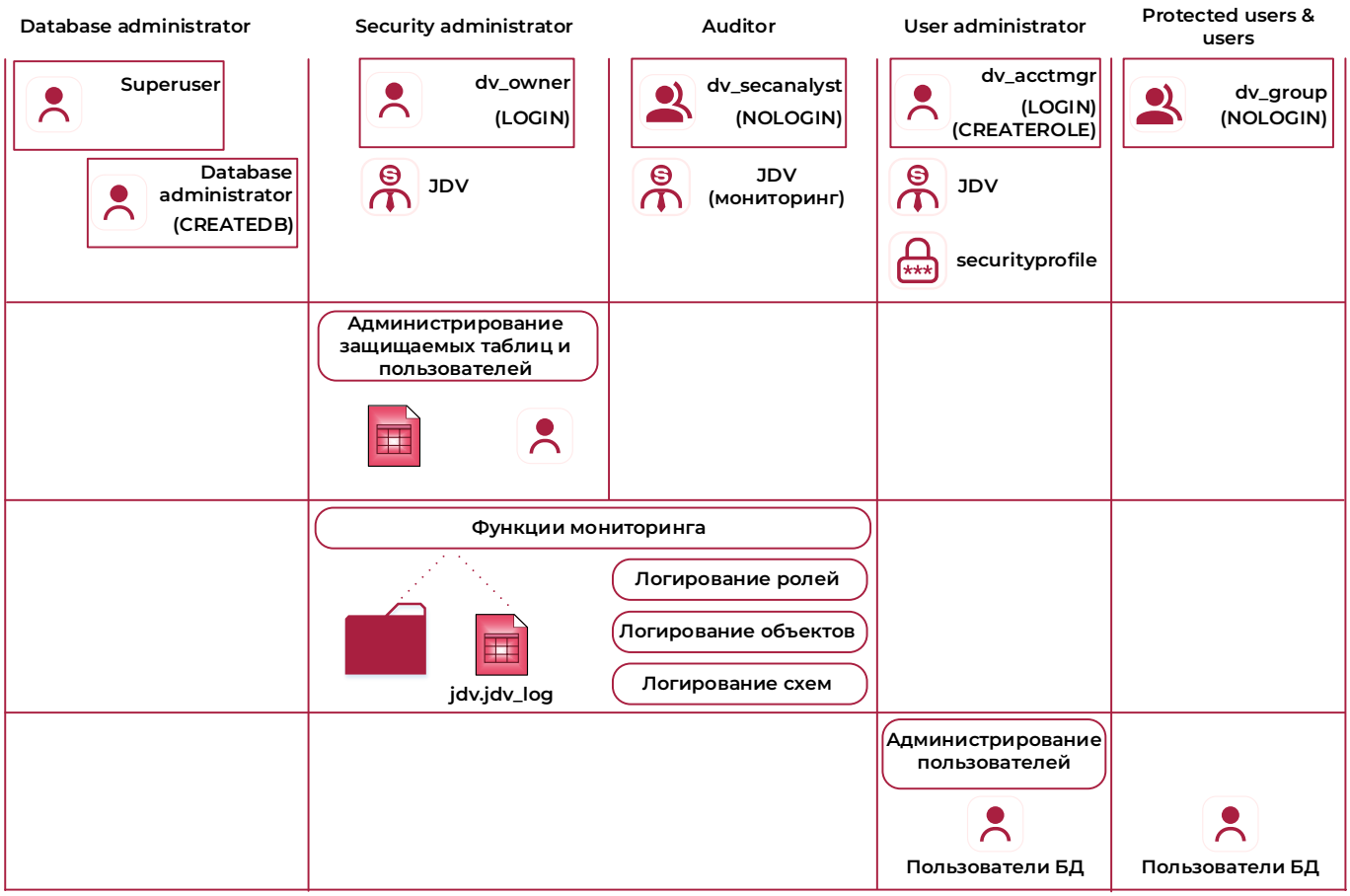


Рисунок 3.17 – Распределение функциональных возможностей

В компоненте JDS двухкомпонентная ролевая модель доступа реализует функцию безопасности назначения минимально необходимых прав и привилегий пользователям.

### 3.2.5. Мера защиты УПД.6

СУБД «Jatoba» выполняет меру безопасности УПД.6 «Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)» в части следующих требований:

– СУБД обеспечивает блокирование учетной записи с атрибутом «Login» при превышении пользователем ограничения количества неуспешных попыток входа в информационную систему.

Ограничение количества неуспешных попыток входа в информационную систему (доступа к информационной системе) должно обеспечиваться в соответствии с ИАФ.4 и реализовано в параметре securityprofile.failed_login_attempts расширения SecurityProfile.

Компонент JDS в разделе «Парольные политики», при установленном компоненте SecurityProfile на целевой СУБД имеет возможность управления параметрами парольных политик, в частности параметром «Блокировка при неудачной попытке аутентификации».

Идентичным параметром JDS управляет для собственных пользователей в разделе «Безопасность».

#### 3.2.5.1. Усиление УПД.6(1)

СУБД «Jatoba» реализует усиление меры защиты УПД.6(1) в части следующего требования:

– СУБД обеспечивает автоматическое блокирование учетной записи пользователя при превышении пользователем ограничения количества неуспешных попыток входа в информационную систему (доступа к информационной системе) за установленный период времени с возможностью разблокирования только администратором или иным лицом, имеющим соответствующие полномочия (роль).

При инициализированном расширении SecurityProfile устанавливаются параметры:

– securityprofile.failed_login_attempts – количество неудачных попыток аутентификации;

– securityprofile.failed_login_attempts_max_time – время, в течение которого допустимо ошибиться;

– securityprofile.password_lock_time – время блокирования пользователя.

В случае, когда пользователь в течение установленного времени (failed_login_attempts_max_time) превышает количество неудачных попыток аутентификации (failed_login_attempts), параметр «password_lock_time» игнорируется и пользователь блокируется навсегда, т.е. до момента разблокирования его администратором.

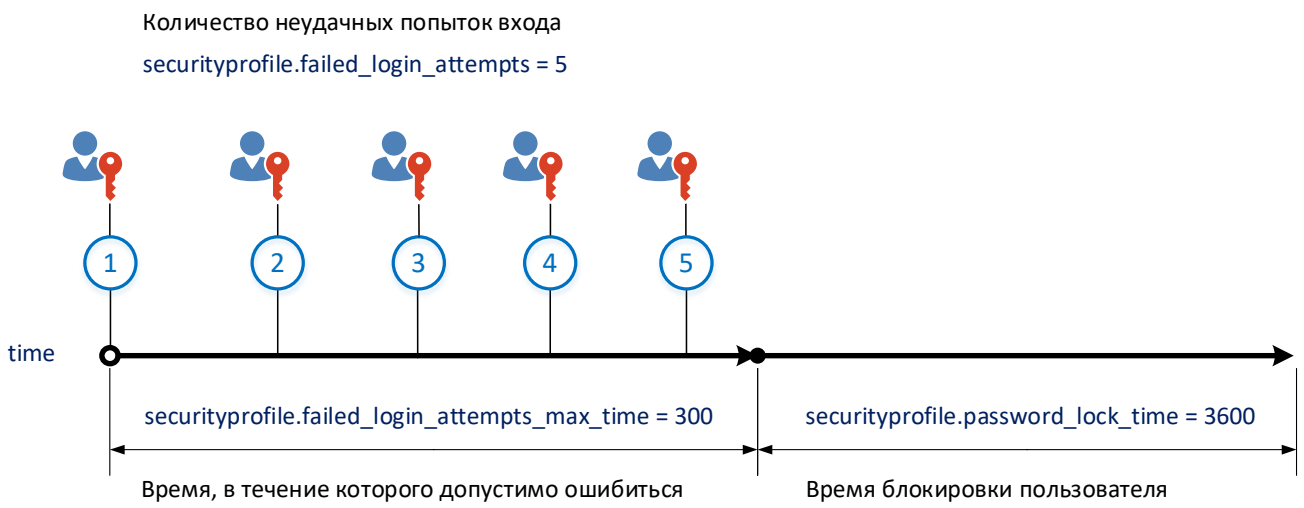


Рисунок 3.18 – Временная диаграмма

Разблокировать учетную запись может только субъект, обладающий полномочиями управления учетными записями пользователей. Например, администратор БД с атрибутом роли «Createrole». При активированном расширении JDV данный субъект должен входить в группу «dv_acctmgr».

### 3.2.6. Мера защиты УПД.9

СУБД «Jatoba» выполняет меру безопасности УПД.9 «Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы» в части следующего требования:

– СУБД обеспечивает ограничение числа параллельных сеансов доступа (квотой соединений) для каждой учетной записи пользователя (роли и ролей с атрибутом «Login»).

Подключения пользователей JDS ограничиваются в карточке пользователя параметром «Лимит подключений».

#### 3.2.6.1. Усиление УПД.9(3)

СУБД «Jatoba» реализует усиление меры защиты УПД.9(3) в части следующего требования:

– СУБД позволяет контролировать и отображать администратору число активных параллельных (одновременных) сеансов (сессий) для каждой учетной записи пользователей.

Ограничение числа параллельных сеансов пользователей выполняется встроенными механизмами СУБД установкой параметра «CONNECTION LIMIT» при создании или изменении роли.

Отображение администратору числа параллельных сеансов активных пользователей реализовано функциональными возможностями СУБД при помощи SQL-команды:

```
SELECT * from pg_stat_activity;
```

Дополнительно в компоненте пользовательского веб-интерфейса для администраторов «Jatoba data safe» в подразделе «Активность БД» (DB Activity) на вкладке «Подключения» отображается число активных параллельных (одновременных) сеансов (сессий) для каждой учетной записи пользователей.

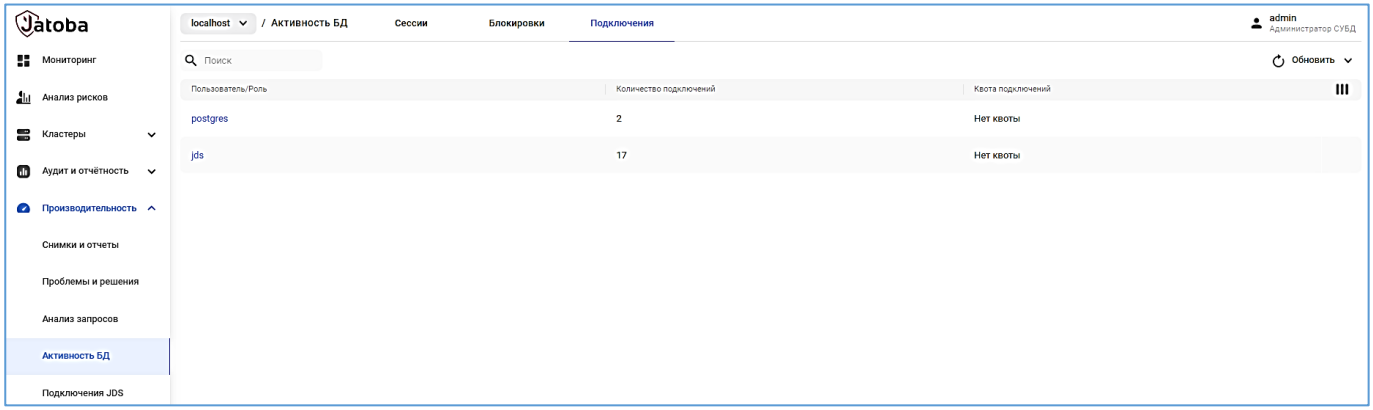


Рисунок 3.19 – Подраздел «Активность БД» (DB Activity), вкладка «Подключения»

Вкладка «Подключения JDS» отображает количество подключений к компоненту пользовательского веб-интерфейса для администраторов «Jatoba data safe».

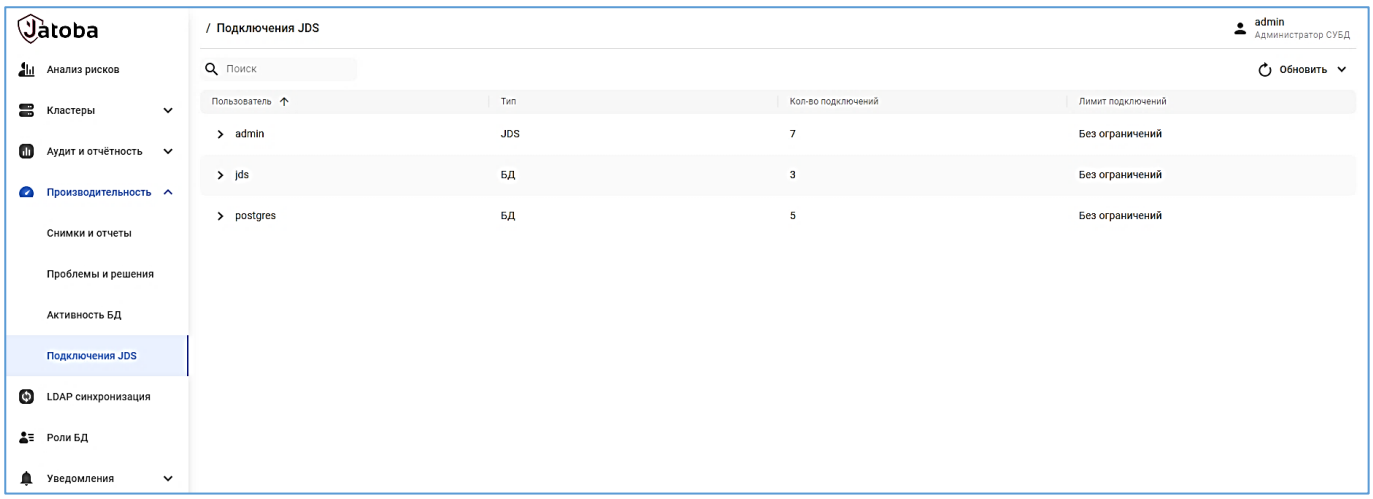


Рисунок 3.20 – Вкладка «Подключения JDS»

### 3.2.6.2. УПД.9 (4)

Компонент «JDS» СУБД «Jatoba» реализует усиление меры защиты УПД.9 (4) в части следующего требования:

– оповещение администратора о попытках превышения числа установленных допустимых активных параллельных (одновременных) сеансов (сессий) для каждой учетной записи.

Для реализации потребуется создать канал событий в разделе «Уведомления» в компоненте «JDS».

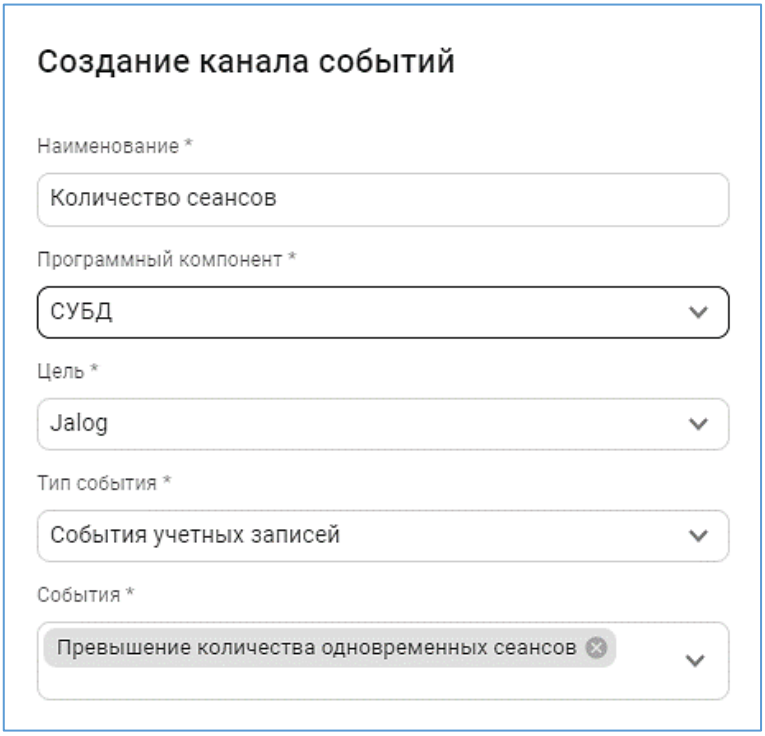


Рисунок 3.21 – Настройка канала событий для контроля параллельных сеансов пользователей

При создании канала событий должны быть выбраны параметры:

– Программный компонент – «СУБД»;

– Цель – служебная БД «ja_log»;

– Тип события – «События учетных записей»;

– События – «Превышение количества одновременных сеансов».

На контролируемой СУБД должен быть установлен агент компонента «ja_Log» который будет передавать журнал событий в служебная БД «ja_log».

Компонент «JDS» периодически будет просматривать служебную БД «ja_log» выбирать события безопасности и при их нахождении перешлет сообщение через сервисы E-mail и/или Zulip.

## 3.3. Обеспечение целостности информационной системы информации и информации

### 3.3.1. Мера защиты ОЦЛ.1

СУБД «Jatoba» выполняет меру безопасности ОЦЛ.1 «Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации» в части следующего требования:

– СУБД осуществляет контроль целостности собственных компонентов, по контрольным суммам компонентов средств защиты информации динамически в процессе работы СУБД.

Компонент СУБД «ja_CSum» – компонент контроля целостности по алгоритму MD, который с установленной периодичностью проверяет контрольные суммы установленных на контроль файлов. Компонент выполнен в формате extension (расширения) СУБД.

Контрольные суммы файлов импортируются с дистрибутивного диска № 2 файлами формата *.csv. Для каждого из компонентов предназначен отдельный файл.

Результаты проверки контроля целостности передаются в служебную СУБД через компонент централизованного сбора записей событий СУБД «ja_Log».

### 3.3.2. Мера защиты ОЦЛ.2

СУБД «Jatoba» выполняет меру безопасности ОЦЛ.2 «Контроль целостности информации, содержащейся в базах данных информационной системы» в части следующего требования:

– СУБД осуществляет контроль целостности, объектов баз данных (хранимых процедур, триггеров и т.д.), по контрольным суммам в процессе загрузки и (или) динамически в процессе работы.

СУБД имеет внешний компонент initdb, одной из функциональных возможностей которого является проверка контрольных сумм при использовании параметра -k --data-checksums. В этом случае осуществляется проверка всех компонентов СУБД динамически, в процессе работы СУБД.

Запуск проверки контрольных сумм можно установить в процессе инсталляции СУБД.

### 3.3.3. Мера защиты ОЦЛ.7

СУБД «Jatoba» выполняет меру безопасности ОЦЛ.7 «Контроль точности, полноты и правильности данных, вводимых в информационную систему» в части следующего требования:

– СУБД осуществляет контроль точности, полноты и правильности данных, вводимых в БД, устанавливая:

а) типы данных в таблицах;

б) размерность вводимых значений;

в) допустимые наборы символов.

СУБД имеет собственный механизм контроля вводимых данных, который работает со всеми типами данных (целочисленными, вещественными, строковыми, бинарными и т.д.) и не позволяет вводить данные, отличные от установленного типа.

## 3.4. Регистрация событий безопасности (РСБ)

Сбор событий безопасности осуществляется путем сбора событий с целевых СУБД. В данном случае под определением СУБД понимается как узел кластера СУБД, так и отдельная СУБД.

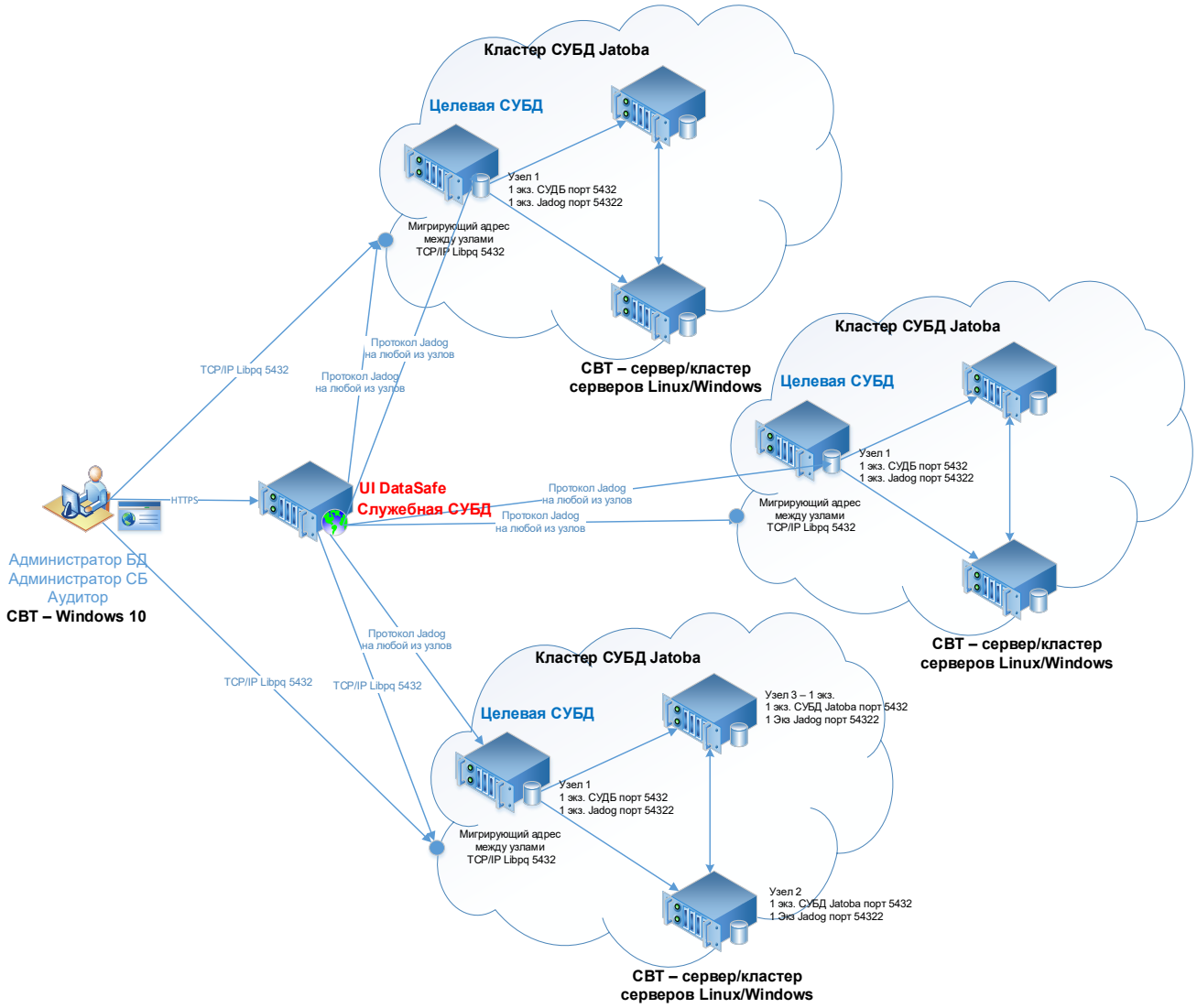


Рисунок 3.22 – Схема взаимодействия Jatoba Data Safe с целевыми СУБД

Для выполнения мер защиты информации в части регистрации событий безопасности должна быть выполнена настройка целевых СУБД.

### 3.4.1. Мера защиты РСБ.2

#### 3.4.1.1. Усиление РСБ.2(1а)

СУБД «Jatoba» выполняет меру безопасности РСБ.2 «Определение состава и содержания информации о событиях безопасности, подлежащих регистрации» в части следующего требования к усилению меры защиты РСБ.2(1а):

– СУБД «Jatoba» обеспечивает запись дополнительной информации о событиях безопасности, включающую полнотекстовую запись привилегированных команд (команд, управляющих системными функциями).

В дополнении к стандартным механизмам регистрации событий безопасности, используется расширение «pgAudit», которое помимо указанной меры позволяет выполнить требования ГОСТ Р 59548 – 2022 «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации».

При этом структура событий безопасности меняется, как представлено на рисунке 3.23.

| time stamp with milliseconds | user name | database name | process ID | client host | port number | session ID | per-session line number | command tag | session start time | virtual transaction ID | regular transaction ID | error severity | SQLSTATE code | error message | | | | | | | | | error message detail | hint | internal query that led to the error | character count of the error position therein | error context | user query that led to the error | character count of the error position therein | location of the error in the PostgreSQL source code |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| штамп времени с миллисекундами | имя пользователя | имя базы данных | идентификатор процесса | клиентский узел | номер порта | идентифи катор сессии | номер строки каждой сессии | тег команды | время начала сессии | виртуальный идентификатор транзакции | идентификатор транзакции | уровень важности ошибки | код ошибки SQLSTATE | сообщение об ошибке | | | | | | | | | подробности о сообщение об ошибке | подсказка к сообщение об ошибке | внутренний запрос | номер символа внутреннего запроса, где произошла ошибка | контекст ошибки | запрос пользователя | номер символа з запроса пользователя | расположение ошибки в исходном коде |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | | | | | | | | | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| | | | | | | | | | | | | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | | | | | | | | |
| | | | | | | | | | | | | | | pg_audit | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | Тип записи события | № выражения | № подвыражения | класс события | SQL операция | Тип объекта БД | Имя объекта БД | Полный текст SQL запроса (скрыто) | параметры SQL запроса (скрыто) | | | | | | | | |

Рисунок 3.23 – Структура события безопасности

### 3.4.2. Мера защиты РСБ.3

СУБД «Jatoba» выполняет меру безопасности РСБ.3 «Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения» в части следующих требований:

– СУБД «Jatoba» обеспечивает сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;

– СУБД предоставляет возможность АБ в текущий момент времени выбора событий безопасности.

Время хранения событий безопасности устанавливается в конфигурационном файле «postgresql.conf» в параметре «log_rotation_age» равный «90d».

Использовать параметр ротации по размеру файла «log_rotation_size» не целесообразно. Рекомендуется оставить параметр ротации равным «0», что соответствует отключению параметра.

При использовании компонента JDS, как описано в Усиление РСБ.3(1), время хранения увеличивается, т.к. СУБД не имеет ограничений по размеру БД.

#### 3.4.2.1. Усиление РСБ.3(1)

СУБД «Jatoba» реализует усиление меры защиты РСБ.3(1) в части следующего требования:

– СУБД обеспечивает централизованное автоматизированное управление сбором, записью и хранением информации о событиях безопасности.

При использовании компонента JDS события безопасности сохраняются в служебной БД. Данные собираются в автоматическом режиме при помощи агентов сбора данных с каждой инсталляции: сервера СУБД, кластера СУБД.

Предварительно, каждая из подконтрольных инсталляций проходит конфигурирование и для установки сроков хранения событий безопасности параметр ротация задается в конфигурационном файле в соответствии с описанием в пункте 3.4.2.

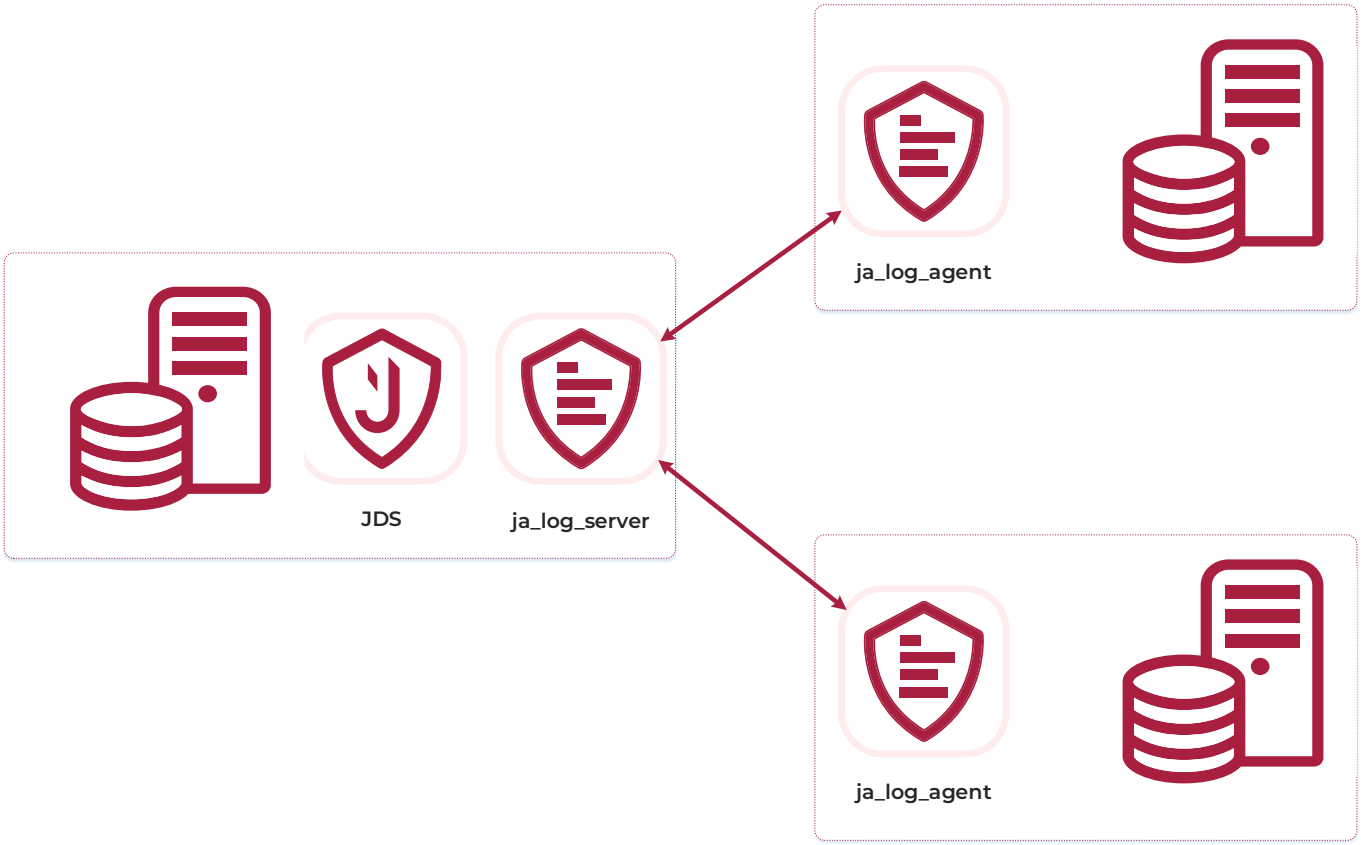


Рисунок 3.24 – Схема работы компонента

Для передачи событий безопасности используется компонент «ja_Log», описанный в документе 643.72410666.00067-07 98 01-12. «Руководство по настройке. Часть 12. Централизованный сбор записей событий СУБД. Компонент «ja_Log».

Компонент устанавливается на целевых СУБД и на служебной СУБД JDS.

В служебной СУБД JDS создается служебная БД «ja_log», в которую будут передаваться события безопасности. Просмотр событий будет доступен через раздел JDS Event List.

Управление сбором событий безопасности осуществляется с сервера JDS в виде директивы, что обеспечивает централизованное управление событиями безопасности.

### 3.4.3. Мера защиты РСБ.6

СУБД «Jatoba» выполняет меру безопасности РСБ.6 «Генерирование временных меток и (или) синхронизация системного времени» в части следующего требования:

– СУБД осуществляет синхронизацию системного времени.

СУБД в процессе функционирования автоматически синхронизирует системное время со временем операционной системы, на которой она установлена.

### 3.4.4. Мера защиты РСБ.7

СУБД «Jatoba» выполняет меру безопасности РСБ.7 «Защита информации о событиях безопасности» в части следующих требований к мере защиты РСБ.7:

– СУБД обеспечивает защиту информации о событиях безопасности;

– доступ к настройке механизмов регистрации событий безопасности должен осуществляться АБ либо с использованием специальной учетной записи.

Защита информации о событиях безопасности обеспечивается в несколько этапов:

1) На стороне целевой СУБД защита осуществляется на уровне доступа к каталогам data и log. Доступ возможен от имени и с правами системной учетной записи операционной системы «postgres», от имени и с правами учетной записи, входящей в группу «Администраторы».

2) На стороне служебной СУБД механизм защиты идентичен.

3) Для защиты данных используется весь спектр мер защиты, таких как ИАФ, УПД и т.д., поскольку события безопасности хранятся в БД.

4) На уровне приложения доступ к разделам ограничен предустановленной двухкомпонентной ролевой моделью. Прямого доступа к СУБД пользователи Jatoba data safe не имеют.

### 3.4.5. Мера защиты РСБ.8

СУБД «Jatoba» выполняет меру безопасности РСБ.8 «Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе» в части следующего требования:

– СУБД обеспечивает возможность просмотра и анализа информации о действиях отдельных пользователей СУБД.

#### 3.4.5.1. Усиление РСБ.8(1)

СУБД «Jatoba» реализует усиление меры защиты РСБ.8(1) в части следующего требования:

– СУБД «Jatoba» обеспечивает возможность автоматизированной обработки записей регистрации (аудита) событий безопасности на основе критериев избирательности.

Для выполнения меры защиты информации в конфигурационном файле «postgresql.conf» для параметра «log_line_prefix» устанавливаются следующие значения:

%a = application name;

%u = user name;

%d = database name;

%r = remote host and port;

%i = command tag;

%e = SQL state.

Просмотр событий безопасности после их накопления возможен как стандартными средствами, так и при помощи компонента JDS.

При агрегации событий безопасности они сопоставляются категориям (критериям) важности события. Список столбцов доступен для выбора пользователям.

Функциональные возможности просмотра событий безопасности приведены в п. 2.3.3 «Раздел JDS «Event List».

Таблица 3.8 – Список столбцов

| Наименование | Описание |
|---|---|
| **Event data** | Дата события |
| **Criticality** | Критичность события |
| **Class** | Тип события |
| **User name** | Имя пользователя |
| **Database name** | Имя базы данных |
| **Process ID** | Идентификатор процесса |

| Наименование | Описание |
|---|---|
| **Client host** | Клиентский узел |
| **Port number** | Номер порта |
| **Session ID** | Идентификатор сессии |
| **Per-session line number** | Номер строки каждой сессии |
| **Command tag** | Тег команды |
| **Session start time** | Время начала сессии |
| **Virtual transaction ID** | Виртуальный идентификатор транзакции |
| **Regular transaction ID** | Идентификатор транзакции |
| **Error severity** | Уровень важности ошибки |
| **SQLSTATE code** | Код ошибки SQLSTATE |
| **Error message** | Сообщение об ошибке |
| **Error message detail** | Подробности к сообщению об ошибке |
| **Hint** | Подсказка к сообщению об ошибке |
| **Internal query that led to the error** | Внутренний запрос |
| **Character count of the error position therein** | Номер символа внутреннего запроса, где произошла ошибка |
| **Error context** | Контекст ошибки |
| **User query that led to the error** | Запрос пользователя |
| **Character count of the error position therein** | Номер символа в запросе пользователя |
| **Location of the error in the PostgreSQL source code** | Расположение ошибки в исходном коде |

Дополнительно автоматически обрабатывает журналы регистрации событий безопасности компонент «pgBadger», который собирает данные о SQL-запросах:

- Overall statistics – общая статистика;
- The most frequent waiting queries – наиболее частые ожидающие запросы;
- Queries that waited the most – запросы с наибольшим временем ожидания;
- Queries generating the most temporary files – запросы, генерирующие больше всего временных файлов;

– Queries generating the largest temporary files – запросы, генерирующие самые большие временные файлы;

– The slowest queries – самые медленные запросы;

– Queries that took up the most time – запросы, занимавшие больше всего времени;

– The most frequent queries – самые частые запросы;

– The most frequent errors – самые частые ошибки;

– Histogram of query times – гистограмма продолжительности запросов;

– Histogram of sessions times – гистограмма продолжительности сессий;

– Users involved in top queries – пользователи наиболее частых запросов;

– Applications involved in top queries – приложения наиболее частых запросов;

– Queries generating the most cancellation – запросы, вызывающие наибольшее количество отмен;

– Queries most cancelled – наиболее частые отмененные запросы;

– The most time consuming prepare/bind queries – самые трудоемкие запросы на подготовку/привязку параметров.

Доступны следующие отчеты с почасовыми графиками, разделенными на периоды по пять минут:

– SQL queries statistics – статистика SQL-запросов;

– Temporary file statistics – статистика временных файлов;

– Checkpoints statistics – статистика контрольных точек;

– Autovacuum and autoanalyze statistics – статистика автовакуума и автоанализа;

– Cancelled queries – отмененные запросы;

– Error events (panic, fatal, error and warning) – события ошибок (паника, фатальная ошибка, ошибка и предупреждение);

– Error class distribution – распределение классов ошибок.

Круговые диаграммы о распределении:

– Locks statistics – статистика блокировок;

– Queries by type (select/insert/update/delete) – запросы по типу (выбрать/вставить/обновить/удалить);

– Distribution of queries type per database/application – распределение типов запросов по базе данных/приложению;

– Sessions per database/user/client/application – сеансы для каждой базы данных/пользователей/клиентов/приложений;

– Connections per database/user/client/application – количество подключений для каждой базы данных/пользователей/клиентов/приложений;

– Autovacuum and autoanalyze per table – автовакуум и автоанализ по таблице;

– Queries per user and total duration per user – запросы пользователя и общая продолжительность запросов пользователя.

## 3.5. Обеспечение доступности информации (резервирование, кластеризация и восстановление информации) (ОДТ)

### 3.5.1. Мера защиты ОДТ.4

СУБД «Jatoba» выполняет меру безопасности ОДТ.4 «Периодического резервного копирования информации на резервные машинные носители информации» в части следующих требований:

– СУБД обеспечивает резервное копирование информации на резервные машинные носители информации с установленной периодичностью;

– СУБД обеспечивает регистрацию событий, связанных с резервным копированием информации на резервные машинные носители информации.

### 3.5.2. Мера защиты ОДТ.5

СУБД «Jatoba» выполняет меру безопасности ОДТ.5 «Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала» в части следующих требований:

– СУБД обеспечивает восстановление информации с резервных машинных носителей информации (резервных копий);

– СУБД обеспечивает регистрацию событий, связанных с восстановлением информации с резервных машинных носителей информации.

Меры защиты информации ОДТ.5 и ОДТ.6, т.е. резервирование и восстановление информации выполняются компонентом «pg_ProBackup», описанным в документе 643.72410666.00067-07 98 01-04 «Руководство по настройке. Часть 4. Расширенное резервное копирование. Компонент «pg_ProBackup».

Используя «pg_ProBackup», можно выполнить полное или инкрементальное резервное копирование:

– полные резервные копии содержат все файлы данных, необходимые для восстановления кластера баз данных с нуля;

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

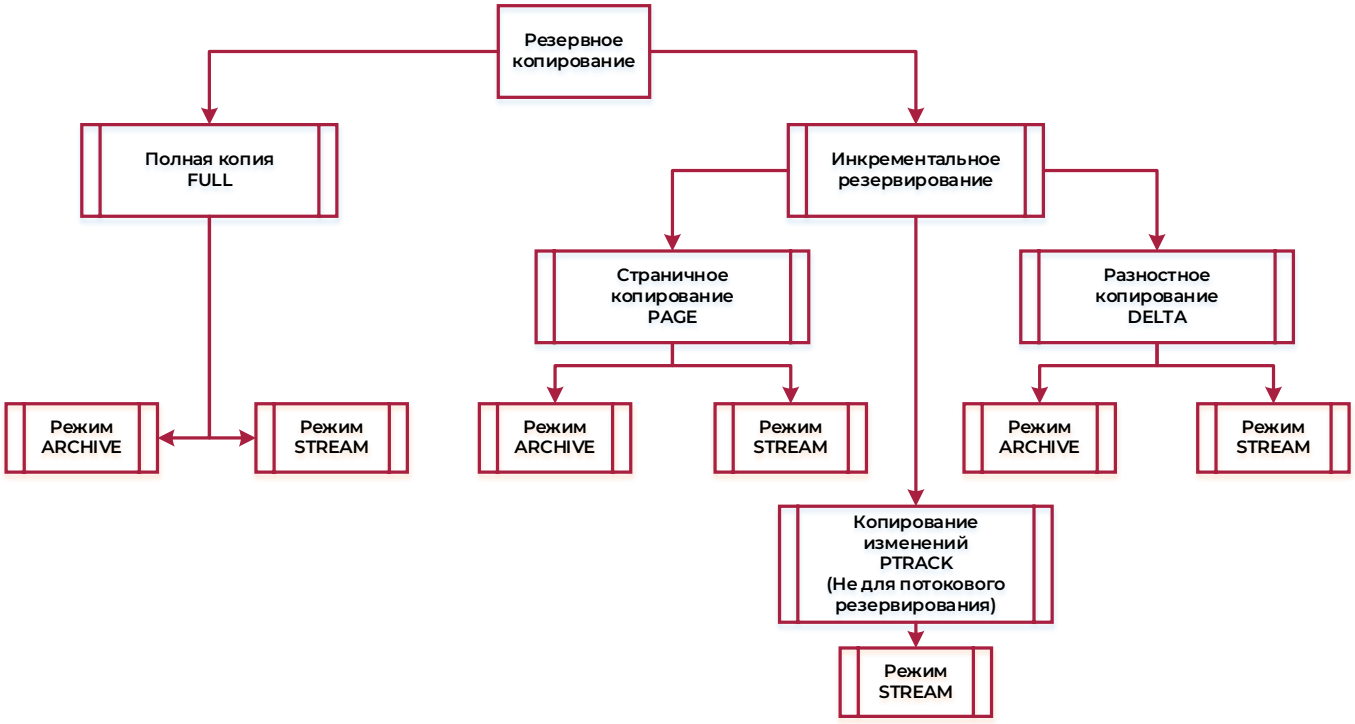


Рисунок 3.25 – Схема режимов копирования

Раздел «Резервное копирование» (BACKUP) компонента JDS управляет компонентом «pg_ProBackup», т.е. резервированием и восстановлением информации, и выполняет меры защиты информации ОДТ.5 и ОДТ.6.

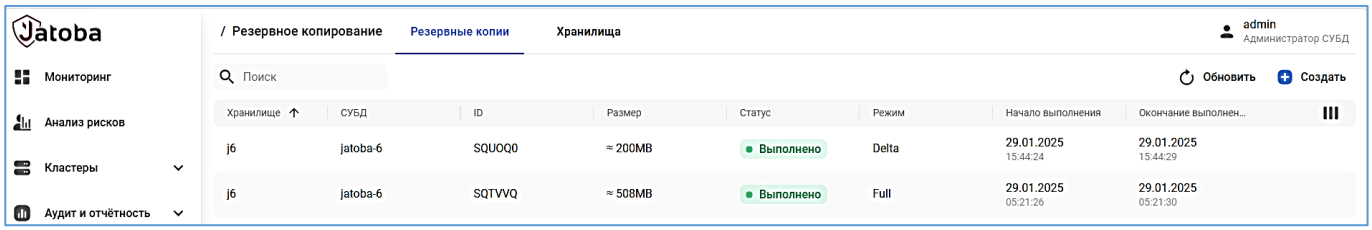


Рисунок 3.26 – Список резервных копий

### 3.5.3. Мера защиты ОДТ.6

#### 3.5.3.1. Усиление ОДТ.6 (2)

СУБД «Jatoba» выполняет меру безопасности ОДТ.6 «Кластеризация информационной системы и (или) ее сегментов» в части следующего требования к усилению меры защиты ОДТ.6 (2):

– СУБД осуществляет кластеризацию серверов баз данных.

Кластеризация осуществляется компонентом «jaDog», описанным в документе 643.72410666.00067-07 98 01-01 «Руководство по настройке. Часть 1. Управление режимом работы узлов кластера. Компонент «jaDog».

При формировании кластера выбираются несколько самостоятельных серверов с установленными СУБД. На каждом из серверов конфигурируется утилита jadog_ctl. На сервере, который планируется использовать в роли Master, на сетевой интерфейс устанавливается дополнительный публичный IP – адрес, на который будут обращаться пользователи.

Между серверами настраивается репликация, внесенные изменения на сервере Master записываются на сервер или сервера с ролью Slave.

В случае критического сбоя применяется механизм STONITH (Shoot-The-Other-Node-In-The-Head). Далее один из серверов берет на себя роль Master.

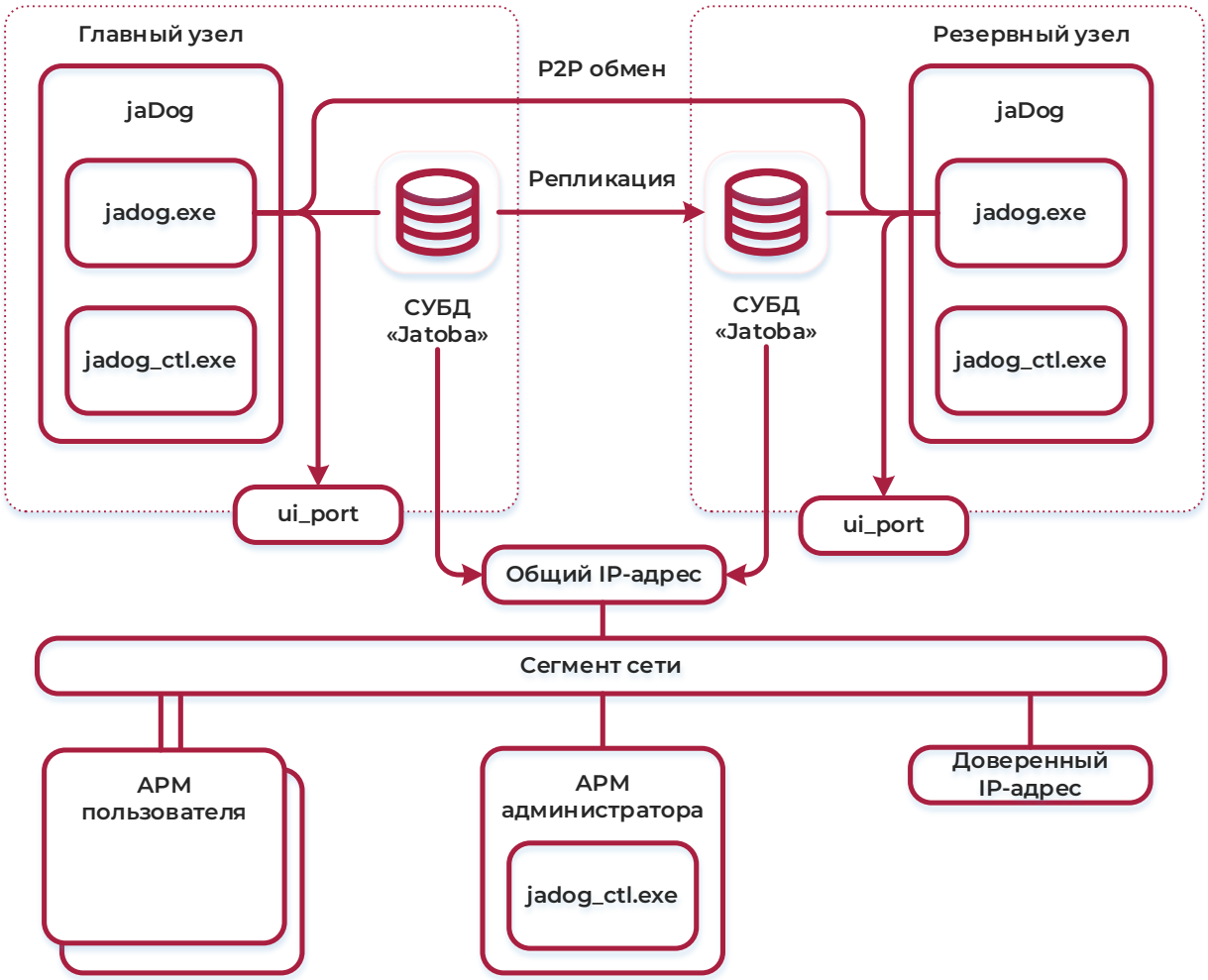


Рисунок 3.27 – Физическая структура узлов кластера

Компонент JDS в разделе «Ландшафт» выполняет формирование и подключение к кластеру сформированного компонентом jaDog.

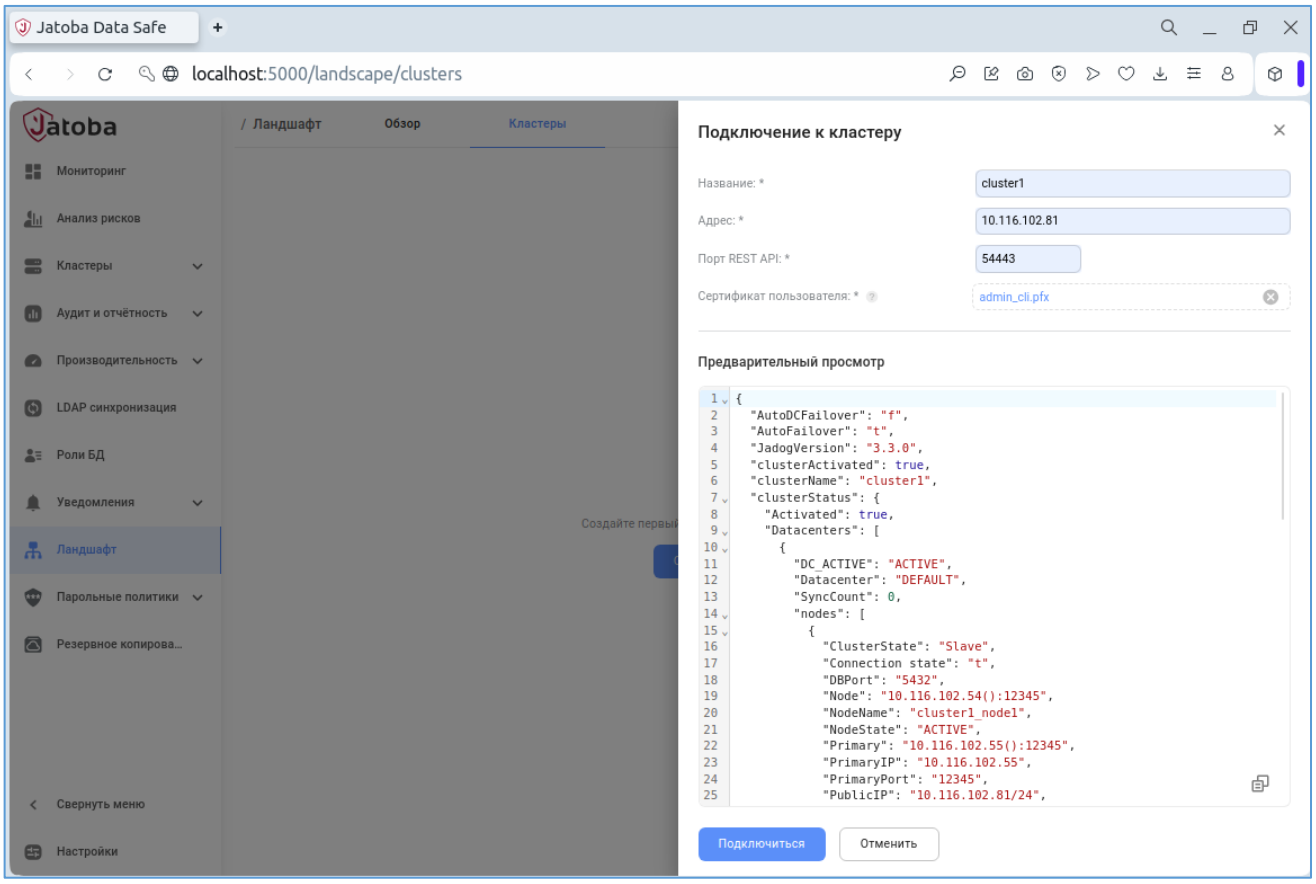


Рисунок 3.28 – Подключение к кластеру

Управление кластером производится в разделе «Кластеры» (CLUSTERS)

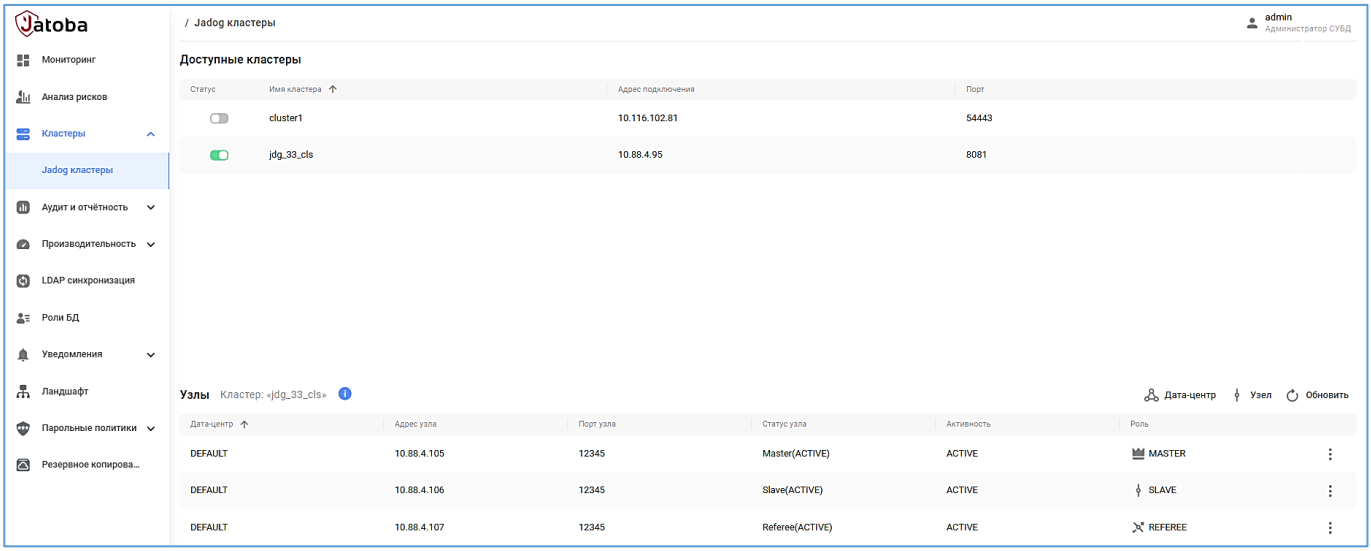


Рисунок 3.29 – Доступные кластеры

Кластеризация серверов СУБД позволяет использовать компонент балансировки подключений пользователей «jaPooler». Компонент разбирает запросы от пользователей и отправляет на master-сервер запросы READ-WRITE, а запросы типа READ-ONLY на slave-сервер. Таким образом распределяется нагрузка на серверы СУБД.

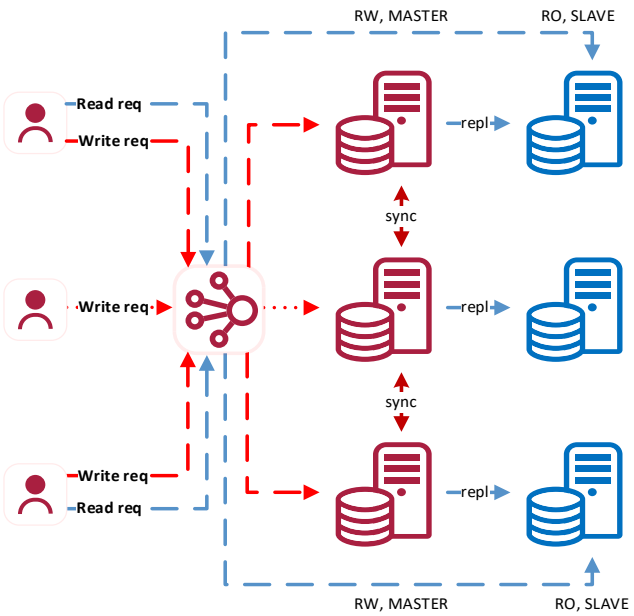


Рисунок 3.30 – Схема работы компонента Japooler

# 4. ТРЕБОВАНИЯ ПО БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПО ПРИКАЗУ ФСТЭК № 64

Выполнение требований по безопасности информации аналогично выполнению мер защиты информации, приведенных в разделе 3 «Меры защиты информации» настоящего документа.

Сопоставление мер защиты информации и требований по безопасности информации приведено в таблице 4.1.

Таблица 4.1 – Функции и требования по защите информации

| № | Версии ядра СУБД | | | | | | Приказы ФСТЭК | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | J4 | | J5 | | J6 | | | ГИС | ИСПДн | КИИ и КВО |
| | | | | | | | №64 | №17 | №21 | №239, №31 |
| | Дист.[1] | Обр.к.[2] | Дист. | Обр.к. | Дист. | Обр.к. | Требования по безопасности информации | Меры защиты информации | | |
| 1 | X | X | X | X | X | X | Идентификация и аутентификация пользователей в СУБД (ИАФ) | Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ) | | |
| 2 | X | X | X | X | X | X | Управление доступом в СУБД (УПД) | Управление доступом субъектов доступа к объектам доступа (УПД) | | |
| 3 | X | X | X | X | X | X | Контроль целостности в СУБД (ОЦЛ) | Обеспечение целостности информационной системы и информации (ОЦЛ) | | |
| 4 | X | X | X | X | X | X | Регистрация событий безопасности в СУБД (РСБ) | Регистрация событий безопасности (РСБ) | | |
| 5 | X | — | X | — | X | — | Резервное копирование и восстановление в СУБД (ОДТ) | Обеспечение доступности информации (ОДТ) | | |
| 6 | X | — | X | — | X | — | Обеспечение доступности СУБД (ОДТ) | Обеспечение доступности информации (ОДТ) | | |
| 7 | X | X | X | X | X | X | Ограничение программной среды в СУБД (ОПС) | | | |

Примечание:

1) Дистрибутив.

2) Образ контейнера.

## 4.1. Ограничение программной среды в СУБД (ОПС)

СУБД реализует выполнение требований по безопасности информации, установленные п. 15 «Ограничение программной среды» приказа ФСТЭК России от 14.04.2023 № 64 в части следующих требований:

Выявление и блокирование загрузки в адресное пространство СУБД:

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

Сервер СУБД при попытке аутентифицированного пользователя, такого как:

- Администратор СУБД;
- Администратор БД;

имеющего соответствующие атрибуты роли и привилегии установить расширение, СУБД проверяет по специальным атрибутам подлинность программного обеспечения входящего в комплект поставки.

На стадии контроля оригинальности ПО СУБД принимает решение о продолжении проверок или о блокировании попытки установки ПО.

Программное обеспечение прошедшее проверку на подлинность, проверяется на целостность компонентом СУБД «ja_CSum». Если проверка пройдена успешно, ПО устанавливается, в обратном случае ПО блокируется для установки.

## 4.2. Контроль целостности в системе управления базами данных

СУБД реализует обеспечивает выполнение требований по безопасности информации, установленные п. 9 «Обеспечение целостности» приказа ФСТЭК России от 14.04.2023 № 64 в части следующих требований:

- СУБД должна контролировать целостность в процессе запуска системы управления базами данных[1] для:
    - конфигурации системы управления базами данных;

[1] контроль целостности в процессе запуска СУБД для процедур (программного кода) системы управления базами данных не применим к данному типу СУБД

- конфигураций баз данных;
- процедур (программного кода), хранимых в базах данных.

Контроль целостности в СУБД осуществляется компонентом «ja_CSum» с установленной периодичностью и при запуске СУБД.

Контроль конфигурации СУБД выполняется по:

- конфигурационным файлам самой СУБД:
  - pg_hba.conf;
  - pg_ident.conf;
  - postgresql.conf;
- конфигурационным файлам компонент;
- служебным, конфигурационным таблицам встроенных компонент;
- составу встроенных компонент (расширений);
- внутренней структуре СУБД (перечень БД и т.п.).

Обнаружение несоответствия вызовет компонент SecurityProfile, который блокирует пользователей СУБД.

Контроль конфигурация БД осуществляется по параметрам, присущих конкретной БД, таких как:

- имя БД;
- владелец БД (OWNER);
- кодировка (Encoding);
- OID;
- набор расширений.

Обнаружение несоответствия вызовет компонент SecurityProfile, который блокирует пользователей БД и СУБД.

При контроле процедур (программного кода) БД контролируется целостность:

- процедур;

- функций;
- триггеров;
- пользовательских типов данных;
- представлений;
- материальных представлений.

Обнаружение несоответствия вызовет компонент SecurityProfile, который блокирует пользователей СУБД.

Все события регистрируются в журнале событий СУБД. Однако учитывая важность инцидента ИБ, рекомендуется создать канал событий в разделе «Уведомления» компонента JDS для оперативного оповещения администраторов СУБД и БД.

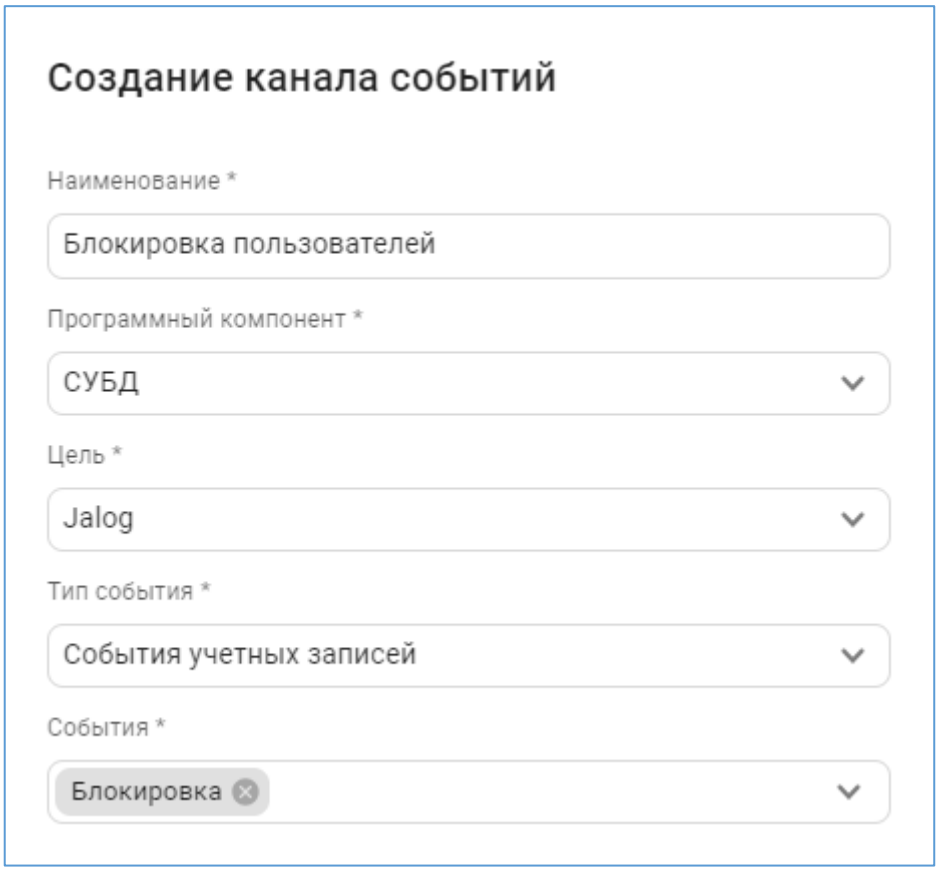


Рисунок 4.1 – Создание канала событий

# 5. ТРЕБОВАНИЯ ПО БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПО ГОСТ Р 57580.1-2017

Выполнение базового состава технических мер защиты информации, установленных ГОСТ Р 57580.1-2017, аналогично выполнению мер защиты информации приведенных в разделах:

- 3 «Меры защиты информации»;
- 4 «Требования по безопасности информации по Приказу ФСТЭК № 64».

Сопоставление базового состава технических мер защиты информации, мер защиты информации и требований по безопасности информации приведено в таблице 5.1.

Таблица 5.1 – Сопоставление базового состава технических мер защиты информации, мер защиты информации и требований по безопасности информации

| № | Версии ядра СУБД | | | | ГОСТ Р 57580.1-2017 | | | Приказы ФСТЭК | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | J4 | | J5 | | | | | | | | |
| | Дист.[1] | Обр.к.[2] | Дист. | Обр.к. | Процесс | | | | ГИС | ИСПДн | КИИ и КВО |
| | | | | | | Подпроцесс | | №64 | №17 | №21 | №239, №31 |
| | | | | | | | Базовый состав мер | Требования по безопасности информации | Меры защиты информации | | |
| 1 | X | X | X | X | **Процесс 1 «Обеспечение защиты информации при управлении доступом»** | | | Идентификация и аутентификация пользователей в СУБД (ИАФ) | Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ) | | |
| | | | | | | **Подпроцесс «Идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа»** | | | | | |
| | | | | | | | Базовый состав мер по идентификации и аутентификации субъектов логического доступа | | | | |
| | | | | | | | Базовый состав мер по организации управления и организации защиты идентификационных и аутентификационных данных | | | | |
| | | | | | | | Базовый состав мер по авторизации (разграничению доступа) при осуществлении логического доступа | | | | |
| 2 | X | X | X | X | **Процесс 1 «Обеспечение защиты информации при управлении доступом»** | | | Управление доступом в СУБД (УПД) | Управление доступом субъектов доступа к объектам доступа (УПД) | | |
| | | | | | | **Подпроцесс «Управление учетными записями и правами субъектов логического доступа»** | | | | | |
| | | | | | | | Базовый состав мер по организации и контролю использования учетных записей субъектов логического доступа | | | | |

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

| № | Версии ядра СУБД | | | | ГОСТ Р 57580.1-2017 | | | Приказы ФСТЭК | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | J4 | | J5 | | | | | | | | |
| | Дист.[1] | Обр.к.[2] | Дист. | Обр.к. | Процесс | | | | ГИС | ИСПДн | КИИ и КВО |
| | | | | | | Подпроцесс | | №64 | №17 | №21 | №239, №31 |
| | | | | | | | Базовый состав мер | Требования по безопасности информации | Меры защиты информации | | |
| | | | | | | | Базовый состав мер по организации, контролю предоставления (отзыва) и блокированию логического доступа | | | | |
| 3 | X | X | X | X | | | | Контроль целостности в СУБД (ОЦЛ) | Обеспечение целостности информационной системы и информации (ОЦЛ) | | |
| 4 | X | X | X | X | | **Подпроцесс «Идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа»** | | Регистрация событий безопасности в СУБД (РСБ) | Регистрация событий безопасности (РСБ) | | |
| | | | | | | | Базовый состав мер по регистрации событий защиты информации, связанных с идентификацией, аутентификацией и авторизацией (разграничением доступа) при осуществлении логического доступа | | | | |
| | | | | | | **Подпроцесс «Управление учетными записями и правами субъектов логического доступа»** | | | | | |
| | | | | | | | Базовый состав мер по регистрации событий защиты информации и контролю использования предоставленных прав логического доступа | | | | |
| | | | | | **Процесс 6 «Управление инцидентами защиты информации»** | | | | | | |
| | | | | | | **Подпроцесс «Мониторинг и анализ событий защиты информации»** | | | | | |
| | | | | | | | Базовый состав мер по организации мониторинга данных регистрации о событиях защиты информации, | | | | |

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

| № | Версии ядра СУБД | | | | ГОСТ Р 57580.1-2017 | | | Приказы ФСТЭК | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | J4 | | J5 | | | | | | | | |
| | Дист.[1] | Обр.к.[2] | Дист. | Обр.к. | Процесс | | | | ГИС | ИСПДн | КИИ и КВО |
| | | | | | | Подпроцесс | | №64 | №17 | №21 | №239, №31 |
| | | | | | | | Базовый состав мер | Требования по безопасности информации | Меры защиты информации | | |
| | | | | | | | формируемых объектами информатизации | | | | |
| 5 | X | — | X | — | | | | Резервное копирование и восстановление в СУБД (ОДТ) | Обеспечение доступности информации (ОДТ) | | |
| 6 | X | — | X | — | | | | Обеспечение доступности СУБД (ОДТ) | Обеспечение доступности информации (ОДТ) | | |
| 7 | X | X | X | X | | | | Ограничение программной среды в СУБД (ОПС) | | | |
| | | | | | **Процесс 3 «Контроль целостности и защищенности информационной инфраструктуры»** | | | | | | |
| | | | | | | | Базовый состав мер по контролю отсутствия известных (описанных) уязвимостей защиты информации объектов информатизации | | | | |

Примечание:

1) Дистрибутив.

2) Образ контейнера.

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

## 5.1. Процесс 1 «Обеспечение защиты информации при управлении доступом»

### 5.1.1. Подпроцесс «Управление учетными записями и правами субъектов логического доступа»

СУБД в подпроцессе «Управление учетными записями и правами субъектов логического доступа» выполняет базовый состав технических мер защиты информации в части следующих требований, представленных в пунктах:

– 5.1.1.1 «Базовый состав мер по организации и контролю использования учетных записей субъектов логического доступа»;

– 5.1.1.2 «Базовый состав мер по организации, контролю предоставления (отзыва) и блокированию логического доступа»;

– 5.1.1.3 «Базовый состав мер по регистрации событий защиты информации и контролю использования предоставленных прав логического доступа».

#### 5.1.1.1 Базовый состав мер по организации и контролю использования учетных записей субъектов логического доступа

Таблица 5.2 – Базовый состав мер по организации и контролю использования учетных записей субъектов логического доступа

| Условное обозначение и номер меры | Содержание мер системы защиты информации | Уровень защиты информации | Реализация в СУБД «Jatoba» |
|---|---|---|---|
| | | 1 | |
| УЗП.1 | Осуществление логического доступа пользователями и эксплуатационным персоналом под уникальными и персонифицированными учетными записями | Т | Мера защиты ИАФ.1 в части следующих требований: идентификацию и аутентификацию пользователей, являющихся работником оператора; |
| УЗП.3 | Контроль отсутствия незаблокированных учетных записей:<br>- уволенных работников; | Т | Выполняется уполномоченным администратором на основании сведений о фактическом режиме работы сотрудников с использованием функции «Управление доступом субъектов доступа к объектам |

| Условное обозначение и номер меры | Содержание мер системы защиты информации | Уровень защиты информации | Реализация в СУБД «Jatoba» |
|---|---|---|---|
| | | 1 | |
| | - работников, отсутствующих на рабочем месте более 90 календарных дней; | | доступа» (Защитная мера **УПД.1).** |
| | - работников внешних (подрядных) организаций, прекративших свою деятельность в организации | | Выполняется уполномоченным администратором на основании сведений о фактическом режиме работы сотрудников с использованием функции «Управление доступом субъектов доступа к объектам доступа» (Защитная мера УПД.1). Для пользователей, выполняющих работы по договорным обязательствам фиксированного срока проведения работ усиление меры защиты УПД.1(2) в части следующих требований:<br>автоматическое блокирование временных учетных записей пользователей по окончании установленного периода времени для их использования. |

### 5.1.1.2 Базовый состав мер по организации, контролю предоставления (отзыва) и блокированию логического доступа

Таблица 5.3 – Базовый состав мер по организации, контролю предоставления (отзыва) и блокированию логического доступа

| Условное обозначение и номер меры | Содержание мер системы защиты информации | Уровень защиты информации | Реализация в СУБД «Jatoba» |
|---|---|---|---|
| | | 1 | |
| УЗП.8 | Хранение эталонной информации о предоставленных правах логического доступа и обеспечение целостности | Т | Компонент «Jatoba data safe» имеет функциональную возможность формировать «Матрицу доступа» по атрибутам пользователей и выгружать ее в файл MS Excel. (п. 3.3.1) |

| Условное обозначение и номер меры | Содержание мер системы защиты информации | Уровень защиты информации | Реализация в СУБД «Jatoba» |
|---|---|---|---|
| | | 1 | |
| | указанной информации | | А также в разделе «User Risk» формировать матрицу назначенных системных привилегий. (п. 3.1)<br>Документ 643.72410666.00067-07 98 01-07 |
| УЗП.10 | Исключение возможного бесконтрольного самостоятельного расширения пользователями предоставленных им прав логического доступа | Т | УПД.2 «Реализация необходимых методов, типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа».<br>На уровне СУБД назначаются атрибуты ролей и системные привилегии, которые исключают бесконтрольное расширение прав |
| УЗП.11 | Исключение возможного бесконтрольного изменения пользователями параметров настроек средств и систем защиты информации, параметров настроек АС, связанных с защитой информации | Т | УПД.2 «Реализация необходимых методов, типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа».<br>Настройки конфигурации СУБД и БД производятся уполномоченным пользователем с соответствующим набором привилегий.<br>ОЦЛ.1 «Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации»<br>Компонент «ja_CSum» обеспечивает контроль целостности и в том числе целостность конфигурационных фалов<br>Документ 643.72410666.00067-07 98 01-14 |
| УЗП.13 | Контроль прекращения предоставления логического доступа и блокирование учетных записей при истечении периода (срока) предоставления логического доступа | Т | Усиление меры защиты УПД.1(2) в части следующих требований: автоматическое блокирование временных учетных записей пользователей по окончании установленного периода времени для их использования |
| УЗП.15 | Установление фактов неиспользования субъектами логического доступа предоставленных им прав на осуществление | Т | Усиление меры защиты УПД.1 (3б) в части требований:<br>3) в информационной системе должно осуществляться автоматическое блокирование неактивных (неиспользуемых) учетных |

| Условное обозначение и номер меры | Содержание мер системы защиты информации | Уровень защиты информации | Реализация в СУБД «Jatoba» |
|---|---|---|---|
| | | 1 | |
| | логического доступа на протяжении периода времени, превышающего 45 дней | | записей пользователей после периода времени неиспользования:<br>б) более 45 дней;<br>По истечении указанного времени УЗ будет заблокирована о чем будет соответствующая запись в журнале аудита СУБД. |
| УЗП.18 | Реализация возможности определения состава предоставленных прав логического доступа для конкретного субъекта логического доступа | Т | Компонент «Jatoba data safe» имеет функциональную возможность формировать «Матрицу доступа» по атрибутам пользователей (п. 3.3.1)<br>А также в разделе «User Risk» формировать матрицу назначенных системных привилегий. (п. 3.1)<br>Документ 643.72410666.00067-07 98 01-07 |

#### 5.1.1.3 Базовый состав мер по регистрации событий защиты информации и контролю использования предоставленных прав логического доступа

Таблица 5.4 – Базовый состав мер по регистрации событий защиты информации и контролю использования предоставленных прав логического доступа

| Условное обозначение и номер меры | Содержание мер системы защиты информации | Уровень защиты информации | Реализация в СУБД «Jatoba» |
|---|---|---|---|
| | | 1 | |
| УЗП.22 | Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала, обладающего привилегированными | Т | РСБ.2 «Определение состава и содержания информации о событиях безопасности, подлежащих регистрации».<br>Усиление меры защиты РСБ.2(1а) в части следующего требования:<br>• запись дополнительной информации о событиях безопасности, |

| Условное обозначение и номер меры | Содержание мер системы защиты информации | Уровень защиты информации | Реализация в СУБД «Jatoba» |
|---|---|---|---|
| | | 1 | |
| | правами логического доступа, позволяющими осуществить деструктивное воздействие, приводящее к нарушению выполнения бизнес-процессов или технологических процессов финансовой организации | | включающую полнотекстовую запись привилегированных команд (команд, управляющих системными функциями) |
| УЗП.23 | Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала и пользователей, обладающих правами логического доступа, в том числе в АС, позволяющими осуществить операции (транзакции), приводящие к финансовым последствиям для финансовой организации, клиентов и контрагентов | Т | Все события безопасности регистрируются Изделием. РСБ.3 «Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения» |
| УЗП.24 | Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала, обладающего правами по управлению логическим доступом | Т | |
| УЗП.25 | Регистрация событий защиты информации, связанных с действиями по управлению учетными записями и правами субъектов логического доступа | Т | |

### 5.1.2. Подпроцесс «Идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа»

СУБД в подпроцессе «Идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа» выполняет базовый состав технических мер защиты информации в части следующих требований, представленных в пунктах:

– 5.1.2.1 «Базовый состав мер по идентификации и аутентификации субъектов логического доступа»;

– 5.1.2.2 «Базовый состав мер по организации управления и организации защиты идентификационных и аутентификационных данных»;

– 5.1.2.3 «Базовый состав мер по авторизации (разграничению доступа) при осуществлении логического доступа»;

– 5.1.2.4 «Базовый состав мер по регистрации событий защиты информации, связанных с идентификацией, аутентификацией и авторизацией (разграничением доступа) при осуществлении логического доступа».

#### 5.1.2.1 Базовый состав мер по идентификации и аутентификации субъектов логического доступа

Таблица 5.5 – Базовый состав мер по идентификации и аутентификации субъектов логического доступа

| Условное обозначение и номер меры | Содержание мер системы защиты информации | Уровень защиты информации | Реализация в СУБД «Jatoba» |
|---|---|---|---|
| | | 1 | |
| РД.1 | Идентификация и однофакторная аутентификация пользователей | Н | ИАФ.1 «Идентификация и аутентификация пользователей, являющихся работниками оператора» |
| РД.3 | Идентификация и однофакторная аутентификация эксплуатационного персонала | Н | ИАФ.1 «Идентификация и аутентификация пользователей, являющихся работниками оператора» |

| Условное обозначение и номер меры | Содержание мер системы защиты информации | Уровень защиты информации | Реализация в СУБД «Jatoba» |
|---|---|---|---|
| | | 1 | |
| РД.8 | Сокрытие (неотображение) паролей при их вводе субъектами доступа | Т | ИАФ.5 «Защита обратной связи при вводе аутентификационной информации» |
| РД.11 | Временная блокировка учетной записи пользователей после выполнения ряда неуспешных последовательных попыток аутентификации на период времени не менее 30 мин. | Т | ИАФ.4 «Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средствами аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации».<br>Усиление к мере защиты ИАФ.1 (1Г).<br>(УПД.6) «Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)» |
| РД.12 | Запрет множественной аутентификации субъектов логического доступа с использованием одной учетной записи путем открытия параллельных сессий логического доступа с использованием разных АРМ, в том числе виртуальных | Т | УПД.9 «Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы» |

### 5.1.2.2 Базовый состав мер по организации управления и организации защиты идентификационных и аутентификационных данных

Таблица 5.6 – Базовый состав мер по организации управления и организации защиты идентификационных и аутентификационных данных

| Условное обозначение и номер меры | Содержание мер системы защиты информации | Уровень защиты информации | Реализация в СУБД «Jatoba» |
|---|---|---|---|
| | | 1 | |
| РД.19 | Смена паролей пользователей не реже одного раза в год | Т | Усиление к мере защиты ИАФ.1 (1Г) |
| РД.20 | Смена паролей эксплуатационного персонала не реже одного раза в квартал | Т | Усиление к мере защиты ИАФ.1 (1Г) |
| РД.21 | Использование пользователями паролей длиной не менее восьми символов | Т | Усиление к мере защиты ИАФ.1 (1Г) |
| РД.22 | Использование эксплуатационным персоналом паролей длиной не менее шестнадцати символов | Т | Усиление к мере защиты ИАФ.1 (1Г) |
| РД.23 | Использование при формировании паролей субъектов логического доступа символов, включающих буквы (в верхнем и нижнем регистрах) и цифры | Т | ИАФ.4 «Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средствами аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации» |

### 5.1.2.3 Базовый состав мер по авторизации (разграничению доступа) при осуществлении логического доступа

Таблица 5.7 – Базовый состав мер по авторизации (разграничению доступа) при осуществлении логического доступа

| Условное обозначение и номер меры | Содержание мер системы защиты информации | Уровень защиты информации | Реализация в СУБД «Jatoba» |
|---|---|---|---|
| | | 1 | |
| РД.30 | Авторизация логического доступа к ресурсам доступа, в том числе АС | Т | ИАФ.1 «Идентификация и аутентификация пользователей, являющихся работниками оператора» |
| РД.31 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод) при разграничении логического доступа к ресурсам доступа | Т | УПД.2 «Реализация необходимых методов, типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа» |
| РД.32 | Реализация ролевого метода (с определением для каждой роли прав доступа) при разграничении логического доступа в АС | Т | УПД.2 «Реализация необходимых методов, типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа» |
| РД.33 | Реализация необходимых типов (чтение, запись, выполнение или иной тип) и правил разграничения логического доступа к ресурсам доступа, в том числе АС | Т | УПД.2 «Реализация необходимых методов, типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа» |

### 5.1.2.4 Базовый состав мер по регистрации событий защиты информации, связанных с идентификацией, аутентификацией и авторизацией (разграничением доступа) при осуществлении логического доступа

Таблица 5.8 – Базовый состав мер по регистрации событий защиты информации, связанных с идентификацией, аутентификацией и авторизацией (разграничением доступа) при осуществлении логического доступа

| Условное обозначение и номер меры | Содержание мер системы защиты информации | Уровень защиты информации | Реализация в СУБД «Jatoba» |
|---|---|---|---|
| | | 1 | |
| РД.39 | Регистрация выполнения субъектами логического доступа ряда неуспешных последовательных попыток аутентификации | Т | РСБ.3 «Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения» |
| РД.40 | Регистрация осуществления субъектами логического доступа идентификации и аутентификации | Т | РСБ.3 «Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения» |
| РД.41 | Регистрация авторизации, завершения и (или) прерывания (приостановки) осуществления эксплуатационным персоналом и пользователями логического доступа, в том числе в АС | Т | РСБ.3 «Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения» |
| РД.42 | Регистрация запуска программных сервисов, осуществляющих логический доступ | Т | РСБ.3 «Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения» |
| РД.43 | Регистрация изменений аутентификационных данных, используемых для осуществления логического доступа | Т | РСБ.3 «Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения» |

## 5.2. Процесс 3 «Контроль целостности и защищенности информационной инфраструктуры»

### 5.2.1. Базовый состав мер по контролю отсутствия известных (описанных) уязвимостей защиты информации объектов информатизации

Таблица 5.9 – Базовый состав мер по контролю отсутствия известных (описанных) уязвимостей защиты информации объектов информатизации

| Условное обозначение и номер меры | Содержание мер системы защиты информации | Уровень защиты информации | Реализация в СУБД «Jatoba» |
|---|---|---|---|
| | | 1 | |
| ЦЗИ.8 | Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей, указанных в пунктах ЦЗИ.1 – ЦЗИ.6 настоящей таблицы, путем сканирования и анализа состава, версий и параметров настроек прикладного ПО, ПО АС и системного ПО, реализующего функции обеспечения защиты информации и (или) влияющего на обеспечение защиты информации (далее в настоящем разделе – системное ПО) <*>, установленного на серверном и сетевом оборудовании | | см. п. 5.4.2 |

## 5.3. Процесс 6 «Управление инцидентами защиты информации»

### 5.3.1. Подпроцесс «Мониторинг и анализ событий защиты информации»

СУБД в подпроцессе «Мониторинг и анализ событий защиты информации» выполняет базовый состав технических мер защиты информации в части следующих требований, представленных в пункте 5.3.1.1.

#### 5.3.1.1 Базовый состав мер по организации мониторинга данных регистрации о событиях защиты информации, формируемых объектами информатизации

Таблица 5.10 – Базовый состав мер по организации мониторинга данных регистрации о событиях защиты информации, формируемых объектами информатизации

| Условное обозначение и номер меры | Содержание мер системы защиты информации | Уровень защиты информации | Реализация в СУБД «Jatoba» |
|---|---|---|---|
| | | 1 | |
| МАС.4 | Организация мониторинга данных регистрации о событиях защиты информации, формируемых системным ПО, операционными системами, СУБД | Т | Доступ на чтение данных предоставляется учетным записям пользователей согласно матрице доступа УПД.2 «Реализация необходимых методов, типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа».<br>Усиление меры защиты РСБ.3(1) в части следующего требования:<br>• централизованное автоматизированное управление сбором, записью и хранением информации о событиях безопасности |

## 5.4. Описание реализации отдельных базовых мер защиты информации

### 5.4.1. Базовая мера МАС.4 «Организация мониторинга данных регистрации о событиях защиты информации, формируемых системным ПО, операционными системами, СУБД»

В СУБД «Jatoba» организация мониторинга данных регистрации о событиях защиты информации, формируемых СУБД, выполнена взаимодействием компонентов:

– компонент «pgAudit» выполняет расширение механизма регистрации событий СУБД;

– компонент «ja_Log» обеспечивает централизованный сбор событий СУБД;

– компонент пользовательского веб-интерфейса для администраторов «Jatoba data safe» предоставляет графический интерфейс просмотра событий СУБД и механизм уведомлений.

**Компонент «pgAudit»**

В дополнение к стандартным механизмам регистрации событий безопасности, в СУБД «Jatoba» используется расширение «pgAudit», которое позволяет выполнить требования ГОСТ Р 59548 – 2022 «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации». И таким образом обеспечивает запись дополнительной информации о событиях безопасности, включающую полнотекстовую запись привилегированных команд (команд, управляющих системными функциями).

При этом структура событий безопасности меняется, как представлено на рисунке 3.23.

| time stamp with milliseconds | user name | database name | process ID | client host | port number | session ID | per-session line numbe | command tag | session start time | virtual transaction ID | regular transaction ID | error severity | SQLSTATE code | error message | error message detail | hint | internal query that led to the error | character count of the error position therein | error context | user query that led to the error | character count of the error position therein | location of the error in the PostgreSQL source code |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| штамп времени с миллисекундами | имя пользователя | имя базы данных | идентификатор процесса | клиентский узел | номер порта | идентифи катор сессии | номер строки каждой сессии | тег команды | время начала сессии | виртуальный идентификатор транзакции | идентификатор транзакции | уровень важности ошибки | код ошибки SQLSTATE | сообщение об ошибке | подробности к сообщению об ошибке | подсказка к сообщению об ошибке | внутренний запрос | номер символа внутреннего запроса, где произошла ошибка | контекст ошибки | запрос пользователя | номер символа в запросе пользователя | расположение ошибки в исходном коде |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|
| Pg_audit | | | | | | | | |
| тип записи события | № выражения | № подвыражения | класс события | SQL операция | Тип объекта БД | Имя объекта БД | Полный текст SQL запроса (скрипта) | параметры SQL запроса (скрипта) |

Рисунок 5.1 – Структура события безопасности

Сравнение регистрируемых SQL-команд при стандартной регистрации событий безопасности СУБД и с применением компонента «pgAudit» приведено в таблице 5.11.

Таблица 5.11 – Сравнительная таблица регистрируемых SQL-команд

| **log_statement** | | **pgAudit** | |
|---|---|---|---|
| **Параметр** | **SQL-команды записываемые в журнал** | **Параметр** | **SQL-команды записываемые 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 |

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

| log_statement | | pgAudit | |
|---|---|---|---|
| **Параметр** | **SQL-команды записываемые в журнал** | **Параметр** | **SQL-команды записываемые в журнал** |
| | | **FUNCTION** | CALL |
| | | | DO |
| | | **ROLE** | GRANT |
| | | | REVOKE |
| | | | ALTER DEFAULT PRIVILEGES |
| | | | SET ROLE |
| | | **MISC** | DISCARD |
| | | | FETCH |
| | | | CHECKPOINT |
| | | | VACUUM |
| | | | SET |
| | | **MISC_SET** | SET |
| **NONE** | | NONE | |

**Компонент «ja_Log»**

Компонент устанавливается на целевых СУБД и на служебной СУБД JDS.

В служебной СУБД JDS создается служебная БД «ja_log», в которую будут передаваться события безопасности. Данные собираются в автоматическом режиме при помощи агентов сбора данных с каждой инсталляции:

– сервера СУБД;

– кластера СУБД,

что обеспечивает централизованное управление событиями безопасности.

Схема работы компонента представлена на рисунке 5.2.

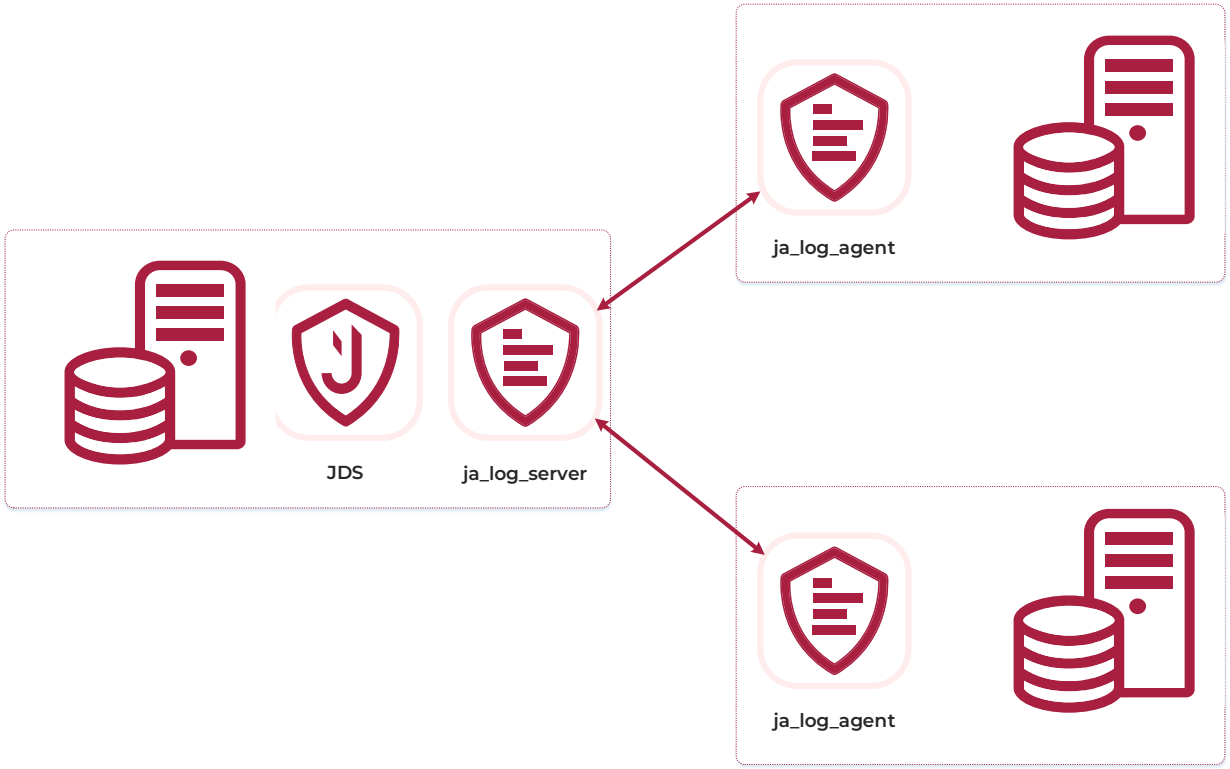


Рисунок 5.2 – Схема работы компонента

Просмотр событий будет доступен через раздел JDS «Event List».

**Компонент пользовательского веб-интерфейса для администраторов «Jatoba Data Safe»**

**Раздел JDS «Event List» (Список событий)**

Раздел JDS «Event List» разработан с учетом требований ГОСТ Р 59548-2022 «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации» (утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 13 января 2022 г. № 2-ст).

Раздел «Event List» предназначен для просмотра событий, собранных с каждой инсталляции СУБД.

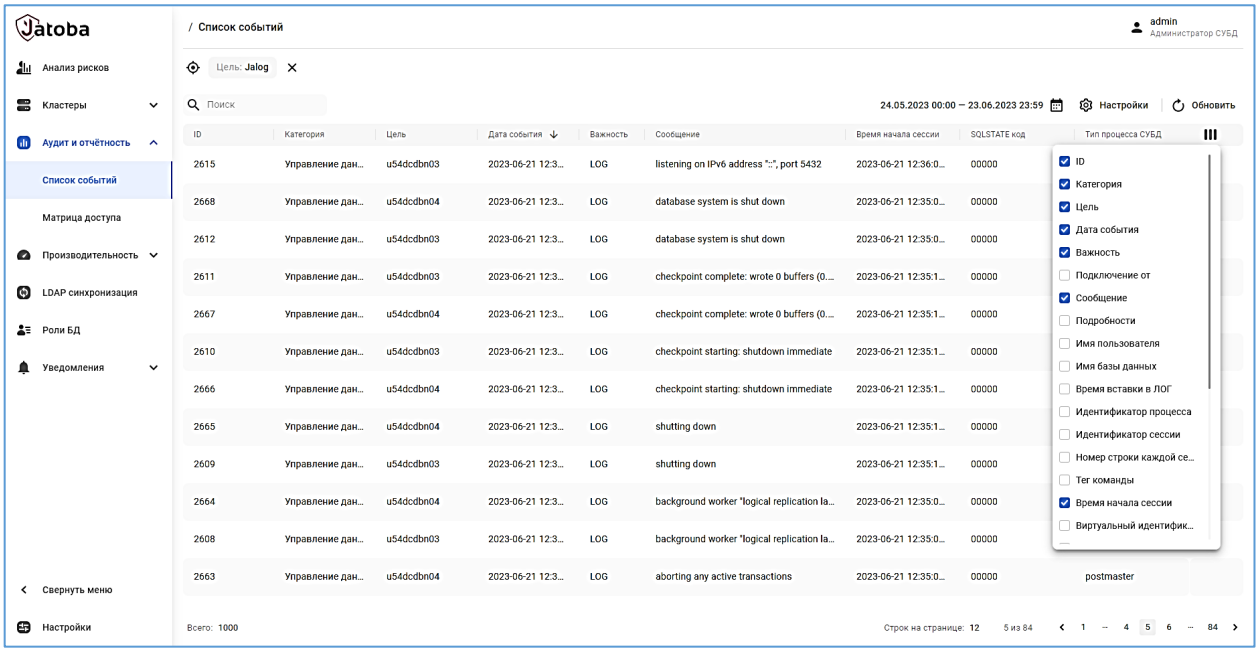


Рисунок 5.3 – Раздел «Event List» (Список событий)

Раздел JDS «Event List» оснащен:

– полем контекстного поиска;

– набором фильтров;

– механизмом выбора отображаемых полей;

– механизмом автоматического обновления.

Время хранения журналов событий СУБД ограничено только выделенным дисковым пространством для служебной БД «ja_log».

**Раздел «Уведомления» (Notifications)**

Организация мониторинга событий СУБД не ограничивается только централизованным сбором событий с СУБД и графическим интерфейсом для их просмотра. В дополнении к описанному реализован механизм уведомлений администраторов СУБД и БД.

Компонент «JDS» периодически будет просматривать служебную БД «ja_log» выбирать события безопасности и при их нахождении перешлет сообщение через сервисы E-mail и/или Zulip.

Механизм уведомлений содержит в себе три типа поиска сообщений:

1) Ошибки БД.

Поиск выполняется по классу события или по коду события.

2) События учетных записей.

Поиск выполняется по ключевым фразам для выполнения мер безопасности УПД.1 (5) и УПД.9 (4) в соответствии с Приказом № 17 ФСТЭК России.

3) Произвольный текст.

Поиск выполняется по ключевым словам, задаваемым пользователем JDS.

Вид раздела «Уведомления» (Notifications) представлен на рисунке 5.4.

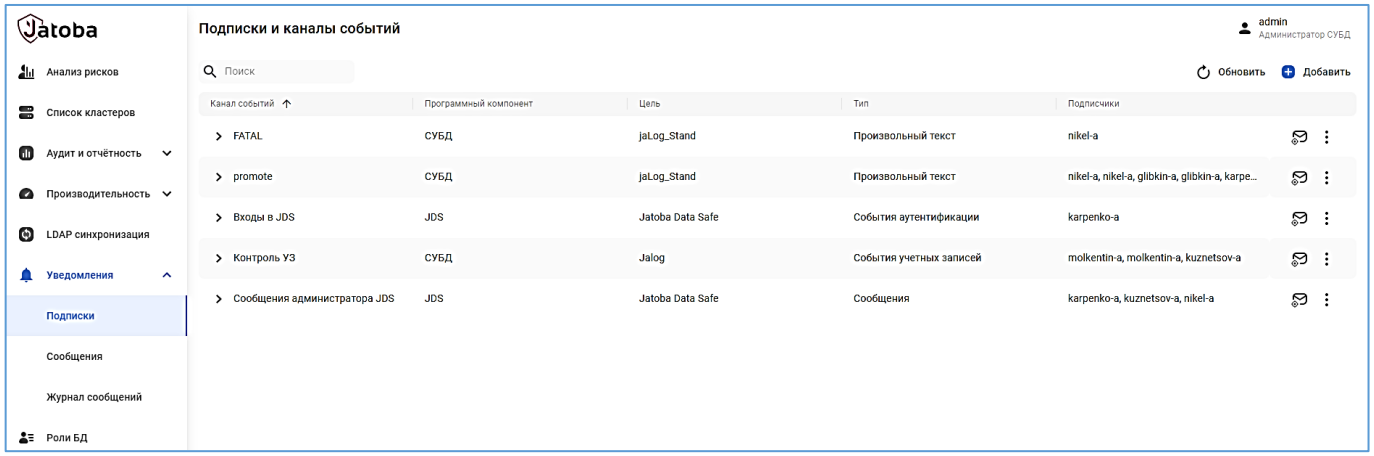


Рисунок 5.4 – Список каналов событий

Перечисленные функциональные возможности обеспечивают возможность организации мониторинга событий информационной безопасности СУБД и реализации меры МАС.4.

### 5.4.2. Базовая мера ЦЗИ.8 Контроль отсутствия известных (описанных) уязвимостей защиты информации объектов информатизации

СУБД «Jatoba» в составе своих функциональных возможностей не имеет технической возможности самостоятельного контроля и устранения уязвимостей, путем сканирования версии СУБД.

Выполнение базовой меры защиты ЦЗИ.8 обеспечивается гарантийными обязательствами Разработчика (производителя) СУБД «Jatoba», зафиксированными в подразделе «Процедура устранения уязвимостей» Формуляра на Изделие.

**ПРИЛОЖЕНИЕ 1**

## Парольные политики

### Параметры парольной политики по умолчанию

Таблица П1.1 – Параметры парольной политики по умолчанию

| Параметр | Примечание | Параметры в профиле по умолчанию | Мин-е значение | Макс-е значение |
|---|---|---|---|---|
| **Параметры для конфигурирования парольной политики** | | | | |
| securityprofile.profile_name | имя профиля по умолчанию | 'default' | | |
| 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 | 0 | 256 |
| securityprofile.upper_case_count | пароль должен содержать как минимум 1 символ в верхнем регистре | 1 | 0 | 256 |
| securityprofile.numbers_count | пароль должен содержать как минимум 1 цифру | 1 | 0 | 256 |
| securityprofile.special_count | пароль должен содержать как минимум 1 спецсимвол из заданного набора special_chars | 1 | 0 | 256 |
| securityprofile.minimum_length | минимальная длина пароля равна 6 символам | 6 | 6 | 256 |
| securityprofile.maximum_length | максимальная длина пароля равна 32 символам | 32 | 6 | 256 |
| securityprofile.minimum_changes | минимальное количество изменений, которое должен содержать новый пароль по сравнению с предыдущим | 0 | 0 | 256 |
| securityprofile.failed_login_attempts | количество неудачных попыток входа в СУБД | 10 | 0 | Int_Max |
| securityprofile.password_lock_time | время, на которое блокируется пользователь при превышении количества неудачных попыток входа в СУБД (1 час в секундах) | 3600 | -1 | 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 |

| Параметр | Примечание | Параметры в профиле по умолчанию | Мин-е значение | Макс-е значение |
|---|---|---|---|---|
| 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<br>(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 = true | Хранение паролей в закрытом виде | True | True | False |
| **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 |

**Параметры парольной политики FSTEC _1_Class**

Таблица П1.2 – 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 |
| 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 спецсимвол 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_tim | время, на которое блокируется пользователь при превышении количества неудачных попыток входа в СУБД (в секундах) | 2700 | 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 |

**Параметры парольной политики FSTEC _2_Class**

Таблица П1.3 – 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 спецсимвол 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 | 5 | Int_Max |
| securityprofile.password_lock_time | время, на которое блокируется пользователь при превышении количества неудачных попыток входа в СУБД (секундах) | 1200 | 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 |

| Параметр | Примечание | Параметры в профиле | Макс-е значение |
|---|---|---|---|
| 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 |

**Параметры парольной политики CIS**

Таблица П1.4 – 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 спецсимвол 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.password_min_life_time | время в секундах, в течение которого пароль должен использоваться и не может быть изменен | 6400 | Int_Max |
| securityprofile.password_life_time | время в секундах, в течение которого может быть использован текущий пароль (в секундах) | 7776000 | Int_Max |

| Параметр | Примечание | Параметры в профиле | Макс-е значение |
|---|---|---|---|
| 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 |

**Параметры парольной политики Corporate_1**

Таблица П1.5 – 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 |
| 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 спецсимвол 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 = 0 | 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) | -1 | Int_Max |
| securityprofile.password_min_life_time | время в секундах, в течение которого пароль должен использоваться и не может быть изменен | 0 | Int_Max |

| Параметр | Примечание | Параметры в профиле | Макс-е значение |
|---|---|---|---|
| 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. 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 |

**Параметры парольной политики Corporate_2**

Таблица П1.6 – 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 0 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 спецсимвол 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 час в секундах) | -1 | 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 |

| Параметр | Примечание | Параметры в профиле | Макс-е значение |
|---|---|---|---|
| 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 |

**Параметры парольной политики Corporate_3**

Таблица П1.7 – 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 | \!"#$%&()*+ ,- ./:;<=>?@[]^ _`{\|}~ | |
| securityprofile.lower_case_count | пароль должен содержать как минимум 0 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 спецсимвол 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 час в секундах) | -1 | 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 |

| Параметр | Примечание | Параметры в профиле | Макс-е значение |
|---|---|---|---|
| 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 | -1 | 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 |

**ПРИЛОЖЕНИЕ 2**

## Соответствие требованиям приказов ФСТЭК к составу событий безопасности

Таблица П2.1 – Состав и содержание регистрируемой информации

| № | Наименование поля | Расположение поля | Описание | Расширение СУБД | Требования приказов ФСТЭК к составу событий | |
|---|---|---|---|---|---|---|
| | | | | | Приказ ФСТЭК № 17 | Приказ ФСТЭК № 64 |
| 1 | **Target** | **DB ja_Log** | **Цель** | | | |
| 2 | **Id** | **DB ja_Log** | **Идентификатор записи** | | | Уникальный идентификатор |
| 3 | **cat_id** | **DB ja_Log** | **Тип события** | | Тип события | Тип события |
| 4 | **comp_id** | **DB ja_Log** | **Наименование компонента** | | | |
| 5 | **sql_state_code_class** | **DB ja_Log** | **Код класса события** | | | |
| 6 | **time stamp with milliseconds** | postgres.csv | штамп времени с миллисекундами | | Дата и время события | Дата и время события |
| 7 | **Criticality** | postgres.csv | критичность события | | | |
| 8 | **Class** | postgres.csv | класс события | | | |
| 9 | **user name** | postgres.csv | имя пользователя | | Идентификатор субъекта доступа | |
| 10 | **database name** | postgres.csv | имя базы данных | | Спецификация объекта доступа (логическое имя, тип, номер) | |
| 11 | **process ID** | postgres.csv | идентификатор процесса | | | |
| 12 | **client host** | postgres.csv | клиентский узел | | | |
| 13 | **port number** | postgres.csv | номер порта | | | |
| 14 | **session ID** | postgres.csv | идентификатор сессии | | | |
| 15 | **per-session line number** | postgres.csv | номер строки каждой сессии | | | |

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

| № | Наименование поля | Расположение поля | Описание | Расширение СУБД | Требования приказов ФСТЭК к составу событий | |
|---|---|---|---|---|---|---|
| | | | | | Приказ ФСТЭК № 17 | Приказ ФСТЭК № 64 |
| 16 | **command tag** | postgres.csv | тег команды | | | |
| 17 | **session start time** | postgres.csv | время начала сессии | | | |
| 18 | **virtual transaction ID** | postgres.csv | виртуальный идентификатор транзакции | | | |
| 19 | **regular transaction ID** | postgres.csv | идентификатор транзакции | | | |
| 20 | **error severity** | postgres.csv | уровень важности ошибки (Уровень ошибки) | | | Сведения о важности события |
| 21 | **SQLSTATE code** | postgres.csv | код ошибки SQLSTATE | | | |
| 22 | **error message** | postgres.csv | сообщение об ошибке | | Результат | |
| *22.1* | *Audit_type* | postgres.csv | тип записи события | pgAudit | | |
| *22.2* | *Statement_id* | postgres.csv | № выражения | pgAudit | | |
| *22.3* | *Substatement_id* | postgres.csv | № подвыражения | pgAudit | | |
| *22.4* | *Class* | postgres.csv | класс события | pgAudit | | |
| *22.5* | *Command* | postgres.csv | SQL-операция | pgAudit | | |
| *22.6* | *Object_type* | postgres.csv | Тип объекта БД | pgAudit | Спецификация объекта доступа (логическое имя, тип, номер) | |
| *22.7* | *Object_name* | postgres.csv | Имя объекта БД | pgAudit | Спецификация объекта доступа (логическое имя, тип, номер) | |
| *22.8* | *Statement* | postgres.csv | Полный текст SQL-запроса (скрипта) | pgAudit | | |
| *22.9* | Parameter | postgres.csv | параметры SQL-запроса (скрипта) | pgAudit | | |
| 23 | **error message detail** | postgres.csv | подробности к сообщению об ошибке | | Результат | |
| 24 | **hint** | postgres.csv | подсказка к сообщению об ошибке | | | |

| № | Наименование поля | Расположение поля | Описание | Расширение СУБД | Требования приказов ФСТЭК к составу событий | |
|---|---|---|---|---|---|---|
| | | | | | Приказ ФСТЭК № 17 | Приказ ФСТЭК № 64 |
| 25 | **internal query that led to the error** | postgres.csv | внутренний запрос | | | |
| 26 | **character count of the error position therein** | postgres.csv | номер символа внутреннего запроса, где произошла ошибка | | | |
| 27 | **error context** | postgres.csv | контекст ошибки | | | |
| 28 | **user query that led to the error** | postgres.csv | запрос пользователя | | | |
| 29 | **character count of the error position therein** | postgres.csv | номер символа в запросе пользователя | | | |
| 30 | **location of the error in the PostgreSQL source code** | postgres.csv | расположение ошибки в исходном коде | | | |

**ПРИЛОЖЕНИЕ 3**

## Соответствие событий СУБД категориям мер защиты приказов ФСТЭК

Таблица П3.1 – Соответствие событий СУБД категориям мер защиты приказов ФСТЭК

| Категория события | Аббревиатура категории события | sql_state_code | Наименование |
|---|---|---|---|
| **Class 00 — Successful Completion** | | | |
| Управление данными | | 00000 | successful_completion |
| **Class 01 — Warning** | | | |
| Управление данными | | 01000 | warning |
| Управление данными | | 0100C | dynamic_result_sets_returned |
| Управление данными | | 01008 | implicit_zero_bit_padding |
| Управление данными | | 01003 | null_value_eliminated_in_set_function |
| Управление данными | | 01007 | privilege_not_granted |
| Управление доступом | УПД | 01006 | privilege_not_revoked |
| Управление данными | | 01004 | string_data_right_truncation |
| Управление данными | | 01P01 | deprecated_feature |
| **Class 02 — No Data (this is also a warning class per the SQL standard)** | | | |
| Управление данными | | 02000 | no_data |
| Управление данными | | 02001 | no_additional_dynamic_result_sets_returned |
| **Class 03 — SQL Statement Not Yet Complete** | | | |
| Управление данными | | 03000 | sql_statement_not_yet_complete |
| **Class 08 — Connection Exception** | | | |
| Управление доступом | УПД | 08000 | connection_exception |

| Категория события | Аббревиатура категории события | sql_state_code | Наименование |
|---|---|---|---|
| Управление доступом | УПД | 08003 | connection_does_not_exist |
| Управление доступом | УПД | 08006 | connection_failure |
| Управление доступом | УПД | 08001 | sqlclient_unable_to_establish_sqlconnection |
| Управление доступом | УПД | 08004 | sqlserver_rejected_establishment_of_sqlconnection |
| Управление доступом | УПД | 08007 | transaction_resolution_unknown |
| Управление доступом | УПД | 08P01 | protocol_violation |
| **Class 09 — Triggered Action Exception** | | | |
| Управление данными | | 09000 | triggered_action_exception |
| **Class 0A — Feature Not Supported** | | | |
| Управление данными | | 0A000 | feature_not_supported |
| **Class 0B — Invalid Transaction Initiation** | | | |
| Управление данными | | 0B000 | invalid_transaction_initiation |
| **Class 0F — Locator Exception** | | | |
| Прочее | | 0F000 | locator_exception |
| Прочее | | 0F001 | invalid_locator_specification |
| **Class 0L — Invalid Grantor** | | | |
| Управление доступом | УПД | 0L000 | invalid_grantor |
| Управление доступом | УПД | 0LP01 | invalid_grant_operation |
| **Class 0P — Invalid Role Specification** | | | |
| Управление доступом | УПД | 0P000 | invalid_role_specification |
| **Class 0Z — Diagnostics Exception** | | | |
| Управление данными | | 0Z000 | diagnostics_exception |
| Управление данными | | 0Z002 | stacked_diagnostics_accessed_without_active_handler |
| **Class 20 — Case Not Found** | | | |

| Категория события | Аббревиатура категории события | sql_state_code | Наименование |
|---|---|---|---|
| Управление данными | | 20000 | case_not_found |
| **Class 21 — Cardinality Violation** | | | |
| Прочее | | 21000 | cardinality_violation |
| **Class 22 — Data Exception** | | | |
| Управление данными | | 22000 | data_exception |
| Управление данными | | 2202E | array_subscript_error |
| Управление данными | | 22021 | character_not_in_repertoire |
| Управление данными | | 22008 | datetime_field_overflow |
| Управление данными | | 22012 | division_by_zero |
| Управление данными | | 22005 | error_in_assignment |
| Управление данными | | 2200B | escape_character_conflict |
| Управление данными | | 22022 | indicator_overflow |
| Управление данными | | 22015 | interval_field_overflow |
| Управление данными | | 2201E | invalid_argument_for_logarithm |
| Управление данными | | 22014 | invalid_argument_for_ntile_function |
| Управление данными | | 22016 | invalid_argument_for_nth_value_function |
| Управление данными | | 2201F | invalid_argument_for_power_function |
| Управление данными | | 2201G | invalid_argument_for_width_bucket_function |
| Управление данными | | 22018 | invalid_character_value_for_cast |
| Управление данными | | 22007 | invalid_datetime_format |
| Управление данными | | 22019 | invalid_escape_character |
| Управление данными | | 2200D | invalid_escape_octet |

| Категория события | Аббревиатура категории события | sql_state_code | Наименование |
|---|---|---|---|
| Управление данными | | 22025 | invalid_escape_sequence |
| Управление данными | | 22P06 | nonstandard_use_of_escape_character |
| Управление данными | | 22010 | invalid_indicator_parameter_value |
| Управление данными | | 22023 | invalid_parameter_value |
| Управление данными | | 22013 | invalid_preceding_or_following_size |
| Управление данными | | 2201B | invalid_regular_expression |
| Управление данными | | 2201W | invalid_row_count_in_limit_clause |
| Управление данными | | 2201X | invalid_row_count_in_result_offset_clause |
| Управление данными | | 2202H | invalid_tablesample_argument |
| Управление данными | | 2202G | invalid_tablesample_repeat |
| Управление данными | | 22009 | invalid_time_zone_displacement_value |
| Управление данными | | 2200C | invalid_use_of_escape_character |
| Управление данными | | 2200G | most_specific_type_mismatch |
| Управление данными | | 22004 | null_value_not_allowed |
| Управление данными | | 22002 | null_value_no_indicator_parameter |
| Управление данными | | 22003 | numeric_value_out_of_range |
| Управление данными | | 2200H | sequence_generator_limit_exceeded |
| Управление данными | | 22026 | string_data_length_mismatch |
| Управление данными | | 22001 | string_data_right_truncation |
| Управление данными | | 22011 | substring_error |
| Управление данными | | 22027 | trim_error |
| Управление данными | | 22024 | unterminated_c_string |

| Категория события | Аббревиатура категории события | sql_state_code | Наименование |
|---|---|---|---|
| Управление данными | | 2200F | zero_length_character_string |
| Управление данными | | 22P01 | floating_point_exception |
| Управление данными | | 22P02 | invalid_text_representation |
| Управление данными | | 22P03 | invalid_binary_representation |
| Управление данными | | 22P04 | bad_copy_file_format |
| Управление данными | | 22P05 | untranslatable_character |
| Управление данными | | 2200L | not_an_xml_document |
| Управление данными | | 2200M | invalid_xml_document |
| Управление данными | | 2200N | invalid_xml_content |
| Управление данными | | 2200S | invalid_xml_comment |
| Управление данными | | 2200T | invalid_xml_processing_instruction |
| Управление данными | | 22030 | duplicate_json_object_key_value |
| Управление данными | | 22031 | invalid_argument_for_sql_json_datetime_function |
| Управление данными | | 22032 | invalid_json_text |
| Управление данными | | 22033 | invalid_sql_json_subscript |
| Управление данными | | 22034 | more_than_one_sql_json_item |
| Управление данными | | 22035 | no_sql_json_item |
| Управление данными | | 22036 | non_numeric_sql_json_item |
| Управление данными | | 22037 | non_unique_keys_in_a_json_object |
| Управление данными | | 22038 | singleton_sql_json_item_required |
| Управление данными | | 22039 | sql_json_array_not_found |
| Управление данными | | 2203A | sql_json_member_not_found |

| Категория события | Аббревиатура категории события | sql_state_code | Наименование |
|---|---|---|---|
| Управление данными | | 2203B | sql_json_number_not_found |
| Управление данными | | 2203C | sql_json_object_not_found |
| Управление данными | | 2203D | too_many_json_array_elements |
| Управление данными | | 2203E | too_many_json_object_members |
| Управление данными | | 2203F | sql_json_scalar_required |
| Управление данными | | 2203G | sql_json_item_cannot_be_cast_to_target_type |
| **Class 23 — Integrity Constraint Violation** | | | |
| Контроль целостности | | 23000 | integrity_constraint_violation |
| Контроль целостности | | 23001 | restrict_violation |
| Контроль целостности | | 23502 | not_null_violation |
| Контроль целостности | | 23503 | foreign_key_violation |
| Контроль целостности | | 23505 | unique_violation |
| Контроль целостности | | 23514 | check_violation |
| Контроль целостности | | 23P01 | exclusion_violation |
| **Class 24 — Invalid Cursor State** | | | |
| Прочее | | 24000 | invalid_cursor_state |
| **Class 25 — Invalid Transaction State** | | | |
| Управление данными | | 25000 | invalid_transaction_state |
| Управление данными | | 25001 | active_sql_transaction |
| Управление данными | | 25002 | branch_transaction_already_active |
| Управление данными | | 25008 | held_cursor_requires_same_isolation_level |
| Управление данными | | 25003 | inappropriate_access_mode_for_branch_transaction |
| Управление данными | | 25004 | inappropriate_isolation_level_for_branch_transaction |

| Категория события | Аббревиатура категории события | sql_state_code | Наименование |
|---|---|---|---|
| Управление данными | | 25005 | no_active_sql_transaction_for_branch_transaction |
| Управление данными | | 25006 | read_only_sql_transaction |
| Управление данными | | 25007 | schema_and_data_statement_mixing_not_supported |
| Управление данными | | 25P01 | no_active_sql_transaction |
| Управление данными | | 25P02 | in_failed_sql_transaction |
| Управление данными | | 25P03 | idle_in_transaction_session_timeout |
| **Class 26 — Invalid SQL Statement Name** | | | |
| Управление данными | | 26000 | invalid_sql_statement_name |
| **Class 27 — Triggered Data Change Violation** | | | |
| Управление доступом | УПД | 27000 | triggered_data_change_violation |
| **Class 28 — Invalid Authorization Specification** | | | |
| Идентификация | ИАФ | 28000 | invalid_authorization_specification |
| Идентификация | ИАФ | 28P01 | invalid_password |
| **Class 2B — Dependent Privilege Descriptors Still Exist** | | | |
| Управление доступом | УПД | 2B000 | dependent_privilege_descriptors_still_exist |
| Управление доступом | УПД | 2BP01 | dependent_objects_still_exist |
| **Class 2D — Invalid Transaction Termination** | | | |
| Управление данными | | 2D000 | invalid_transaction_termination |
| **Class 2F — SQL Routine Exception** | | | |
| Управление доступом | УПД | 2F000 | sql_routine_exception |
| Управление доступом | УПД | 2F005 | function_executed_no_return_statement |
| Управление доступом | УПД | 2F002 | modifying_sql_data_not_permitted |
| Управление доступом | УПД | 2F003 | prohibited_sql_statement_attempted |

| Категория события | Аббревиатура категории события | sql_state_code | Наименование |
|---|---|---|---|
| Управление доступом | УПД | 2F004 | reading_sql_data_not_permitted |
| **Class 34 — Invalid Cursor Name** | | | |
| Прочее | | 34000 | invalid_cursor_name |
| **Class 38 — External Routine Exception** | | | |
| Управление доступом | УПД | 38000 | external_routine_exception |
| Управление доступом | УПД | 38001 | containing_sql_not_permitted |
| Управление доступом | УПД | 38002 | modifying_sql_data_not_permitted |
| Управление доступом | УПД | 38003 | prohibited_sql_statement_attempted |
| Управление доступом | УПД | 38004 | reading_sql_data_not_permitted |
| **Class 39 — External Routine Invocation Exception** | | | |
| Управление данными | | 39000 | external_routine_invocation_exception |
| Управление данными | | 39001 | invalid_sqlstate_returned |
| Управление данными | | 39004 | null_value_not_allowed |
| Управление данными | | 39P01 | trigger_protocol_violated |
| Управление данными | | 39P02 | srf_protocol_violated |
| Управление данными | | 39P03 | event_trigger_protocol_violated |
| **Class 3B — Savepoint Exception** | | | |
| Резервное копирование | ОДТ | 3B000 | savepoint_exception |
| Резервное копирование | ОДТ | 3B001 | invalid_savepoint_specification |
| **Class 3D — Invalid Catalog Name** | | | |
| Прочее | | 3D000 | invalid_catalog_name |
| **Class 3F — Invalid Schema Name** | | | |
| Управление данными | | 3F000 | invalid_schema_name |

| Категория события | Аббревиатура категории события | sql_state_code | Наименование |
|---|---|---|---|
| **Class 40 — Transaction Rollback** | | | |
| Управление данными | | 40000 | transaction_rollback |
| Управление данными | | 40002 | transaction_integrity_constraint_violation |
| Управление данными | | 40001 | serialization_failure |
| Управление данными | | 40003 | statement_completion_unknown |
| Управление данными | | 40P01 | deadlock_detected |
| **Class 42 — Syntax Error or Access Rule Violation** | | | |
| Управление доступом | УПД | 42000 | syntax_error_or_access_rule_violation |
| Управление данными | | 42601 | syntax_error |
| Управление доступом | УПД | 42501 | insufficient_privilege |
| Управление доступом | УПД | 42846 | cannot_coerce |
| Управление доступом | УПД | 42803 | grouping_error |
| Управление данными | | 42P20 | windowing_error |
| Управление данными | | 42P19 | invalid_recursion |
| Идентификация | ИАФ | 42830 | invalid_foreign_key |
| Управление данными | | 42602 | invalid_name |
| Управление данными | | 42622 | name_too_long |
| Управление данными | | 42939 | reserved_name |
| Контроль целостности данных | ОЦЛ | 42804 | datatype_mismatch |
| Контроль целостности данных | ОЦЛ | 42P18 | indeterminate_datatype |
| Управление данными | | 42P21 | collation_mismatch |
| Управление данными | | 42P22 | indeterminate_collation |

| Категория события | Аббревиатура категории события | sql_state_code | Наименование |
|---|---|---|---|
| Контроль целостности данных | ОЦД | 42809 | wrong_object_type |
| Управление данными | | 428C9 | generated_always |
| Управление данными | | 42703 | undefined_column |
| Управление данными | | 42883 | undefined_function |
| Управление данными | | 42P01 | undefined_table |
| Управление данными | | 42P02 | undefined_parameter |
| Управление данными | | 42704 | undefined_object |
| Управление данными | | 42701 | duplicate_column |
| Управление данными | | 42P03 | duplicate_cursor |
| Управление данными | | 42P04 | duplicate_database |
| Управление данными | | 42723 | duplicate_function |
| Управление данными | | 42P05 | duplicate_prepared_statement |
| Управление данными | | 42P06 | duplicate_schema |
| Управление данными | | 42P07 | duplicate_table |
| Управление данными | | 42712 | duplicate_alias |
| Управление данными | | 42710 | duplicate_object |
| Управление данными | | 42702 | ambiguous_column |
| Управление данными | | 42725 | ambiguous_function |
| Управление данными | | 42P08 | ambiguous_parameter |
| Управление данными | | 42P09 | ambiguous_alias |
| Управление данными | | 42P10 | invalid_column_reference |
| Управление данными | | 42611 | invalid_column_definition |

| Категория события | Аббревиатура категории события | sql_state_code | Наименование |
|---|---|---|---|
| Управление данными | | 42P11 | invalid_cursor_definition |
| Управление данными | | 42P12 | invalid_database_definition |
| Управление данными | | 42P13 | invalid_function_definition |
| Управление данными | | 42P14 | invalid_prepared_statement_definition |
| Управление данными | | 42P15 | invalid_schema_definition |
| Управление данными | | 42P16 | invalid_table_definition |
| Управление данными | | 42P17 | invalid_object_definition |
| **Class 44 — WITH CHECK OPTION Violation** | | | |
| Прочее | | 44000 | with_check_option_violation |
| **Class 53 — Insufficient Resources** | | | |
| Прочее | | 53000 | insufficient_resources |
| Прочее | | 53100 | disk_full |
| Прочее | | 53200 | out_of_memory |
| Прочее | | 53300 | too_many_connections |
| Прочее | | 53400 | configuration_limit_exceeded |
| **Class 54 — Program Limit Exceeded** | | | |
| Управление данными | | 54000 | program_limit_exceeded |
| Управление данными | | 54001 | statement_too_complex |
| Управление данными | | 54011 | too_many_columns |
| Управление данными | | 54023 | too_many_arguments |
| **Class 55 — Object Not In Prerequisite State** | | | |
| Управление данными | | 55000 | object_not_in_prerequisite_state |
| Управление данными | | 55006 | object_in_use |

| Категория события | Аббревиатура категории события | sql_state_code | Наименование |
|---|---|---|---|
| Управление данными | | 55P02 | cant_change_runtime_param |
| Управление данными | | 55P03 | lock_not_available |
| Управление данными | | 55P04 | unsafe_new_enum_value_usage |
| **Class 57 — Operator Intervention** | | | |
| Прочее | | 57000 | operator_intervention |
| Прочее | | 57014 | query_canceled |
| Прочее | | 57P01 | admin_shutdown |
| Прочее | | 57P02 | crash_shutdown |
| Прочее | | 57P03 | cannot_connect_now |
| Прочее | | 57P04 | database_dropped |
| Прочее | | 57P05 | idle_session_timeout |
| **Class 58 — System Error (errors external to PostgreSQL itself)** | | | |
| Прочее | | 58000 | system_error |
| Прочее | | 58030 | io_error |
| Управление данными | | 58P01 | undefined_file |
| Управление данными | | 58P02 | duplicate_file |
| | | **Class 72 — Snapshot Failure** | |
| Управление данными | | 72000 | snapshot_too_old |
| **Class F0 — Configuration File Error** | | | |
| Прочее | | F0000 | config_file_error |
| Прочее | | F0001 | lock_file_exists |
| **Class HV — Foreign Data Wrapper Error (SQL/MED)** | | | |
| Управление данными | | HV000 | fdw_error |

| Категория события | Аббревиатура категории события | sql_state_code | Наименование |
|---|---|---|---|
| Управление данными | | HV005 | fdw_column_name_not_found |
| Управление данными | | HV002 | fdw_dynamic_parameter_value_needed |
| Управление данными | | HV010 | fdw_function_sequence_error |
| Управление данными | | HV021 | fdw_inconsistent_descriptor_information |
| Управление данными | | HV024 | fdw_invalid_attribute_value |
| Управление данными | | HV007 | fdw_invalid_column_name |
| Управление данными | | HV008 | fdw_invalid_column_number |
| Управление данными | | HV004 | fdw_invalid_data_type |
| Управление данными | | HV006 | fdw_invalid_data_type_descriptors |
| Управление данными | | HV091 | fdw_invalid_descriptor_field_identifier |
| Управление данными | | HV00B | fdw_invalid_handle |
| Управление данными | | HV00C | fdw_invalid_option_index |
| Управление данными | | HV00D | fdw_invalid_option_name |
| Управление данными | | HV090 | fdw_invalid_string_length_or_buffer_length |
| Управление данными | | HV00A | fdw_invalid_string_format |
| Управление данными | | HV009 | fdw_invalid_use_of_null_pointer |
| Управление данными | | HV014 | fdw_too_many_handles |
| Управление данными | | HV001 | fdw_out_of_memory |
| Управление данными | | HV00P | fdw_no_schemas |
| Управление данными | | HV00J | fdw_option_name_not_found |
| Управление данными | | HV00K | fdw_reply_handle |
| Управление данными | | HV00Q | fdw_schema_not_found |

| Категория события | Аббревиатура категории события | sql_state_code | Наименование |
|---|---|---|---|
| Управление данными | | HV00R | fdw_table_not_found |
| Управление данными | | HV00L | fdw_unable_to_create_execution |
| Управление данными | | HV00M | fdw_unable_to_create_reply |
| Управление данными | | HV00N | fdw_unable_to_establish_connection |
| **Class P0 — PL/pgSQL Error** | | | |
| Управление данными | | P0000 | plpgsql_error |
| Управление данными | | P0001 | raise_exception |
| Управление данными | | P0002 | no_data_found |
| Управление данными | | P0003 | too_many_rows |
| Управление данными | | P0004 | assert_failure |
| **Class XX — Internal Error** | | | |
| Прочее | | XX000 | internal_error |
| Управление данными | | XX001 | data_corrupted |
| Управление данными | | XX002 | index_corrupted |

# ПРИЛОЖЕНИЕ 4

## Соответствие требованиям приказов ФСТЭК к составу событий безопасности и структура справочной таблицы со всеми полями для формирования JSON

Таблица 4.1 – Структура справочной таблицы со всеми полями для формирования JSON

| Ключ JSON | Наименование | Требование ГОСТ Р 59548-2022 | Приказ ФСТЭК № 17 | Приказ ФСТЭК № 64 |
|---|---|---|---|---|
| timestamp | Дата и время<br>(Формат «Дата и время», пример: 2019-05-20T18:30:15.587+04:00) | X | Дата и время события | Дата и время события |
| user | Идентификатор учетной записи<br>(по умолчанию – имя пользователя) | X | Идентификатор субъекта доступа | – |
| dbname | Имя базы данных | X | Спецификация объекта доступа (логическое имя, тип, номер) | – |
| pid | Идентификатор процесса | X | – | – |
| remote_host | Имя компьютера клиента | X | – | – |
| remote_port | Порт компьютера клиента | X | – | – |
| session_id | Идентификатор сеанса | X | – | – |
| line_num | Номер строки внутри сеанса | X | – | – |
| ps | Тег команды | X | – | – |
| session_start | Время начала сессии | X | – | – |
| vxid | Идентификатор виртуальной транзакции | X | – | – |
| txid | Идентификатор транзакции | X | – | – |
| error_severity | Уровень важности ошибки | X | – | Сведения о важности события |
| state_code | Код SQLSTATE | X | – | – |
| message | Сообщение об ошибке | X | – | – |
| Audit_type | Тип записи события | X | – | – |
| Statement_id | № выражения | X | – | – |

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

| Ключ JSON | Наименование | Требование ГОСТ Р 59548-2022 | Приказ ФСТЭК № 17 | Приказ ФСТЭК № 64 |
|---|---|---|---|---|
| Substatement_id | № подвыражения | X | – | – |
| Class | Класс выражения | X | – | – |
| Command | SQL-выражение | X | – | – |
| Object_type | Тип объекта БД | X | Спецификация объекта доступа (логическое имя, тип, номер) | – |
| Object_name | Имя объекта БД | X | Спецификация объекта доступа (логическое имя, тип, номер) | – |
| Statement | Полный текст SQL-выражения | X | – | – |
| Parameter | Параметры SQL-выражения | X | – | – |
| application_name | Имя клиентского приложения | X | – | – |
| backend_type | Тип обслуживающего процесса | X | – | – |
| leader_pid | Идентификатор ведущего процесса группы параллельных исполнителей | X | – | – |
| query_id | Идентификатор запроса | X | – | – |
| secEventId | Идентификатор (Код типа события безопасности + Код наименования события безопасности + Код компонента) | X | – | Идентификатор события |
| secEventType | Тип (из поля «Сокращенное наименование типа события безопасности») | X | – | – |
| secEventName | Наименование (из поля «Сокращенное наименование события безопасности») | X | – | – |
| secEventSubject | Субъект доступа (по умолчанию – имя пользователя) | X | – | – |
| secEventLevel | Уровень важности (из поля «Уровень важности») | X | – | – |
| secEventHostName | Имя сервера базы данных (pg_gethostname()) | X | – | – |
| secEventResultOperation | Результат операции (Принимаемые значения: успешный/неуспешный) | X | Результат | – |

| Ключ JSON | Наименование | Требование ГОСТ Р 59548-2022 | Приказ ФСТЭК № 17 | Приказ ФСТЭК № 64 |
|---|---|---|---|---|
| secEventAdminRights | Наличие прав администратора<br>(Принимаемые значения: да/нет) | X | – | – |
| secEventIp | Сетевой адрес источника входа<br>(Формат «Сетевой адрес») | X | – | – |
| secEventInputType | Тип входа<br>(Принимаемое значение: интерактивный) | X | – | – |
| secEventFullPath | Наименование процесса (полный путь)<br>(Формат «Текст». Указывают полный путь) | X | – | – |
| secEventLastInput | Дата и время последнего входа<br>(Формат «Дата и время». Указывают дату и время последней авторизации учетной записи) | X | – | – |
| secEventValidUntil | Срок действия учетной записи<br>(Формат «Дата/время». Указывают дату и время окончания срока действия пароля учетной записи. Если срок действия пароля учетной записи не ограничен, указывают значение, определяемое изготовителем средства) | X | – | – |
| secEventTypeAction | Тип действия<br>(Принимаемые значения: создание/ изменение/ удаление/ чтение/ запись/ исполнение/ установка/ остановка/ запуск/ резервное копирование/восстановление/другое) | X | – | – |
| secEventComponentName | Компонент ПО<br>(Указывают краткое наименование) | X | – | – |
| secEventComponentVersion | Версия компонента<br>(Формат «Версия ПО») | X | – | – |
| secEventComponentDeveloper | Разработчик компонента<br>(Указывают полное официальное наименование компании) | X | – | – |
| secEventComponentType | Тип компонента | X | – | – |
| secEventSoftName | Наименование ПО<br>(Указывают полное официальное наименование ПО) | X | – | – |

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

| Ключ JSON | Наименование | Требование ГОСТ Р 59548-2022 | Приказ ФСТЭК № 17 | Приказ ФСТЭК № 64 |
|---|---|---|---|---|
| secEventParameterNew | Новые (измененные) значения параметров конфигурации (Формат «Текст». Указывают в следующем виде: «параметр: старое значение => новое значение;». Если параметров несколько, то они отделяются при помощи разделителя «;») | X | – | – |
| secEventParameterAll | Значения параметров конфигурации ja_seceventlog.<br>Указывается при событиях 119204 и 119205.<br>(Формат "Текст". Указывают в следующем виде: "параметр: значение;". Если параметров несколько, то они отделяются при помощи разделителя ";") | – | – | – |
| secEventLogDelete | Удаленный файл журнала ja_seceventlog.<br>Указывается при событии 119193.<br>Указывается полный путь и имя файла с расширением. | – | – | – |
| secEventPartitionClear | Удаленная партиция таблицы ja_seceventlog.<br>Указывается при событии 119193.<br>Указывается час, за который удалена партиция. | – | – | – |
| secEventLogSizeLimit | Лимит объема памяти, выделенного для хранения журналов регистрации событий безопасности ja_seceventlog.<br>Указывается при событиях 119203 и 119206.<br>При событии 119203 (soft_limit) рассчитывается как ja_seceventlog.log_size_soft_limit * ja_seceventlog.maxsize.<br>При событии 119206 (hard_limit) рассчитывается как ja_seceventlog.log_size_hard_limit * ja_seceventlog.maxsize.<br>Указывается в kB. | – | – | – |
| secEventLogSize | Указывается при событиях 119203 и 119206.<br>Заполненный объем памяти, выделенного для хранения журналов регистрации событий безопасности ja_seceventlog (Общий размер всех файлов логов).<br>Указывается в kB. | – | – | – |

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

## Структура справочной таблицы с правилами кодирования событий безопасности для формирования JSON

Таблица 4.2 – Структура справочной таблицы (ja_seceventlog.secevent_code_desc) с типами и уровнем важности событий безопасности

| **Идентификатор события безопасности** | **Тип события безопасности** | **Сокращенное наименование типа события безопасности** | **Наименование события безопасности** | **Сокращенное наименование события безопасности** | **Уровень важности** | **Пример выражения** |
|---|---|---|---|---|---|---|
| **secEventId** | | **secEventType** | | **secEventName** | **secEventLevel** | |
| 100100100 | Идентификация и аутентификация субъекта доступа | ИАСД | Отказ во входе в связи с тем, что идентификатор не зарегистрирован | ИАСД.1 | средний | |
| 100101100 | Идентификация и аутентификация субъекта доступа | ИАСД | Отказ во входе в связи с тем, что идентификатор заблокирован | ИАСД.2 | средний | |
| 100102100 | Идентификация и аутентификация субъекта доступа | ИАСД | Отказ во входе в связи с неправильным паролем | ИАСД.3 | средний | |
| 100104100 | Идентификация и аутентификация субъекта доступа | ИАСД | Отказ во входе в связи с тем, что закончен срок действия пароля | ИАСД.5 | средний | VALID UNTIL |

| Идентификатор события безопасности | Тип события безопасности | Сокращенное наименование типа события безопасности | Наименование события безопасности | Сокращенное наименование события безопасности | Уровень важности | Пример выражения |
|---|---|---|---|---|---|---|
| 100105100 | Идентификация и аутентификация субъекта доступа | ИАСД | Успешный вход в систему | Успешный вход в систему | низкий | |
| 100106100 | Идентификация и аутентификация субъекта доступа | ИАСД | Выход из системы | Выход из системы | низкий | |
| 100107100 | Идентификация и аутентификация субъекта доступа | ИАСД | Другие события безопасности | ИАСД.8 | низкий | |
| 103114100 | Управление учетными записями пользователей | УУЗП | Создание учетной записи | УУЗП.1 | низкий | CREATE ROLE |
| 103115100 | Управление учетными записями пользователей | УУЗП | Изменение наименования учетной записи | УУЗП.2 | низкий | ALTER ROLE … RENAME TO |
| 103116100 | Управление учетными записями пользователей | УУЗП | Изменение пароля учетной записи | УУЗП.3 | низкий | ALTER ROLE … PASSWORD |
| 103117100 | Управление учетными записями пользователей | УУЗП | Удаление учетной записи | УУЗП.4 | низкий | DROP ROLE |
| 105125100 | Управление атрибутами доступа | УАД | Создание типа доступа | УАД.1 | низкий | CREATE POLICY |

| **Идентификатор события безопасности** | **Тип события безопасности** | **Сокращенное наименование типа события безопасности** | **Наименование события безопасности** | **Сокращенное наименование события безопасности** | **Уровень важности** | **Пример выражения** |
|---|---|---|---|---|---|---|
| 105126100 | Управление атрибутами доступа | УАД | Изменение типа доступа | УАД.2 | низкий | ALTER POLICY … RENAME TO … |
| 105127100 | Управление атрибутами доступа | УАД | Удаление типа доступа | УАД.3 | низкий | DROP POLICY |
| 105128100 | Управление атрибутами доступа | УАД | Создание группы пользователей | УАД.4 | низкий | CREATE GROUP |
| 105129100 | Управление атрибутами доступа | УАД | Изменение группы пользователей | УАД.5 | низкий | ALTER GROUP … RENAME TO |
| 105130100 | Управление атрибутами доступа | УАД | Удаление группы пользователей | УАД.6 | низкий | DROP GROUP |
| 105131100 | Управление атрибутами доступа | УАД | Занесение учетной записи в группу пользователей | УАД.7 | низкий | ALTER GROUP … ADD USER |
| 105132100 | Управление атрибутами доступа | УАД | Удаление учетной записи из группы пользователей | УАД.8 | низкий | ALTER GROUP … DROP USER |
| 105133100 | Управление атрибутами доступа | УАД | Изменение прав доступа | УАД.9 | низкий | GRANT |
| 105134100 | Управление атрибутами доступа | УАД | Изменение параметров конфиденциального ресурса | УАД.10 | низкий | ALTER DEFAULT PRIVILEGES |

| **Идентификатор события безопасности** | **Тип события безопасности** | **Сокращенное наименование типа события безопасности** | **Наименование события безопасности** | **Сокращенное наименование события безопасности** | **Уровень важности** | **Пример выражения** |
|---|---|---|---|---|---|---|
| 105136100 | Управление атрибутами доступа | УАД | Другие события безопасности | УАД.12 | низкий | |
| 106138100 | Доступ к защищаемой информации | ДЗИ | Ошибка получения доступа | ДЗИ.2 | средний | |
| 106139100 | Доступ к защищаемой информации | ДЗИ | Поступление запроса на предоставление доступа | ДЗИ.3 | низкий | SELECT |
| 106145100 | Доступ к защищаемой информации | ДЗИ | Создание конфиденциального ресурса | ДЗИ.9 | низкий | CREATE SCHEMA/ TABLE/FUNCTION/ SERVER |
| 106146100 | Доступ к защищаемой информации | ДЗИ | Изменение конфиденциального ресурса | ДЗИ.10 | низкий | ALTER SCHEMA/ TABLE/FUNCTION/ SERVER |
| 106147100 | Доступ к защищаемой информации | ДЗИ | Удаление конфиденциального ресурса | ДЗИ.11 | низкий | DROP SCHEMA/ TABLE/ FUNCTION/ SERVER |
| 106148100 | Доступ к защищаемой информации | ДЗИ | Другие события безопасности | ДЗИ.12 | низкий | |

| **Идентификатор события безопасности** | **Тип события безопасности** | **Сокращенное наименование типа события безопасности** | **Наименование события безопасности** | **Сокращенное наименование события безопасности** | **Уровень важности** | **Пример выражения** |
|---|---|---|---|---|---|---|
| 108152100 | Изменение параметров настроек средств защиты информации | ИПНСЗИ | Конфигурация компонента СЗИ изменена | ИПНСЗИ.1 | высокий | ALTER SYSTEM SET |
| 111162100 | Управление запуском/остановкой компонентов программного обеспечения | УЗОКПО | Запуск (завершение) программ и процессов (заданий, задач) | УЗОКПО.1 | низкий | |
| 110159100 | Установка/удаление компонентов программного обеспечения | УУКПО | ПО установлено | УУКПО.2 | средний | CREATE EXTENSION |
| 110160100 | Установка/удаление компонентов программного обеспечения | УУКПО | Служба удалена | УУКПО.3 | средний | DROP EXTENSION |
| 111162100 | Управление запуском/остановкой компонентов программного обеспечения | УЗОКПО | Запуск (завершение) программ и процессов (заданий, задач) | УЗОКПО.1 | критический | |

| **Идентификатор события безопасности** | **Тип события безопасности** | **Сокращенное наименование типа события безопасности** | **Наименование события безопасности** | **Сокращенное наименование события безопасности** | **Уровень важности** | **Пример выражения** |
|---|---|---|---|---|---|---|
| 119193101 | Управление журналами (записями) регистрации событий безопасности | УЖРСБ | Журнал очищен | УЖРСБ.1 | средний | Событие формируется при:<br>1. удалении файла журнала по истечению периода времени, заданном в параметре maxage.<br>2. очистке партиции в таблице БД.<br>3. удалении файла журнала при наступлении события 119206. |
| 119194101 | Управление журналами (записями) регистрации событий безопасности | УЖРСБ | Журналирование отключено | УЖРСБ.2 | критический | Событие формируется при старте СУБД, если значение параметра ja_seceventlog.log не равно ALL. |

| **Идентификатор события безопасности** | **Тип события безопасности** | **Сокращенное наименование типа события безопасности** | **Наименование события безопасности** | **Сокращенное наименование события безопасности** | **Уровень важности** | **Пример выражения** |
|---|---|---|---|---|---|---|
| 119203101 | Управление журналами (записями) регистрации событий безопасности | УЖРСБ | Предупреждение о заполнении установленного процента объема памяти, выделенного для хранения файлов журналов | УЖРСБ.5 | высокий | Событие формируется, если заполнен установленный процент объема памяти, выделенного для хранения файлов журналов, заданном параметрами<br>ja_seceventlog.maxsize<br>ja_seceventlog.log_size_soft_limit |
| 119205101 | Управление журналами (записями) регистрации событий безопасности | УЖРСБ | Журналирование включено | УЖРСБ.7 | критический | Событие формируется после:<br>1.старта/рестарта СУБД<br>2.перезагрузки postgresql.conf<br>если значение параметра ja_seceventlog.log равно ALL. |

| **Идентификатор события безопасности** | **Тип события безопасности** | **Сокращенное наименование типа события безопасности** | **Наименование события безопасности** | **Сокращенное наименование события безопасности** | **Уровень важности** | **Пример выражения** |
|---|---|---|---|---|---|---|
| 119206101 | Управление журналами (записями) регистрации событий безопасности | УЖРСБ | Перезапись событий в связи с заполнением установленного процента объема памяти, выделенного для хранения файлов журналов | УЖРСБ.8 | высокий | Событие формируется, если заполнен установленный процент объема памяти, выделенного для хранения файлов журналов, заданном параметрами<br>ja_seceventlog.maxsize<br>ja_seceventlog.log_size_hard_limit |

## Структура справочной таблицы с компонентами для формирования JSON

Таблица 4.3– Структура справочной таблицы (ja_seceventlog.secevent_code_desc) с компонентами для формирования JSON

| **Код компонента** | **Компонент ПО (краткое наименование)** | **Разработчик компонента (полное официальное наименование компании)** | **Тип компонента** | **Наименование ПО (полное официальное наименование ПО)** |
|---|---|---|---|---|
| **secEventId** | **secEventComponentName** | **secEventComponentDeveloper** | **secEventComponentType** | **secEventSoftName** |
| 100 | jatoba | ООО «Газинформсервис» | Ядро СУБД | Ядро СУБД Jatoba |
| 101 | ja_seceventlog | ООО «Газинформсервис» | Расширение | Компонент регистрации событий информационной безопасности |
| 103 | jaDOG | ООО «Газинформсервис» | Расширение | Компонент управления режимом работы узлов кластера |

**ПРИЛОЖЕНИЕ 5**

## Список ключей JSON для типа события безопасности «Идентификация и аутентификация субъекта доступа»

Таблица 5.1 – Список ключей JSON для типа события безопасности «Идентификация и аутентификация субъекта доступа»

| **Ключ JSON** | **Наименование** |
|---|---|
| timestamp | Дата и время (Формат «Дата и время») |
| user | Идентификатор учетной записи (По умолчанию – имя пользователя) |
| dbname | Имя базы данных |
| pid | Идентификатор процесса |
| remote_host | Имя компьютера клиента |
| remote_port | Порт компьютера клиента |
| session_id | Идентификатор сеанса |
| line_num | Номер строки внутри сеанса |
| ps | Тег команды |
| session_start | Время начала сессии |
| vxid | Идентификатор виртуальной транзакции |
| txid | Идентификатор транзакции |
| error_severity | Уровень важности ошибки |
| state_code | Код SQLSTATE |
| message | Сообщение об ошибке |
| Audit_type | Тип записи события |
| Statement_id | № выражения |
| Substatement_id | № подвыражения |
| Class | Класс выражения |
| Command | SQL-выражение |
| Object_type | Тип объекта БД |

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

| **Ключ JSON** | **Наименование** |
|---|---|
| Object_name | Имя объекта БД |
| Statement | Полный текст SQL-выражения |
| Parameter | Параметры SQL-выражения |
| application_name | Имя клиентского приложения |
| backend_type | Тип обслуживающего процесса |
| leader_pid | Идентификатор ведущего процесса группы параллельных исполнителей |
| query_id | Идентификатор запроса |
| secEventId | Идентификатор<br>Правило формирования:<br>Код типа события безопасности+Код наименования события безопасности+Код компонента |
| secEventType | Тип (Сокращенное наименование типа события безопасности) |
| secEventName | Наименование (Сокращенное наименование события безопасности) |
| secEventSubject | Субъект доступа (По умолчанию – имя пользователя) |
| secEventLevel | Уровень важности |
| secEventHostName | Имя сервера базы данных (pg_gethostname()) |
| secEventResultOperation | Результат операции<br>(Принимаемые значения: успешный/неуспешный) |
| secEventAdminRights | Наличие прав администратора (Принимаемые значения: да/нет) |
| secEventIp | Сетевой адрес источника входа (Формат «Сетевой адрес») |
| secEventInputType | Тип входа (Принимаемое значение: интерактивный) |
| secEventFullPath | Наименование процесса (полный путь) (Формат «Текст». Указывают полный путь) |
| secEventComponentName | Компонент ПО (Краткое наименование) |
| secEventComponentDeveloper | Разработчик компонента |
| secEventComponentType | Тип компонента |
| secEventSoftName | Наименование ПО |

## Список ключей JSON для типа события безопасности «Управление учетными записями пользователей»

Первые три символа значения ключа secEventId (идентификатор события безопасности) = 103.

Таблица 5.2 – Список ключей JSON для типа события безопасности «Управление учетными записями пользователей»

| **Ключ JSON** | **Наименование** |
|---|---|
| timestamp | Дата и время (Формат «Дата и время») |
| user | Идентификатор учетной записи (По умолчанию – имя пользователя) |
| dbname | Имя базы данных |
| pid | Идентификатор процесса |
| remote_host | Имя компьютера клиента |
| remote_port | Порт компьютера клиента |
| session_id | Идентификатор сеанса |
| line_num | Номер строки внутри сеанса |
| ps | Тег команды |
| session_start | Время начала сессии |
| vxid | Идентификатор виртуальной транзакции |
| txid | Идентификатор транзакции |
| error_severity | Уровень важности ошибки |
| state_code | Код SQLSTATE |
| message | Сообщение об ошибке |
| Audit_type | Тип записи события |
| Statement_id | № выражения |
| Substatement_id | № подвыражения |
| Class | Класс выражения |
| Command | SQL-выражение |
| Object_type | Тип объекта БД |
| Object_name | Имя объекта БД |

| **Ключ JSON** | **Наименование** |
|---|---|
| Statement | Полный текст SQL-выражения |
| Parameter | Параметры SQL-выражения |
| application_name | Имя клиентского приложения |
| backend_type | Тип обслуживающего процесса |
| leader_pid | Идентификатор ведущего процесса группы параллельных исполнителей |
| query_id | Идентификатор запроса |
| secEventId | Идентификатор<br>Правило формирования:<br>Код типа события безопасности+Код наименования события безопасности+Код компонента |
| secEventType | Тип (Сокращенное наименование типа события безопасности) |
| secEventName | Наименование<br>(Сокращенное наименование события безопасности) |
| secEventSubject | Субъект доступа (По умолчанию – имя пользователя) |
| secEventLevel | Уровень важности |
| secEventHostName | Имя сервера базы данных (pg_gethostname()) |
| secEventResultOperation | Результат операции (Принимаемые значения: успешный/неуспешный) |
| secEventAdminRights | Наличие прав администратора (Принимаемые значения: да/нет) |
| secEventIp | Сетевой адрес источника входа (Формат «Сетевой адрес») |
| secEventLastInput | Дата и время последнего входа<br>(Формат «Дата и время». Указывают дату и время последней авторизации учетной записи) |
| secEventValidUntil | Срок действия учетной записи<br>(Формат "Дата/время". Указывают дату и время окончания срока действия учетной записи. Если срок действия учетной записи не ограничен, указывают значение, определяемое изготовителем средства) |
| secEventTypeAction | Тип действия (Принимаемые значения: создание/изменение/удаление) |
| secEventComponentName | Компонент ПО |
| secEventComponentDeveloper | Разработчик компонента |

| **Ключ JSON** | **Наименование** |
|---|---|
| secEventComponentType | Тип компонента |
| secEventSoftName | Наименование ПО |

## Список ключей JSON для типа события безопасности «Управление атрибутами доступа»

Первые три символа значения ключа secEventId (идентификатор события безопасности) = 105.

Таблица 5.3– Список ключей JSON для типа события безопасности «Управление атрибутами доступа»

| **Ключ JSON** | **Наименование** |
|---|---|
| timestamp | Дата и время (Формат «Дата и время») |
| user | Идентификатор учетной записи (По умолчанию – имя пользователя) |
| dbname | Имя базы данных |
| pid | Идентификатор процесса |
| remote_host | Имя компьютера клиента |
| remote_port | Порт компьютера клиента |
| session_id | Идентификатор сеанса |
| line_num | Номер строки внутри сеанса |
| ps | Тег команды |
| session_start | Время начала сессии |
| vxid | Идентификатор виртуальной транзакции |
| txid | Идентификатор транзакции |
| error_severity | Уровень важности ошибки |
| state_code | Код SQLSTATE |
| message | Сообщение об ошибке |
| Audit_type | Тип записи события |
| Statement_id | № выражения |
| Substatement_id | № подвыражения |
| Class | Класс выражения |
| Command | SQL-выражение |
| Object_type | Тип объекта БД |
| Object_name | Имя объекта БД |

| **Ключ JSON** | **Наименование** |
|---|---|
| Statement | Полный текст SQL-выражения |
| Parameter | Параметры SQL-выражения |
| application_name | Имя клиентского приложения |
| backend_type | Тип обслуживающего процесса |
| leader_pid | Идентификатор ведущего процесса группы параллельных исполнителей |
| query_id | Идентификатор запроса |
| secEventId | Идентификатор<br>Правило формирования:<br>Код типа события безопасности+Код наименования события безопасности+Код компонента |
| secEventType | Тип (Сокращенное наименование типа события безопасности) |
| secEventName | Наименование (Сокращенное наименование события безопасности) |
| secEventSubject | Субъект доступа (По умолчанию – имя пользователя) |
| secEventLevel | Уровень важности |
| secEventHostName | Имя сервера базы данных (pg_gethostname()) |
| secEventResultOperation | Результат операции (Принимаемые значения: успешный/неуспешный) |
| secEventAdminRights | Наличие прав администратора (Принимаемые значения: да/нет) |
| secEventIp | Сетевой адрес источника входа (Формат «Сетевой адрес») |
| secEventTypeAction | Тип действия (Принимаемые значения: создание/изменение/удаление/другое) |
| secEventComponentName | Компонент ПО (Краткое наименование) |
| secEventComponentDeveloper | Разработчик компонента |
| secEventComponentType | Тип компонента |
| secEventSoftName | Наименование ПО |

## Список ключей JSON для типа события безопасности «Доступ к защищаемой информации»

Первые три символа значения ключа secEventId (идентификатор события безопасности) = 106.

Таблица 5.4 – Список ключей JSON для типа события безопасности «Доступ к защищаемой информации»

| **Ключ JSON** | **Наименование** |
|---|---|
| timestamp | Дата и время (Формат «Дата и время») |
| user | Идентификатор учетной записи (По умолчанию – имя пользователя) |
| dbname | Имя базы данных |
| pid | Идентификатор процесса |
| remote_host | Имя компьютера клиента |
| remote_port | Порт компьютера клиента |
| session_id | Идентификатор сеанса |
| line_num | Номер строки внутри сеанса |
| ps | Тег команды |
| session_start | Время начала сессии |
| vxid | Идентификатор виртуальной транзакции |
| txid | Идентификатор транзакции |
| error_severity | Уровень важности ошибки |
| state_code | Код SQLSTATE |
| message | Сообщение об ошибке |
| Audit_type | Тип записи события |
| Statement_id | № выражения |
| Substatement_id | № подвыражения |
| Class | Класс выражения |
| Command | SQL-выражение |
| Object_type | Тип объекта БД |
| Object_name | Имя объекта БД |

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

| **Ключ JSON** | **Наименование** |
|---|---|
| Statement | Полный текст SQL-выражения |
| Parameter | Параметры SQL-выражения |
| application_name | Имя клиентского приложения |
| backend_type | Тип обслуживающего процесса |
| leader_pid | Идентификатор ведущего процесса группы параллельных исполнителей |
| query_id | Идентификатор запроса |
| secEventId | Идентификатор<br>Правило формирования:<br>Код типа события безопасности+Код наименования события безопасности+Код компонента |
| secEventType | Тип (Сокращенное наименование типа события безопасности) |
| secEventName | Наименование (Сокращенное наименование события безопасности) |
| secEventSubject | Субъект доступа (По умолчанию – имя пользователя) |
| secEventLevel | Уровень важности |
| secEventHostName | Имя сервера базы данных (pg_gethostname()) |
| secEventResultOperation | Результат операции (Принимаемые значения: успешный/неуспешный) |
| secEventAdminRights | Наличие прав администратора (Принимаемые значения: да/нет) |
| secEventIp | Сетевой адрес источника входа (Формат «Сетевой адрес») |
| secEventFullPath | Наименование процесса (полный путь) (Формат «Текст». Указывают полный путь) |
| secEventTypeAction | Тип действия (Принимаемые значения: изменение/удаление/другое) |
| secEventComponentName | Компонент ПО (Краткое наименование) |
| secEventComponentDeveloper | Разработчик компонента |
| secEventComponentType | Тип компонента |
| secEventSoftName | Наименование ПО |

**Список ключей JSON для типа события безопасности «Изменение параметров настроек средств защиты информации»**

Первые три символа значения ключа secEventId (идентификатор события безопасности) = 108.

Таблица 5.5 – Список ключей JSON для типа события безопасности «Изменение параметров настроек средств защиты информации»

| **Ключ JSON** | **Наименование** |
|---|---|
| timestamp | Дата и время (Формат «Дата и время») |
| user | Идентификатор учетной записи (По умолчанию – имя пользователя) |
| dbname | Имя базы данных |
| pid | Идентификатор процесса |
| remote_host | Имя компьютера клиента |
| remote_port | Порт компьютера клиента |
| session_id | Идентификатор сеанса |
| line_num | Номер строки внутри сеанса |
| ps | Тег команды |
| session_start | Время начала сессии |
| vxid | Идентификатор виртуальной транзакции |
| txid | Идентификатор транзакции |
| error_severity | Уровень важности ошибки |
| state_code | Код SQLSTATE |
| message | Сообщение об ошибке |
| Audit_type | Тип записи события |
| Statement_id | № выражения |
| Substatement_id | № подвыражения |
| Class | Класс выражения |
| Command | SQL-выражение |

| **Ключ JSON** | **Наименование** |
|---|---|
| Object_type | Тип объекта БД |
| Object_name | Имя объекта БД |
| Statement | Полный текст SQL-выражения |
| Parameter | Параметры SQL-выражения |
| application_name | Имя клиентского приложения |
| backend_type | Тип обслуживающего процесса |
| leader_pid | Идентификатор ведущего процесса группы параллельных исполнителей |
| query_id | Идентификатор запроса |
| secEventId | Идентификатор<br>Правило формирования:<br>Код типа события безопасности+Код наименования события безопасности+Код компонента |
| secEventType | Тип (Сокращенное наименование типа события безопасности) |
| secEventName | Наименование (Сокращенное наименование события безопасности) |
| secEventSubject | Субъект доступа (По умолчанию – имя пользователя) |
| secEventLevel | Уровень важности |
| secEventHostName | Имя сервера базы данных (pg_gethostname()) |
| secEventResultOperation | Результат операции (Принимаемые значения: успешный/неуспешный) |
| secEventAdminRights | Наличие прав администратора (Принимаемые значения: да/нет) |
| secEventIp | Сетевой адрес источника входа (Формат «Сетевой адрес») |
| secEventComponentName | Компонент ПО (Краткое наименование) |
| secEventComponentVersion | Версия компонента |
| secEventComponentDeveloper | Разработчик компонента |
| secEventComponentType | Тип компонента |
| secEventSoftName | Наименование ПО |
| secEventParameterNew | Новые (измененные) значения параметров конфигурации<br>(Формат "Текст". Указывают в следующем виде: "параметр: старое значение => новое значение;") |

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

**Список ключей JSON для типа события безопасности «Установка/удаление компонентов программного обеспечения»**

Первые три символа значения ключа secEventId (идентификатор события безопасности) = 110.

Таблица 5.6 - Список ключей json для типа события безопасности «Установка/удаление компонентов программного обеспечения»

| **Ключ JSON** | **Наименование** |
|---|---|
| timestamp | Дата и время<br>(Формат «Дата и время») |
| user | Идентификатор учетной записи<br>(По умолчанию – имя пользователя) |
| dbname | Имя базы данных |
| pid | Идентификатор процесса |
| remote_host | Имя компьютера клиента |
| remote_port | Порт компьютера клиента |
| session_id | Идентификатор сеанса |
| line_num | Номер строки внутри сеанса |
| ps | Тег команды |
| session_start | Время начала сессии |
| vxid | Идентификатор виртуальной транзакции |
| txid | Идентификатор транзакции |
| error_severity | Уровень важности ошибки |
| state_code | Код SQLSTATE |
| message | Сообщение об ошибке |
| Audit_type | Тип записи события |
| Statement_id | № выражения |
| Substatement_id | № подвыражения |
| Class | Класс выражения |

| **Ключ JSON** | **Наименование** |
|---|---|
| Command | SQL-выражение |
| Object_type | Тип объекта БД |
| Object_name | Имя объекта БД |
| Statement | Полный текст SQL-выражения |
| Parameter | Параметры SQL-выражения |
| application_name | Имя клиентского приложения |
| backend_type | Тип обслуживающего процесса |
| leader_pid | Идентификатор ведущего процесса группы параллельных исполнителей |
| query_id | Идентификатор запроса |
| secEventId | Идентификатор<br>Правило формирования:<br>Код типа события безопасности+Код наименования события безопасности+Код компонента |
| secEventType | Тип<br>(Сокращенное наименование типа события безопасности из таблицы "Регистрируемые события безопасности") |
| secEventName | Наименование<br>(Сокращенное наименование события безопасности из таблицы "Регистрируемые события безопасности") |
| secEventLevel | Уровень важности<br>(Уровень важности из таблицы "Регистрируемые события безопасности") |
| secEventHostName | Имя сервера базы данных (pg_gethostname()) |
| secEventResultOperation | Результат операции<br>(Принимаемые значения: успешный/неуспешный) |
| secEventFullPath | Наименование процесса (полный путь)<br>(Формат «Текст». Указывают полный путь) |
| secEventTypeAction | Тип действия<br>(Принимаемые значения: создание/изменение/удаление/чтение/запись/исполнение/установка) |

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

| **Ключ JSON** | **Наименование** |
|---|---|
| secEventComponentName | Компонент ПО<br>(Краткое наименование из таблицы "Компоненты Jatoba, по которым регистрируются события безопасности") |
| secEventComponentDeveloper | Разработчик компонента<br>(Разработчик компонента из таблицы "Компоненты Jatoba, по которым регистрируются события безопасности") |
| secEventComponentType | Тип компонента<br>(Тип компонента из таблицы "Компоненты Jatoba, по которым регистрируются события безопасности") |
| secEventSoftName | Наименование ПО<br>(Наименование ПО из таблицы "Компоненты Jatoba, по которым регистрируются события безопасности") |
| secEventComponentVersion | Версия компонента |

**Список ключей JSON для типа события безопасности «Управление запуском/остановкой компонентов программного обеспечения»**

Первые три символа значения ключа secEventId (идентификатор события безопасности) = 111.

Таблица 5.7 – Список ключей JSON для типа события безопасности «Управление запуском/остановкой компонентов программного обеспечения»

| **Ключ JSON** | **Наименование** |
|---|---|
| timestamp | Дата и время (Формат «Дата и время») |
| user | Идентификатор учетной записи (По умолчанию – имя пользователя) |
| dbname | Имя базы данных |
| pid | Идентификатор процесса |
| remote_host | Имя компьютера клиента |
| remote_port | Порт компьютера клиента |
| session_id | Идентификатор сеанса |
| line_num | Номер строки внутри сеанса |
| ps | Тег команды |
| session_start | Время начала сессии |
| vxid | Идентификатор виртуальной транзакции |
| txid | Идентификатор транзакции |
| error_severity | Уровень важности ошибки |
| state_code | Код SQLSTATE |
| message | Сообщение об ошибке |
| Audit_type | Тип записи события |
| Statement_id | № выражения |
| Substatement_id | № подвыражения |
| Class | Класс выражения |
| Command | SQL-выражение |

| **Ключ JSON** | **Наименование** |
|---|---|
| Object_type | Тип объекта БД |
| Object_name | Имя объекта БД |
| Statement | Полный текст SQL-выражения |
| Parameter | Параметры SQL-выражения |
| application_name | Имя клиентского приложения |
| backend_type | Тип обслуживающего процесса |
| leader_pid | Идентификатор ведущего процесса группы параллельных исполнителей |
| query_id | Идентификатор запроса |
| secEventId | Идентификатор<br>Правило формирования:<br>Код типа события безопасности+Код наименования события безопасности+Код компонента |
| secEventType | Тип (Сокращенное наименование типа события безопасности) |
| secEventName | Наименование (Сокращенное наименование события безопасности) |
| secEventLevel | Уровень важности |
| secEventHostName | Имя сервера базы данных (pg_gethostname()) |
| secEventResultOperation | Результат операции (Принимаемые значения: успешный/неуспешный) |
| secEventFullPath | Наименование процесса (полный путь) (Формат «Текст». Указывают полный путь) |
| secEventTypeAction | Тип действия (Принимаемые значения: останов/запуск) |
| secEventComponentName | Компонент ПО (Краткое наименование) |
| secEventComponentDeveloper | Разработчик компонента |
| secEventComponentType | Тип компонента |
| secEventSoftName | Наименование ПО |

**Список ключей JSON для типа события безопасности «Управлением журналами регистрации событий безопасности»**

Первые три символа значения ключа secEventId (идентификатор события безопасности) = 119.

Таблица 5.8 – Список ключей JSON для типа события безопасности «Управлением журналами регистрации событий безопасности»

| **Ключ JSON** | **Наименование** |
|---|---|
| timestamp | Дата и время<br>(Формат «Дата и время») |
| user | Идентификатор учетной записи<br>(По умолчанию – имя пользователя) |
| dbname | Имя базы данных |
| pid | Идентификатор процесса |
| remote_host | Имя компьютера клиента |
| remote_port | Порт компьютера клиента |
| session_id | Идентификатор сеанса |
| line_num | Номер строки внутри сеанса |
| ps | Тег команды |
| session_start | Время начала сессии |
| vxid | Идентификатор виртуальной транзакции |
| txid | Идентификатор транзакции |
| error_severity | Уровень важности ошибки |
| state_code | Код SQLSTATE |
| message | Сообщение об ошибке |
| Audit_type | Тип записи события |
| Statement_id | № выражения |
| Substatement_id | № подвыражения |

| **Ключ JSON** | **Наименование** |
|---|---|
| Class | Класс выражения |
| Command | SQL-выражение |
| Object_type | Тип объекта БД |
| Object_name | Имя объекта БД |
| Statement | Полный текст SQL-выражения |
| Parameter | Параметры SQL-выражения |
| application_name | Имя клиентского приложения |
| backend_type | Тип обслуживающего процесса |
| leader_pid | Идентификатор ведущего процесса группы параллельных исполнителей |
| query_id | Идентификатор запроса |
| secEventId | Идентификатор<br>Правило формирования:<br>Код типа события безопасности+Код наименования события безопасности+Код компонента |
| secEventType | Тип<br>(Сокращенное наименование типа события безопасности из таблицы "Регистрируемые события безопасности") |
| secEventName | Наименование<br>(Сокращенное наименование события безопасности из таблицы "Регистрируемые события безопасности") |
| secEventLevel | Уровень важности<br>(Уровень важности из таблицы "Регистрируемые события безопасности") |
| secEventHostName | Имя сервера базы данных (pg_gethostname()) |
| secEventResultOperation | Результат операции<br>(Принимаемые значения: успешный/неуспешный) |
| secEventFullPath | Наименование процесса (полный путь)<br>(Формат «Текст». Указывают полный путь) |

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

| **Ключ JSON** | **Наименование** |
|---|---|
| secEventComponentName | Компонент ПО<br>(Краткое наименование из таблицы "Компоненты Jatoba, по которым регистрируются события безопасности") |
| secEventComponentVersion | Версия компонента |
| secEventComponentDeveloper | Разработчик компонента<br>(Разработчик компонента из таблицы "Компоненты Jatoba, по которым регистрируются события безопасности") |
| secEventComponentType | Тип компонента<br>(Тип компонента из таблицы "Компоненты Jatoba, по которым регистрируются события безопасности") |
| secEventSoftName | Наименование ПО<br>(Наименование ПО из таблицы "Компоненты Jatoba, по которым регистрируются события безопасности") |
| secEventParameterNew | Новые (измененные) значения параметров конфигурации ja_seceventlog.<br>Указывается при событии 119204.<br>(Формат "Текст". Указывают в следующем виде: "параметр: старое значение => новое значение;") |
| secEventParameterAll | Значения параметров конфигурации ja_seceventlog.<br>Указывается при событиях 119204 и 119205.<br>(Формат "Текст". Указывают в следующем виде: "параметр: значение;". Если параметров несколько, то они отделяются при помощи разделителя ";") |
| secEventLogDelete | Удаленный файл журнала ja_seceventlog.<br>Указывается при событии 119193.<br>Указывается полный путь и имя файла с расширением. |
| secEventPartitionClear | Удаленная партиция таблицы ja_seceventlog.<br>Указывается при событии 119193.<br>Указывается час, за который удалена партиция. |
| secEventLogSizeLimit | Лимит объема памяти, выделенного для хранения журналов регистрации событий безопасности ja_seceventlog.<br>Указывается при событиях 119203 и 119206. |

| **Ключ JSON** | **Наименование** |
|---|---|
| | При событии 119203 (soft_limit) рассчитывается как ja_seceventlog.log_size_soft_limit * ja_seceventlog.maxsize.<br>При событии 119206 (hard_limit) рассчитывается как ja_seceventlog.log_size_hard_limit * ja_seceventlog.maxsize.<br>Указывается в kB. |
| secEventLogSize | Указывается при событиях 119203 и 119206.<br>Заполненный объем памяти, выделенного для хранения журналов регистрации событий безопасности ja_seceventlog (Общий размер всех файлов логов).<br>Указывается в kB. |

### Идентификаторы событий для компонента «ja_Dog»

События безопасности, относящиеся к компоненту «ja_Dog», записываются в журнал событий безопасности с идентификатором, где Код компонента = 103.

Таблица 5.9 – Идентификаторы событий для компонента «ja_Dog»

| Идентификатор | Текст | Примечание |
|---|---|---|
| **События безопасности, связанные с идентификацией и аутентификацией субъекта доступа** | | |
| 100100103 | Отказ во входе в связи с тем, что идентификатор не зарегистрирован | При попытке соединения, имя УЗ отсутствует в списке УЗ |
| 100101103 | Отказ во входе в связи с тем, что идентификатор заблокирован | При попытке соединения, УЗ заблокирована. |
| 100102103 | Отказ во входе в связи с неправильным паролем | При попытке соединения, пароль УЗ не соответствует |
| 100105103 | Успешный вход в систему | Успешный соединения пользователя в систему |
| 100106103 | Выход из системы | Выход пользователя |
| **События безопасности, связанные с управлением учетными записями пользователей** | | |
| 103114103 | Создание учетной записи | Создание УЗ администратора кластера |
| 103115103 | Изменение наименования учетной записи | Переименование УЗ администратора jaDog |
| 103116103 | Изменение пароля учетной записи | Изменение пароля УЗ администратора jaDog |
| 103117103 | Удаление учетной записи | |
| 103118103 | Блокирование учетной записи | |

| Идентификатор | Текст | Примечание |
|---|---|---|
| 103119103 | Активация учетной записи | |
| **События безопасности, связанные с изменением настроек общего программного обеспечения** | | |
| 120197103 | Конфигурация компонента программного обеспечения изменена | Изменение любого параметра или сброс |
| 120198103 | Компонент программного обеспечения отключен | Выключение, приостановка ja_Dog |
| 120199103 | Другие события безопасности | События с кодом 120, не подпадающие под 120197103, 120198103 события |
| **События безопасности, связанные с управлением запуском/остановкой компонентов программного обеспечения** | | |
| 111162103 | Запуск (завершение) программ и процессов (заданий, задач) | Старт ja_Dog |
| 111163103 | Запрет запуска программы | Неудачный старт сервиса или невозможность по каким либо причинам запуститься в стандартном режиме |
| **События безопасности, связанные с выполнением восстановления информации** | | |
| 114200103 | Успешная синхронизации состояния СУБД | Успешное окончание процесса rewind |
| 114201103 | Ошибка синхронизации СУБД | Неуспешное окончание процесса rewind |
| **События безопасности, связанные с управлением журналами (записями) регистрации событий безопасности** | | |
| 119193103 | Журнал очищен | Очистка журнала аудита |

**Идентификаторы событий для компонента «ja_Log»**

События безопасности, относящиеся к компоненту «ja_log», записываются в журнал событий безопасности с идентификатором, где Код компонента = 108.

Таблица 5.10 – Идентификаторы событий для компонента «ja_Log»

| **Идентификатор события безопасности** | **Тип события безопасности** | **Сокращенное наименование типа события безопасности** | **Наименование события безопасности** | **Сокращенное наименование события безопасности** | **Уровень важности** | **Пример выражения, по которому формируется событие** |
|---|---|---|---|---|---|---|
| **secEventId** | | **secEventType** | | **secEventName** | **secEventLevel** | |
| 119207108 | Управление журналами (записями) регистрации событий безопасности | УЖРСБ | Обработка журнала ja_seceventlog | УЖРСБ.9 | низкий | |
| 119208108 | Управление журналами (записями) регистрации событий безопасности | УЖРСБ | Нехватка дискового пространства при обработке журнала ja_seceventlog | УЖРСБ.10 | высокий | |
| 119195108 | Управление журналами (записями) регистрации событий безопасности | УЖРСБ | Журнал архивирован | УЖРСБ.3 | низкий | |

# ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

| | | |
|---|---|---|
| Инсталляция | – | Под термином «инсталляция» понимается отдельный сервер и (или) кластер СУБД, на котором установлена СУБД «Jatoba» с действующей лицензией. |
| Target | – | Каждая инсталляция СУБД является целью «Target». |
| Двухкомпонентная ролевая модель | – | Вид ролевой модели, в которой предустановленная ролевая модель JDS взаимодействует с ролевой моделью СУБД «Jatoba». В частности роли в JDS соотносятся одноименными групповыми ролями в целевой СУБД. |
| Snapshots | – | Снимок состояния объекта. |
| Инцидент информационной безопасности (information security incident) | | Одно или несколько нежелательных или неожиданных событий информационной безопасности, которые с высокой степенью вероятности могут привести к компрометации в бизнес-процессах и создают угрозы для информационной безопасности. (ГОСТ Р ИСО/МЭК 27000-2021). |

# ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

| | | |
|---|---|---|
| GSSAPI | – | Generic Security Services API |
| JDS | – | Jatoba Data Safe |
| LDAP | – | Lightweight Directory Access Protocol |
| PAM | – | Pluggable Authentication Modules |
| RADIUS | – | Remote Authentication in Dial-In User Service |
| SQL | – | Structured Query Language |
| SSL | – | Secure Sockets Layer |
| SSPI | – | Security Support Provider Interface |
| БД | – | База данных |
| ГИС | – | Государственная информационная система |
| ИАФ | – | Идентификация и аутентификация |
| ИСПДн | – | Информационная система персональных данных |
| КВО | – | Критически важный объект |
| КИИ | – | Критическая информационная инфраструктура |
| НСД | – | Несанкционированный доступ |
| ОДТ | – | Обеспечение доступности информации |
| ОО | – | Объект оценки |
| ОС | – | Операционная система |
| ОЦЛ | – | Обеспечение целостности |
| РСБ | – | Регистрация событий безопасности |
| СЗИ | – | Средство защиты информации |
| СУБД | – | Система управления базами данных |
| УЗ | – | Учетная запись пользователя(ей) |
| УПД | – | Управление доступом |
| ЭВМ | – | Электронно-вычислительная машина |

| Лист регистрации изменений | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Изм.** | **Номера листов (страниц)** | | | | **Всего листов (страниц) в документе** | **Номер документа** | **Входящий номер сопроводительного документа и дата** | **Подпись** | **Дата** |
| | **измененных** | **замененных** | **новых** | **аннулированных** | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

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