

# Руководство пользователя: Защита данных от привилегированных пользователей

Центр разработки PostgreSQL

Exported on 05/29/2020

## Table of Contents

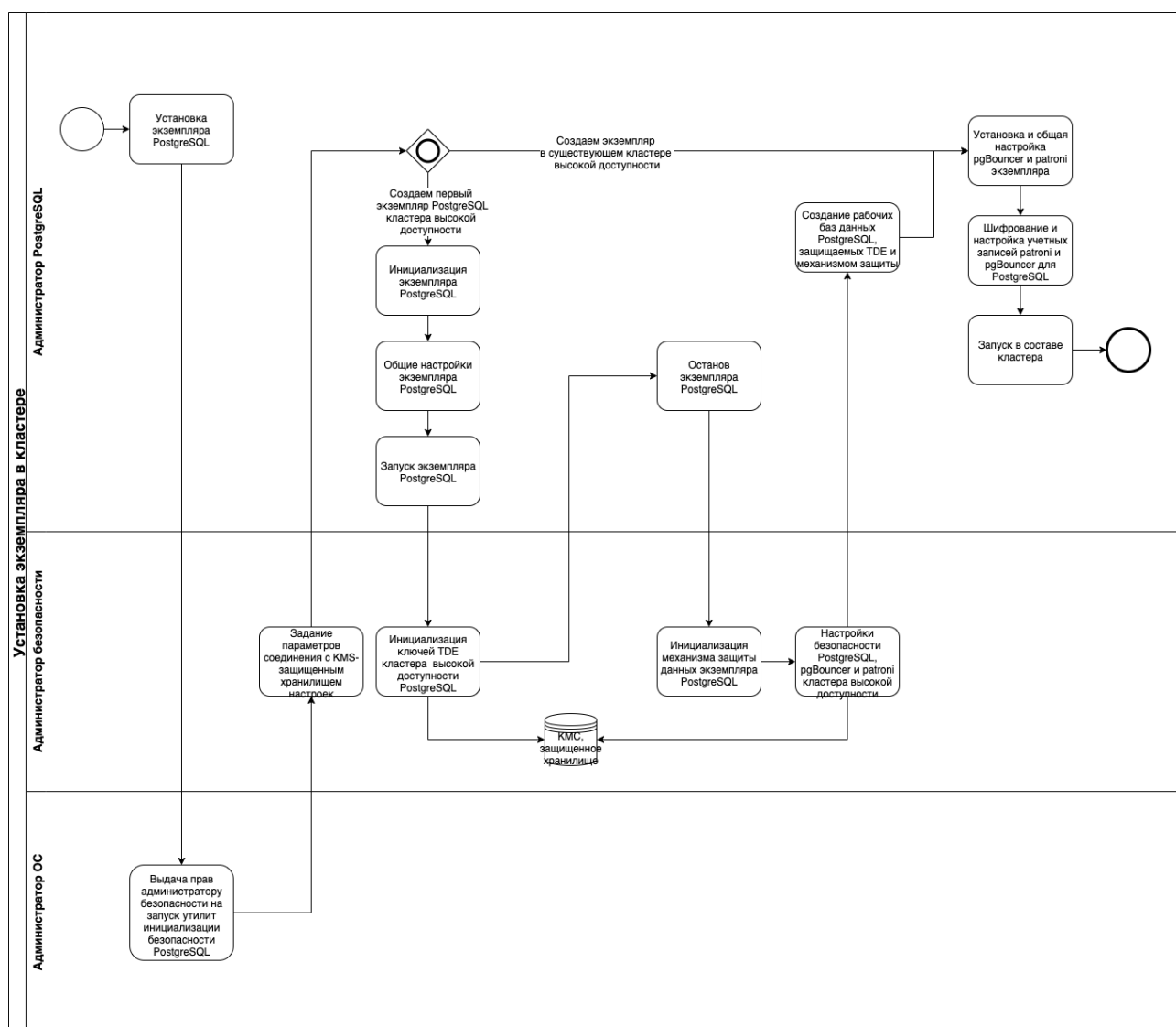
1	Руководство для сотрудника сопровождения.....	14
2	Руководство для администратора безопасности.....	16
2.1	Включение режима защищенного конфигурирования.....	17
2.2	Утилита инициализации механизма защиты данных .....	17
2.3	Функции интерфейса администратора безопасности .....	18
3	Руководство для разработчика прикладных сервисов.....	20
4	Приложения .....	21
5	1. Акторы сценариев утечки пользовательских данных.....	22
6	2. Сценарии утечки пользовательских данных.....	31

PostgreSQL Sber Edition предотвращает доступ к пользовательским данным, хранящимся в базах данных PostgreSQL, со стороны неавторизованных лиц, в том числе имеющих права:

- суперпользователя PostgreSQL, включая управление объектами баз данных, пользователями, ролями и ролями пользователей;
- администратора операционной системы, включая управление файлами, процессами, пользователями и их правами на объекты файловой системы и операционной системы;
- администратора безопасности, включая доступ к ключам шифрования Transparent Data Encryption и управление параметрами безопасности PostgreSQL;
- администратора резервного копирования, включая права на доступ к файлам резервных копий, снятие резервных копий PostgreSQL и подключение к слотам репликации PostgreSQL;

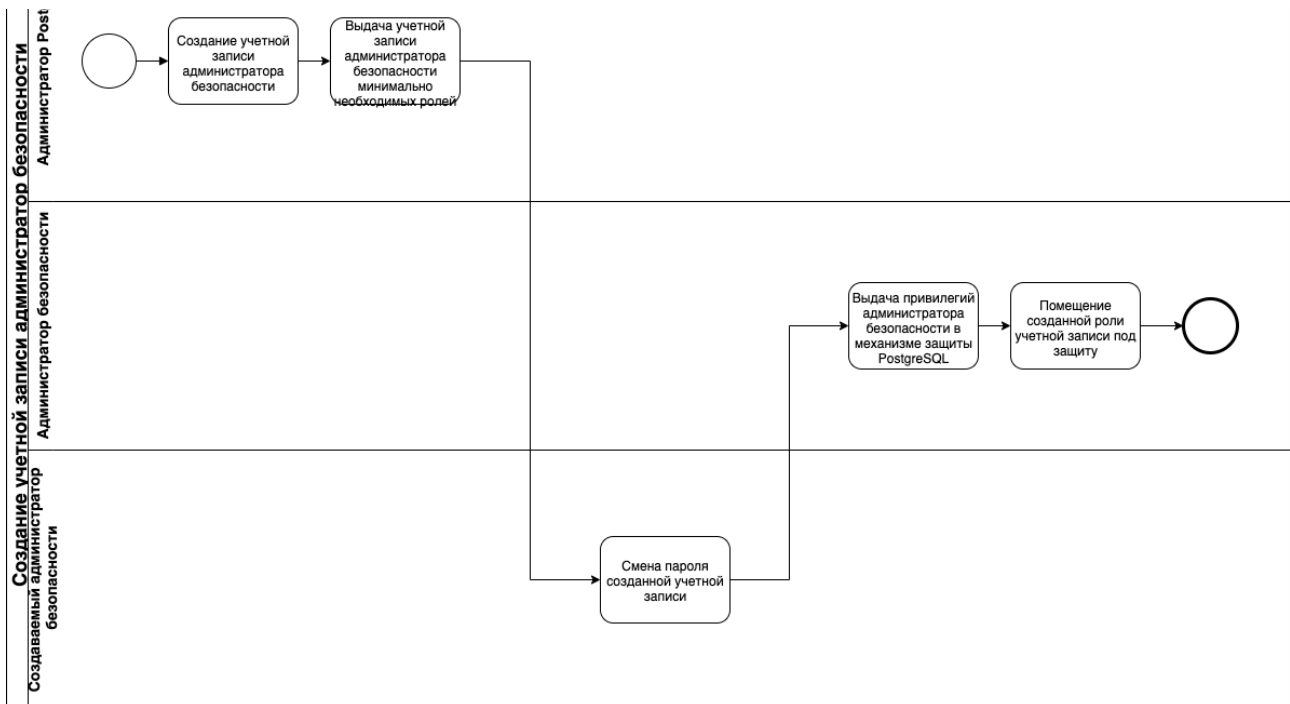
## Схемы процесса

### Создание и настройка инстанса PostgreSQL в составе кластера высокой доступности

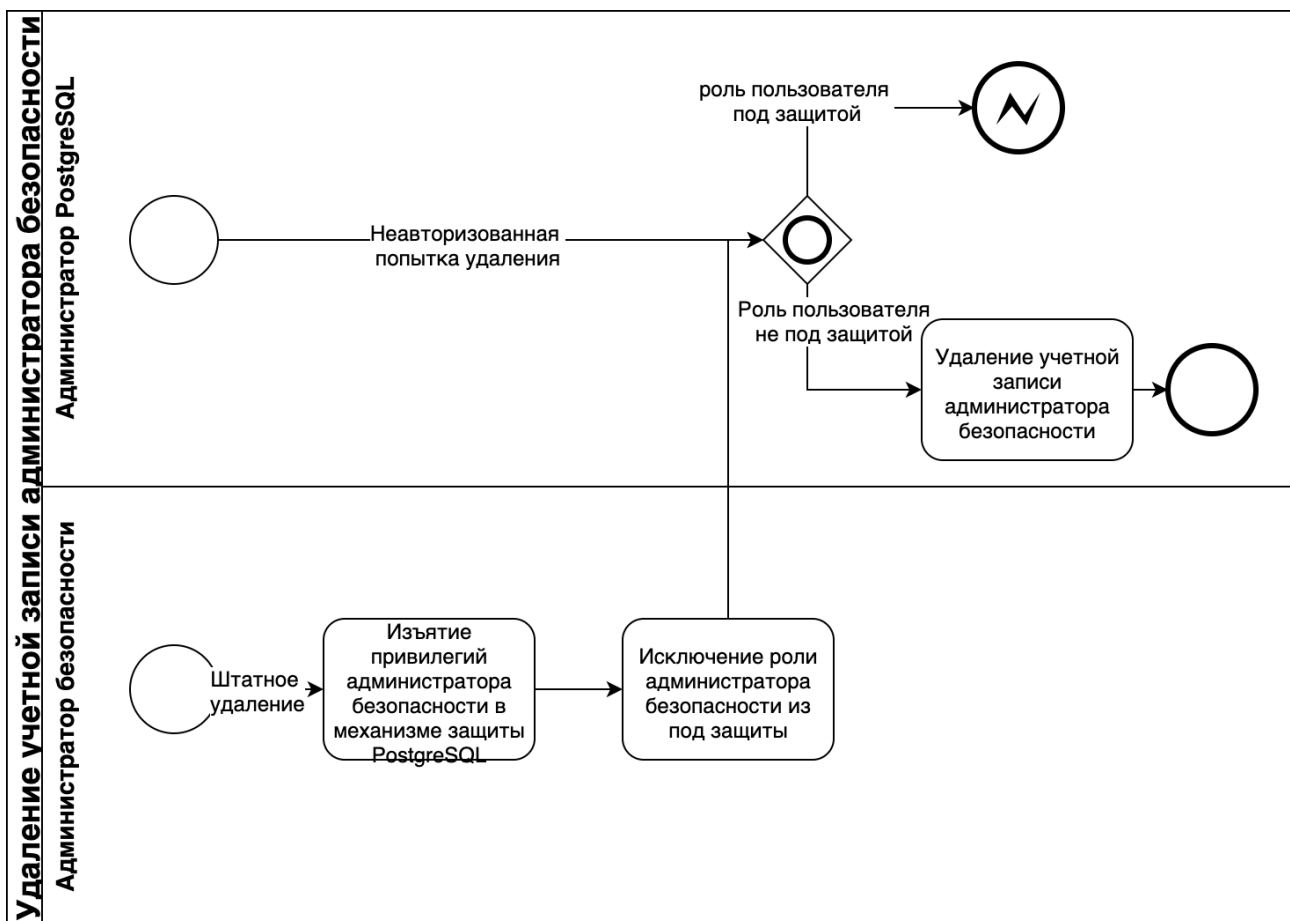


### Создание и настройка учетной записи администратора безопасности PostgreSQL





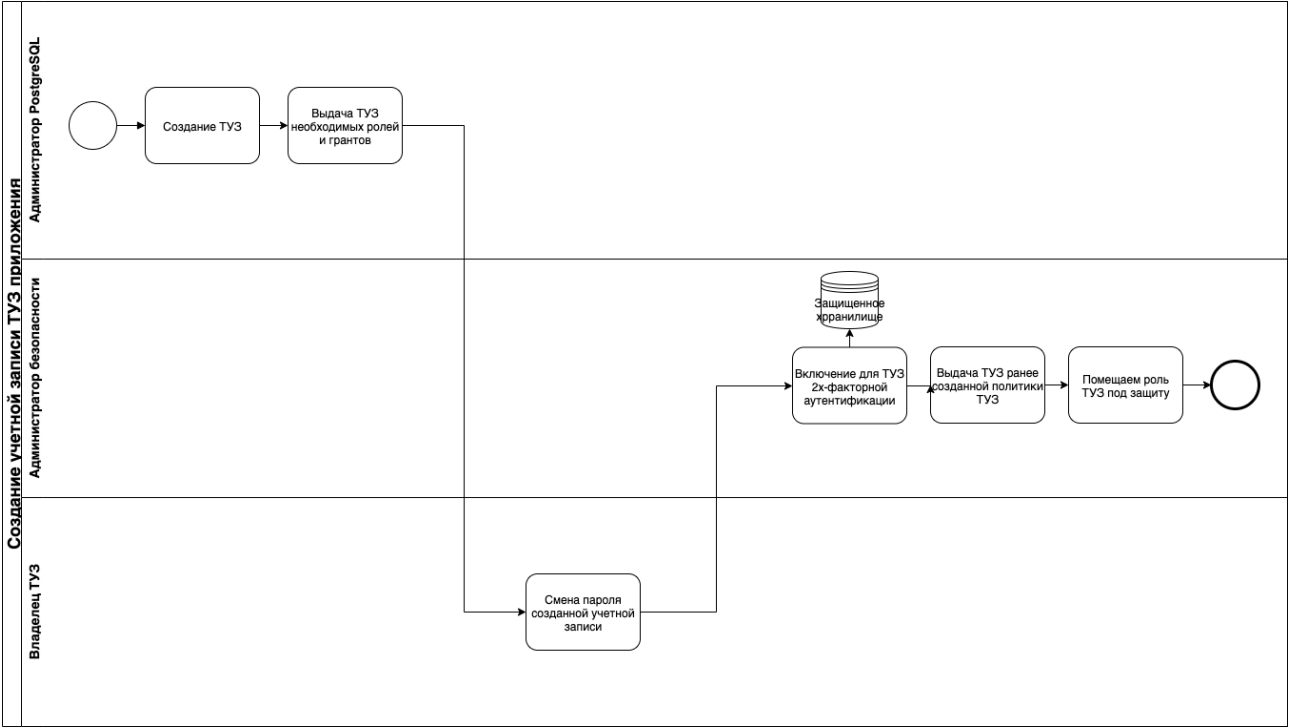
### Удаление учетной записи администратора безопасности PostgreSQL



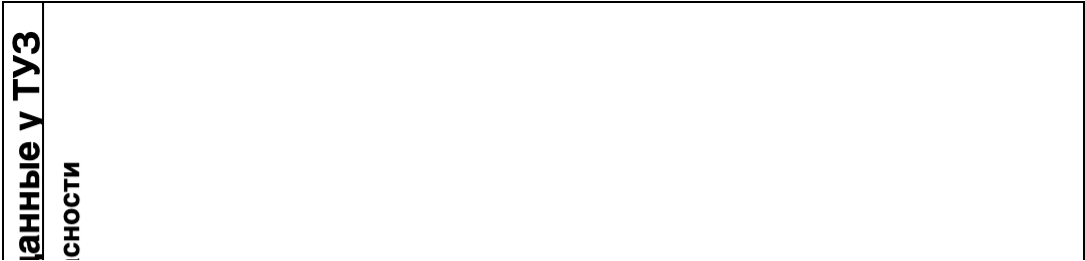
Создание политики защиты в PostgreSQL

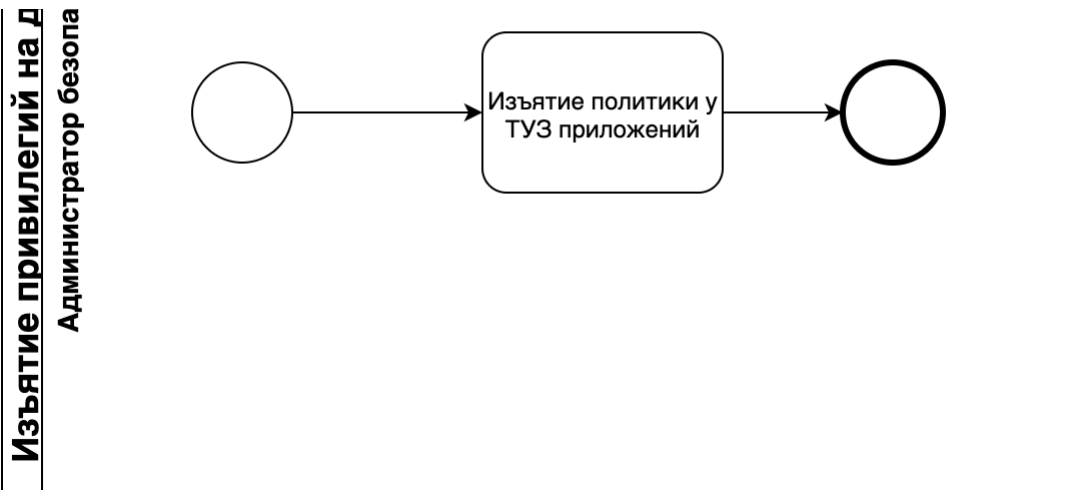


Создание и настройка учетной записи ТУЗ приложения в PostgreSQL через политику

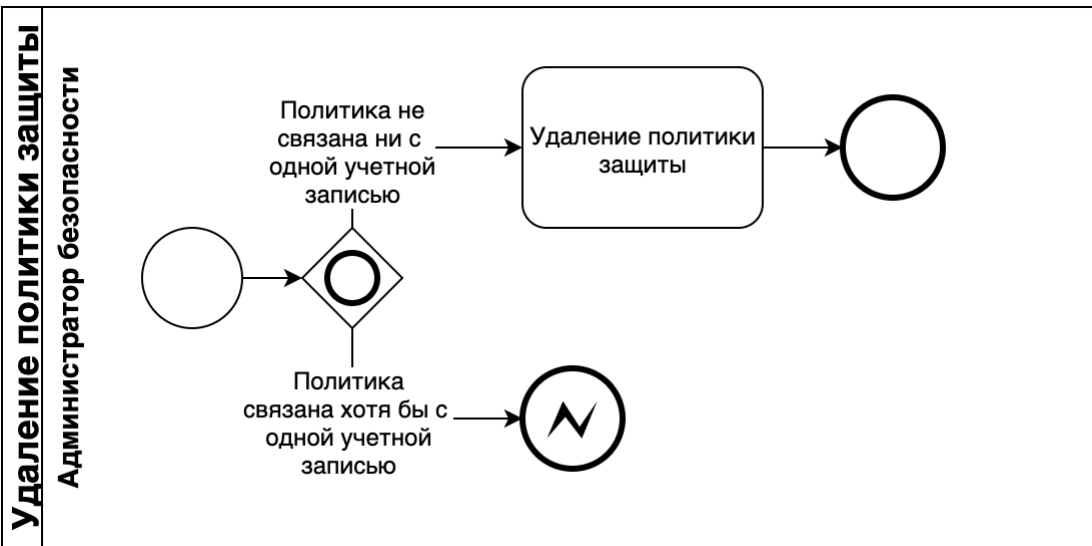


Изъятие привилегий учетной записи ТУЗ приложения, выданных через политику, в PostgreSQL

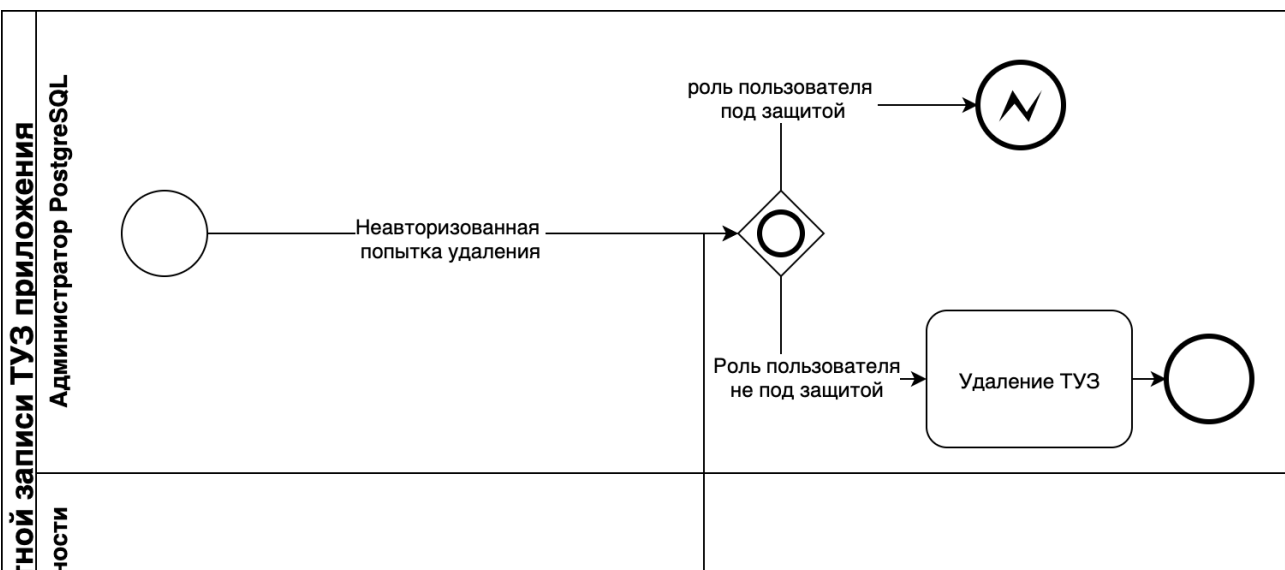


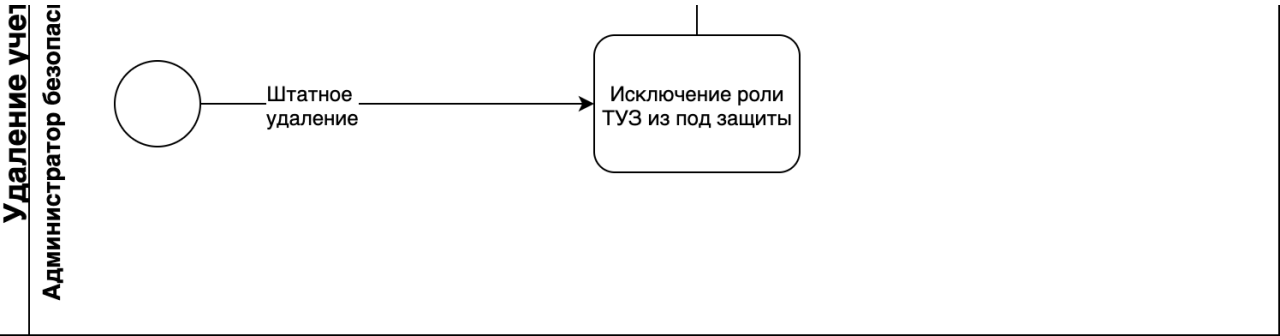


Удаление политики защиты в PostgreSQL

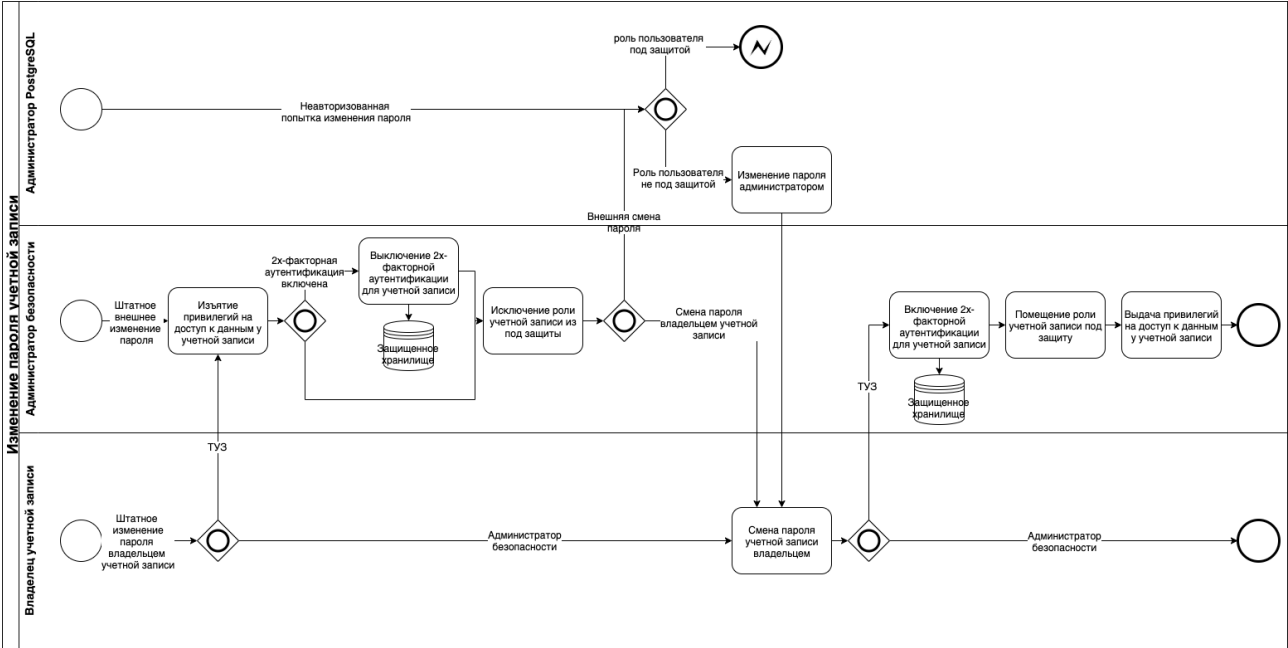


Удаление учетной записи ТУЗ приложения в PostgreSQL

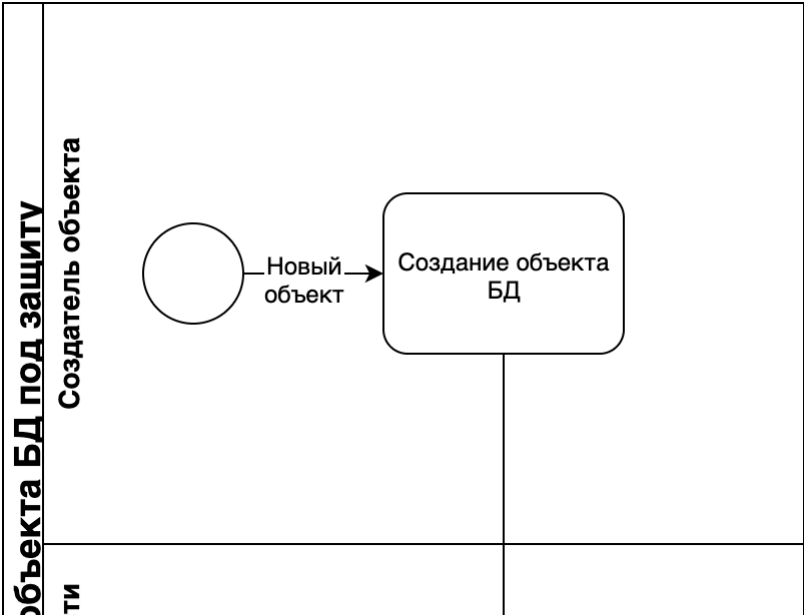


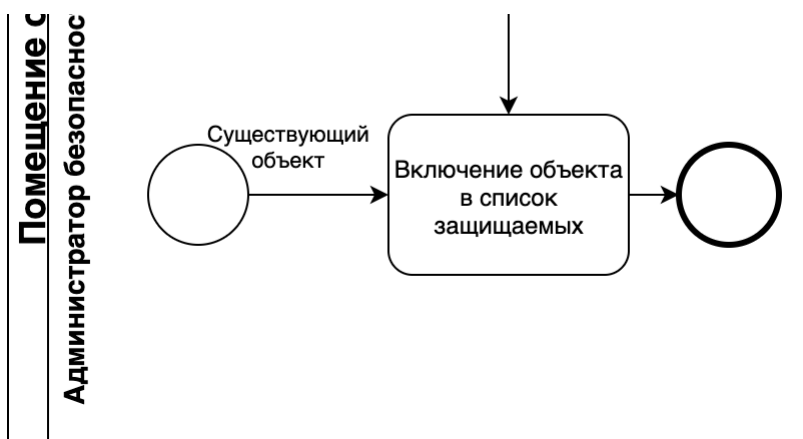


Изменение пароля защищаемой учетной записи в PostgreSQL

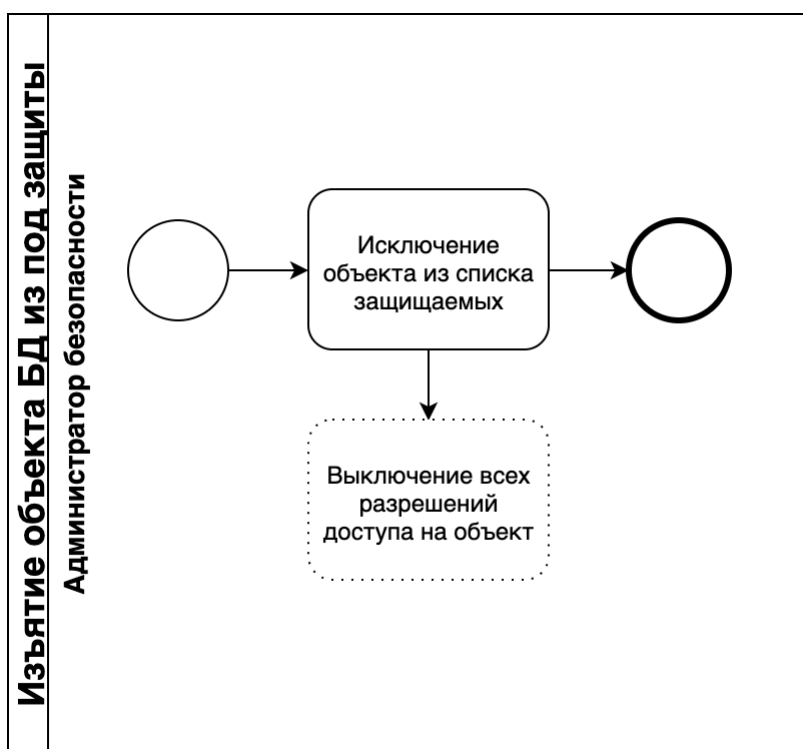


Помещение объектов БД PostgreSQL под защиту

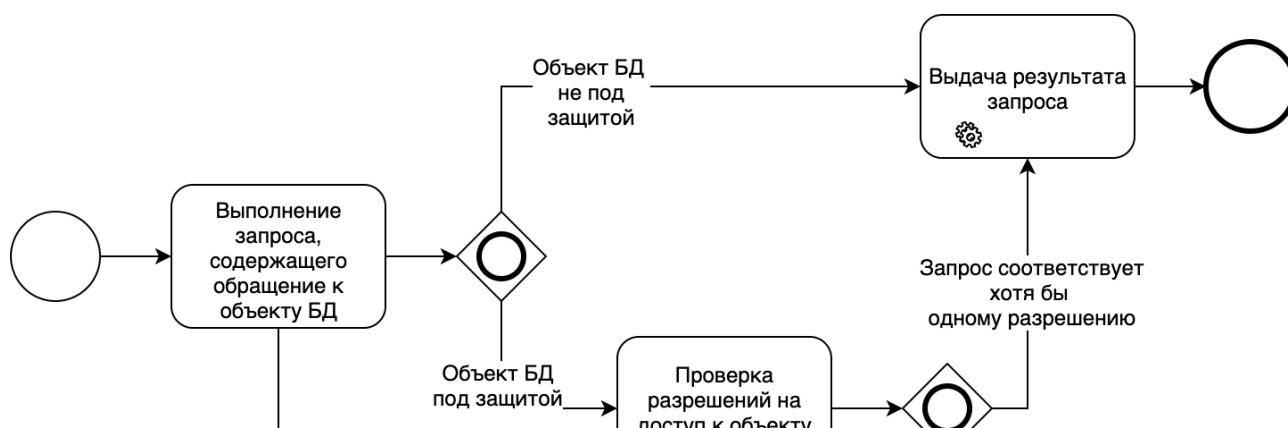




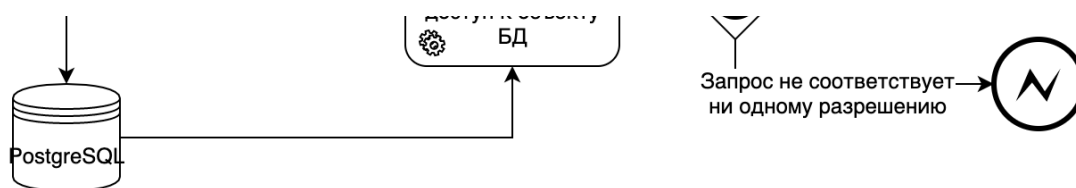
Изъятие объектов БД PostgreSQL из-под защиты



Доступ к данным, содержащимся в защищаемых объектах БД PostgreSQL







### Включение режима защищенного конфигурирования

Для предотвращения несанкционированного доступа к параметрам конфигурации компонент кластера высокой доступности - параметры либо шифруются, либо перенесены в защищенное хранилище (в текущей реализации, HashiCorp Vault).

- ❗ Параметром, управляющим включением режима защищенного конфигурирования является параметр `secure_config`, задаваемый в защищенном хранилище/KMS администратором безопасности.

### Изменения в конфигурационных файлах компонент кластера высокой доступности

- ❗ Отражены только фактические отличия от ванильной версии PostgreSQL и компонент кластера высокой доступности, присутствующие в текущей версии PostgreSQL SberEdition

Комп онент класт ера	Парам етр(ы)	Изменения	Назначение	Именован ие в защищен ном хранилище
Postgr eSQL	postgre sql.con f → passwo rd_encr yption ssl dynami c_librar y_path shared _preloa d_libra ries jit_prov ider is_secu rity_on allowe d_serve rs ssl_pas sphrase _comm and	Добавляются в защищенное хранилище, дублируются в локальном конфигурационном файле	<ul style="list-style-type: none"> <li>▪ управление способом обфускации паролей, хранимых в PostgreSQL</li> <li>▪ управление режимом использования ssl</li> <li>▪ управление составом загружаемых расширений и провайдеров</li> <li>▪ управление составом разрешенных к использованию LDAP или RADIUS серверов аутентификации</li> <li>▪ управление параметром команды, выполняемой для формирования парольной фразы ssl (позволяет выполнить сторонний код)</li> </ul>	postgresql/<ID кластера>/ postgresql/ <имя параметра>

Комп онент класт ера	Парам етр(ы)	Изменения	Назначение	Именован ие в защищен ном хранилище
Postgr eSQL	postgre sql.con f →  ssl_ca_ file ssl_cert _file ssl_crl_ file ssl_key _file ssl_cip hers ssl_pref er_serv er_ciph ers ssl_ecd h_curv e ssl_dh_ params _file	Параметры переносятся в защищенное хранилище	Управление параметрами ssl соединений	postgresql/<ID кластера>/ postgresql/ <имя параметра>
Postgr eSQL	postgre sql.con f →  local_p reload_ librarie s session _preloa d_libra ries	Игнорируются, как заданные в postgresql.conf, так и установленные через параметры роли (ALTER ROLE) или сессии (PGOPTIONS, SET)	Библиотеки расширения, загружаемые для сессии или подключения	

Комп онент класт ера	Парам етр(ы)	Изменения	Назначение	Именован ие в защищен ном хранилище
Postgr eSQL	secure_ config	Добавляется параметр в защищенное хранилище.	Параметр управляет режимом работы - с использованием параметров безопасности из защищенного хранилища или работать только с локальной конфигурацией.  Параметр действует на все компоненты данного кластера высокой доступности	postgresql/<ID кластера>/ postgresql/ secure_config
Postgr eSQL	Файл pg_hba .conf	Файл переносится в защищенное хранилище  Запрещается использование типов аутентификации trust, password, ident и peer	Настройки аутентификации и фильтрации соединений учетных записей PostgreSQL	postgresql/<ID кластера>/ postgresql/ pg_hba
Postgr eSQL	Файл pg_ide nt.conf	Файл переносится в защищенное хранилище	Настройки маппинга на учетные записи PostgreSQL для некоторых способов аутентификации	postgresql/<ID кластера>/ postgresql/ pg_ident
Postgr eSQL	Файл pgpass	При использовании libpq файл расшифровывается	Хранение логинов/паролей, используемых некоторыми утилитами для обращения к PostgreSQL	

**Механизм защиты доступа к объектам баз данных PostgreSQL, со следующими свойствами:**

Механизм защиты функционирует параллельно RBAC PostgreSQL, и управляется только администраторами безопасности.

Механизм защиты представляет **неотключаемое расширение PostgreSQL**, которое управляется дублируемыми параметрами в локальных конфигурационных файлах и защищенном хранилище.

Под защиту могут быть помещены следующие типы объектов:

- таблицы - на действия DML чтения, вставки, изменения и удаления, DDL - изменения и удаления, создания или изменения триггера по таблице, создания или изменения правила по таблице;
- партиции - на действия DML чтения, вставки, изменения и удаления, DDL - изменения и удаления;
- материализованные представления - на действия DML чтения, DDL - изменения и удаления;
- представления - на действия DML чтения, вставки, изменения и удаления, DDL - изменения и удаления, создания или изменения триггера по представлению, создания или изменения правила по представлению;
- функции - на вызов, изменение, удаление;

- роль - на действия удаления, изменения, выдачу роли-объекту, отзыв у роли-объекта, выдачу в качестве роли-объекта, отзыв в качестве роли-объекта, смену пароля, назначения текущей роли сессии;

Хранение информации для ограничения доступа выполняется в таблицах каталога безопасности. Инициализация каталога безопасности и создание учетной записи администратора безопасности выполняется утилитой инициализации каталога безопасности. Учетные записи администраторов безопасности также находятся под защитой и не могут быть изменены администратором PostgreSQL. Наделение привилегиями администратора безопасности выполняется только администраторами безопасности.

#### **Каталоги безопасности для механизма защиты данных**

- `pr_object_kind` - справочник типов защищаемых объектов;
- `pr_action` - справочник действий над защищаемыми типами объектов, регулируемых механизмом защиты;
- `pr_object` - реестр защищаемых объектов;
- `pr_policy` - реестр политик механизма защиты;
- `pr_rule` - реестр разрешений, включенных в политики;
- `pr_grant` - реестр политик, назначенных пользователям;

#### **Алгоритм наделения учетной записи правами администратора безопасности**


Предварительно администратором PostgreSQL должна быть создана роль нового пользователя - администратора безопасности, имеющая минимально необходимые права для подключения к экземпляру PostgreSQL и права на чтение из общего каталога и каталогов баз данных;

Существующий администратор безопасности:

- подключается к экземпляру PostgreSQL под своей учетной записью;
- вызывает функцию `pm_grant_security_admin`, указывая имя пользователя;

#### **Шифрование хэшей паролей и паролей в `pg_authid`**

Изменено хранение паролей и хэшей паролей пользователей в каталоге `pg_authid` - пароли и хэши паролей всегда хранятся в зашифрованном виде.

 Шифрование паролей и хэшей паролей не регулируется никакими параметрами и не отключается

# 1 Руководство для сотрудника сопровождения

Сотрудник сопровождения (Администратор PostgreSQL, Администратор ОС) участвует в процессах (см. Схемы процесса):

- Установка и настройка кластера
- Создание и настройка записи администратора безопасности PostgreSQL
- Удаление учетной записи администратора безопасности PostgreSQL
- Создание и настройка учетной записи ТУЗ приложения в PostgreSQL через политику
- Удаление учетной записи ТУЗ приложения в PostgreSQL
- Изменение пароля защищаемой учетной записи в PostgreSQL
- Помещение объектов БД PostgreSQL под защиту

## Установка и настройка кластера

- Администратор PostgreSQL производит установку ПО СУБД PostgreSQL
- Администратор ОС выдает права администратору безопасности на запуск утилит инициализации безопасности PostgreSQL
- Администратор PostgreSQL выполняет инициализацию экземпляра PostgreSQL
- Администратор PostgreSQL выполняет настройку экземпляра PostgreSQL параметрами, не относящимися к безопасности, или дублирующими параметры безопасности. Указывается идентификатор кластера в конфигурационном файле
- Администратор PostgreSQL выполняет запуск и останов экземпляра PostgreSQL
- Администратор PostgreSQL создает рабочие баз данных PostgreSQL, защищенные TDE и механизмом защиты
- Администратор PostgreSQL устанавливает и настраивает patroni и pgBouncer, задавая значения параметров, не относящихся к безопасности, или дублирующие параметры настройки безопасности
- Администратор PostgreSQL выполняет утилиту шифрования секрета, шифруя пары логин/пароль, используемые patroni и pgBouncer для подключения к PostgreSQL и внося зашифрованные пары в конфигурационные файлы patroni и pgBouncer
- Администратор PostgreSQL запускает сконфигурированные компоненты кластера высокой доступности в составе кластера

## Создание и настройка записи администратора безопасности PostgreSQL

- Администратор PostgreSQL создает учетную запись администратора безопасности в PostgreSQL, задавая логин и пароль для подключения
- Администратор PostgreSQL выдает общие права на подключение, вызов функций управления каталогом безопасности, и доступ к общему системному каталогу

## Удаление учетной записи администратора безопасности PostgreSQL

- Администратор PostgreSQL удаляет учетную запись из PostgreSQL

## Создание и настройка учетной записи ТУЗ приложения в PostgreSQL через политику

- Администратор PostgreSQL создает ТУЗ, задавая логин и пароль
- Администратор PostgreSQL выдает ТУЗ необходимые роли и гранты на доступ к объектам БД в рамках системы прав PostgreSQL

## Удаление учетной записи ТУЗ приложения в PostgreSQL

- Администратор PostgreSQL удаляет ТУЗ

## Изменение пароля защищаемой учетной записи в PostgreSQL

- Администратор PostgreSQL изменяет пароль учетной записи

## **Помещение объектов БД PostgreSQL под защиту**

- Администратор PostgreSQL создает объект в БД штатным образом

## 2 Руководство для администратора безопасности

Администратор безопасности участвует в процессах (см. Схемы процесса):

- Установка и настройка кластера
- Создание и настройка записи администратора безопасности PostgreSQL
- Удаление учетной записи администратора безопасности PostgreSQL
- Создание политики защиты в PostgreSQL
- Создание и настройка учетной записи ТУЗ приложения в PostgreSQL через политику
- Изъятие привилегий учетной записи ТУЗ приложения, выданных через политику, в PostgreSQL
- Удаление политики защиты в PostgreSQL
- Удаление учетной записи ТУЗ приложения в PostgreSQL
- Изменение пароля защищаемой учетной записи в PostgreSQL
- Помещение объектов БД PostgreSQL под защиту
- Изъятие объектов БД PostgreSQL из-под защиты

### Установка и настройка кластера

- выполняет утилиту шифрования секрета для доступа к КМС, создавая файл с шифрованным секретом
- задает мастер-ключ шифрования кластера
- выполняет утилиту инициализации каталога безопасности, задавая логин и пароль учетной записи администратора безопасности для кластера, и указывая табличное пространство для хранения каталога
- заносит в защищенное хранилище параметры компонент кластера высокой доступности, относящиеся к безопасности

### Создание и настройка записи администратора безопасности PostgreSQL

- как владелец созданной учетной записи подключается к PostgreSQL с заданными администратором PostgreSQL логином и паролем и производит замену пароля на новый, известный только ему
- как не владелец создаваемой записи производит создание и назначение политик защиты данных, разрешающих доступ к роли и к функциям администратора безопасности для создаваемой роли администратора безопасности
- как не владелец создаваемой записи производит помещение объекта БД - роли создаваемого администратора безопасности, под защиту механизма защиты данных

### Удаление учетной записи администратора безопасности PostgreSQL

- изымает привилегии администратора безопасности у удаляемой учетной записи
- исключает роль удаляемой учетной записи из-под защиты

### Создание политики защиты в PostgreSQL

- создает политику защиты в каталоге безопасности
- наполняет созданную политику разрешениями на действия над защищаемыми объектами БД

### Создание и настройка учетной записи ТУЗ приложения в PostgreSQL через политику

- указывает необходимость 2х-факторной аутентификации для ТУЗ в pg\_hba.conf в защищенном хранилище.
- назначает ТУЗ ранее созданную политику с разрешениями для ТУЗ приложения
- помещает объект роли ТУЗ под защиту механизма защиты данных

### Изъятие привилегий учетной записи ТУЗ приложения, выданных через политику, в PostgreSQL

- снимает с ТУЗ указанную назначенную политику механизма защиты данных



### Удаление политики защиты в PostgreSQL

- удаляет указанную политику механизма защиты данных

### Удаление учетной записи ТУЗ приложения в PostgreSQL

- исключает роль удаляемой ТУЗ из под защиты механизма защиты данных

### Изменение пароля защищаемой учетной записи в PostgreSQL

- снимает политики, дающие учетной записи доступ к защищаемым данным
- изменяет `pg_hba.conf` в защищенном хранилище, отключая требование 2х-факторной аутентификации для учетной записи
- исключает роль учетной записи из под защиты механизма защиты данных
- изменяет `pg_hba.conf` в защищенном хранилище, включая требование 2х-факторной аутентификации для учетной записи
- помещает роль учетной записи под защиту механизма защиты данных
- назначает политики, дающие учетной записи доступ к защищаемым данным

### Помещение объектов БД PostgreSQL под защиту


- включает объект в каталог безопасности как защищаемый механизмом защиты данных

### Изъятие объектов БД PostgreSQL из-под защиты


- исключает объект БД из каталога безопасности как защищаемый механизмом защиты объект

## 2.1 Включение режима защищенного конфигурирования

Для предотвращения несанкционированного доступа к параметрам конфигурации компонент кластера высокой доступности - параметры либо шифруются, либо перенесены в защищенное хранилище (в текущей реализации, HashiCorp Vault).

-  Параметром, управляющим включением режима защищенного конфигурирования является параметр `secure_config`, задаваемый в защищенном хранилище/KMS администратором безопасности.

Для включения режима защищенного конфигурирования администратором безопасности должна быть выполнена настройка подключения к защищенному хранилищу с помощью утилиты `setup_kms_credentials`, аналогично такому для Transparent Data Encryption.

-  Защищенное конфигурирование и Transparent Data Encryption используют оно и то же подключение к защищенному хранилищу/KMS. При необходимости использовать и то и другое - повторная настройка подключения не требуется.

## 2.2 Утилита инициализации механизма защиты данных

Утилита инициализации механизма защиты данных должна выполняться администратором безопасности на первом из серверов кластера высокой доступности до установки и запуска `patroni`.

Patroni должен устанавливаться и настраиваться поверх существующего экземпляра PostgreSQL и не должен выполнять переинициализацию экземпляра PostgreSQL.

Утилита инициализации каталога безопасности принимает на вход следующие параметры:

- путь к директории PGDATA базы данных - ключом параметра командной строки -D, --pgdata=;
- логин администратора безопасности - ключом параметра командной строки -U, --username=;
- пароль администратора безопасности - запросом у пользователя;

Утилита инициализации каталога безопасности выполняет следующие действия:

- при запуске утилиты для экземпляра PostgreSQL с ранее инициализированным каталогом безопасности утилита выводит сообщение о том, что каталог безопасности находится не в ожидаемом состоянии;
- запрашивает пароль создаваемого администратора безопасности для ввода пользователем с консоли;

**i** Прием параметра пароля администратора безопасности в переменной окружения или параметрах вызова утилиты запрещен в целях безопасности

- заполняет таблицы каталога безопасности согласно п. "Модель данных каталога безопасности для механизма защиты данных";
- создает роль пользователя администратора безопасности с указанными логином и паролем, выдает ему права на чтение из общего каталога и из каталогов баз данных;
- создает функции интерфейса администратора безопасности;
- включает в защищаемые объекты роль администратора безопасности;
- включает в защищаемые объекты таблицы каталога безопасности;
- включает в защищаемые объекты функции интерфейса администратора безопасности;
- создает политику для доступа к роли администратора безопасности с именем adminPolicyOwner\_<имя роли созданного администратор безопасности>, включающую права на смену пароля;
- создает политику для доступа к таблицам каталога безопасности с именем securityCatalogAdmin, включающую права на вставку, чтение, изменение данных в таблице и удаление из таблицы;
- создает политику доступа к функциям интерфейса администратора безопасности securityFunctionsAdmin, включающее права на вызов функций;
- назначает все созданные политики созданной роли администратора безопасности;

**i** После включения механизма защиты загрузка дополнительных расширений через команду LOAD становится недоступна.

## 2.3 Функции интерфейса администратора безопасности

- `pg_get_protected_objects()`, без параметров - возвращает список объектов, находящихся под защитой;
- `pg_protect_object`(имя базы данных, типа объекта, наименование объекта) - помещает объект под защиту;
- `pg_unprotect_object`(имя базы данных, типа объекта, наименование объекта) - снимает защиту с объекта;
- `pg_make_policy`(имя политики) - создает политику;
- `pg_grant_to_policy`(имя политики, имя базы данных, типа объекта, наименование объекта, массив действий над объектом) - вносит в политику разрешение на действия над объектом;
- `pg_revoke_from_policy`(имя политики, имя базы данных, типа объекта, наименование объекта, массив действий над объектом) - исключает из политики разрешения на действия над объектом;
- `pg_assign_policy_to_user`(имя пользователя, имя политики) - назначает политику пользователю;
- `pg_unassign_policy_from_user`(имя пользователя, имя политики) - изымает политику у пользователя;

- `pm_get_assigned_policies`(имя пользователя) - получает список политик, назначенных пользователю;
- `pm_get_policy_grants`(имя политики) - получает список разрешений в составе политики;
- `pm_get_policies`() - получает список политик;
- `pm_grant_security_admin`(имя пользователя) - делает пользователя администратором безопасности;
- `pm_revoke_security_admin`(имя пользователя) - снимает с пользователя политики администратора безопасности;

### 3 Руководство для разработчика прикладных сервисов

Реализованная функциональность не содержит инструкций для разработчика прикладных сервисов.

## 4 Приложения

## 5 1. Акторы сценариев утечки пользовательских данных

Актор	Назначение и особенности
<b>администратор PostgreSQL</b>	<ul style="list-style-type: none"> <li>• общее администрирование инстансов PostgreSQL, за исключением аспектов безопасности</li> <li>• управление учетными записями пользователей</li> <li>• создание/удаление/изменение ролей PostgreSQL</li> <li>• управление ролями пользователей</li> <li>• имеет права superuser в PostgreSQL, т.е. не имеет ограничений на выполняемые действия в рамках RBAC PostgreSQL</li> <li>• не имеет доступа к защищаемым создаваемым механизмом защиты данным и объектам</li> </ul>
<b>администратор ОС</b>	<ul style="list-style-type: none"> <li>• администрирование серверов, файловых систем и ОС</li> <li>• имеет полный доступ к файлам и процессам со стороны ОС</li> <li>• выдает права на доступ к ФС и ОС</li> </ul>
<b>администратор бэкапирования</b>	<ul style="list-style-type: none"> <li>• выполнение бэкапирования баз данных</li> <li>• имеет доступ на чтение к файлам БД</li> <li>• управление бэкапами</li> <li>• имеет доступ к бэкапам БД PostgreSQL</li> <li>• имеет права на выполнение процедур бэкапа, включая создание слота репликации и инициализацию получения WAL по каналам репликации</li> <li>• не имеет доступа к защищаемым создаваемым механизмом защиты данным и объектам</li> </ul>
<b>администратор безопасности</b>	<ul style="list-style-type: none"> <li>• управление параметрами инстансов PostgreSQL, относящимися к безопасности (аудит, парольные политики, механизм ограничения, ssl)</li> <li>• управление разрешениями механизма ограничения действий, в частности - разрешениями на доступ к пользовательским данным</li> <li>• управление параметрами pg_hba.conf</li> <li>• управление параметрами HA кластера, относящимися к безопасности</li> <li>• управление параметрами TDE</li> <li>• не имеет прав на выполнение каких-либо действий над любыми объектами, кроме функций управления механизмом защиты данных и объектов</li> </ul>
<b>администратор приложения</b>	<ul style="list-style-type: none"> <li>• управление схемами приложений</li> <li>• не имеет доступа к защищаемым создаваемым механизмом защиты данным и объектам</li> </ul>
<b>ТУЗ мониторинга</b>	<ul style="list-style-type: none"> <li>• получение метрик по системному каталогу PostgreSQL</li> <li>• снятие метрик серверов и ОС</li> <li>• не имеет доступа к защищаемым создаваемым механизмом защиты данным и объектам</li> </ul>

Актор	Назначение и особенности
ТУЗ приложений	<ul style="list-style-type: none"> <li>• доступ к пользовательским данным</li> <li>• выполнение функций приложения</li> </ul>

Привилегии и ограничения указаны для состояния "как должно быть"

Разрешено	Запрещено	Совместно с другой ролью

[illegible]











[illegible]

[illegible]

## 6 2. Сценарии утечки пользовательских данных

Сценарий	Участники	Действия	Контрмеры
Раскрытие данных в файлах БД PostgreSQL	Администратор ОС, Администратор PostgreSQL или Администратор бэкапирования	<ul style="list-style-type: none"> <li>Чтение данных из незашифрованных файлов данных, WAL, временных файлов PostgreSQL, или аналогичных файлов бэкапов</li> </ul>	Transparent Data Encryption
	Администратор ОС или Администратор PostgreSQL	<ul style="list-style-type: none"> <li>Раскрытие параметров подключения к KMS</li> <li>Извлечение мастер-ключа шифрования из KMS</li> <li>Расшифровка ключей шифрования из keyring</li> <li>Расшифровка и чтение данных из зашифрованных файлов данных, WAL и временных файлов PostgreSQL</li> </ul>	Шифрование параметров соединения с KMS
	Администратор безопасности	<ul style="list-style-type: none"> <li>Получение ключей шифрования из KMS</li> <li>Расшифровка и чтение файлов данных PostgreSQL с помощью полученных ключей</li> </ul>	Отсутствие у администратора безопасности доступа к файлам данных PostgreSQL
Запрос данных из защищаемых таблиц, партиций, материал изованных представлений и индексов БД PostgreSQL через интерфейс с запросов PostgreSQL	Администратор ОС	<ul style="list-style-type: none"> <li>Получение информации о логине ТУЗ приложений</li> <li>Изменение информации в pg_hba.conf, использование trust, password, ident или peer типа аутентификации. Или же в pg_ident.conf, для представления со своими credentials другим пользователем</li> <li>Получение доступа к БД PostgreSQL как авторизованного на чтение данных пользователя</li> </ul>	<ul style="list-style-type: none"> <li>Запрет типа аутентификации trust, password, ident или peer в коде PostgreSQL</li> <li>и</li> <li>Хранение pg_hba.conf и pg_ident.conf в защищенном хранилище</li> </ul>
	Администратор ОС или администратор безопасности	<ul style="list-style-type: none"> <li>Получение credentials Администратора PostgreSQL из конфигурации patroni или pgBouncer</li> <li>Выполнение атак, доступных для Администратора PostgreSQL</li> </ul>	Хранение credentials patroni и pgBouncer в зашифрованном виде

Сценарий	Участники	Действия	Контрмеры
	Администратор ОС или администратор безопасности	<ul style="list-style-type: none"> <li>Получение credentials Администратора PostgreSQL или администратора бэкапирования из формируемого patroni файла .pgpass</li> <li>Выполнение атак, доступных для Администратора PostgreSQL или администратора бэкапирования</li> </ul>	Формирование и хранение credentials в .pgpass в зашифрованном виде
	Администратор ОС	<ul style="list-style-type: none"> <li>Получение информации о логине ТУЗ приложений</li> <li>Установка и настройка собственного Directory Server/ RADIUS сервера/Kerberos сервера, занесение в него записи для ТУЗ с известным паролем</li> <li>Изменение информации в pg_hba.conf, указание для логина ТУЗ аутентификации LDAP/ RADIUS/Kerberos на поддельном Directory Server</li> <li>Получение доступа к БД PostgreSQL как авторизованного на чтение данных пользователя</li> </ul>	<ul style="list-style-type: none"> <li>Верификация LDAP/ RADIUS/Kerberos серверов по списку из защищенного хранилища</li> </ul> <p>или</p> <ul style="list-style-type: none"> <li>Хранение pg_hba.conf в защищенном хранилище</li> </ul>
	Администратор ОС, Администратор PostgreSQL или администратор безопасности	<ul style="list-style-type: none"> <li>Получение информации о credentials пользователей из файла userlist pgBouncer</li> <li>Получение доступа к БД PostgreSQL как авторизованного на чтение данных пользователя</li> </ul>	Запрет хранения паролей в userlist на pgBouncer, аутентификация выполняется только по данным в PostgreSQL
	Администратор ОС или Администратор PostgreSQL	<ul style="list-style-type: none"> <li>подмена pg_hba.conf для pgBouncer записями с уровнем trust, password, ident или peer для аутентификации без пароля</li> <li>Получение доступа к БД PostgreSQL как авторизованного на чтение данных пользователя</li> </ul>	запрет использования trust, password, ident или peer аутентификации в pgBouncer



Сценарий	Участники	Действия	Контрмеры
	Администратор PostgreSQL	<ul style="list-style-type: none"> <li>Получение прав администратора безопасности через выдачу соответствующих ролей или иных квалифицирующих признаков администратора безопасности</li> <li>Снятие защиты с защищаемых объектов БД PostgreSQL</li> <li>Запрос данных из защищаемых объектов БД PostgreSQL через интерфейс запросов PostgreSQL</li> </ul>	Запрет выдачи ролей или иных квалифицирующих признаков администратора безопасности пользователям всем, кроме администраторов безопасности
	Администратор PostgreSQL	<ul style="list-style-type: none"> <li>Получение прав администратора безопасности через выдачу соответствующих ролей или иных квалифицирующих признаков администратора безопасности</li> <li>Выдача привилегий на чтение из защищаемых объектов БД PostgreSQL самому себе</li> <li>Запрос данных из защищаемых объектов БД PostgreSQL через интерфейс запросов PostgreSQL</li> </ul>	Запрет выдачи ролей или иных квалифицирующих признаков администратора безопасности пользователям всем, кроме администраторов безопасности
	Администратор PostgreSQL	<ul style="list-style-type: none"> <li>Получение credentials администратора безопасности через выполнение, создаваемой в рамках работ, утилиты инициализации механизма защиты данных при создании БД</li> <li>Выдача привилегий на чтение из защищаемых объектов БД PostgreSQL самому себе</li> <li>Запрос данных из защищаемых объектов БД PostgreSQL через интерфейс запросов PostgreSQL</li> </ul>	Административный запрет администратору PostgreSQL на выполнение инициализации механизма защиты данных. Дополнительно, включение в создаваемую в рамках работ утилиту инициализации механизма защиты данных запрета повторной инициализации, для возможности контроля ранее проведенных инициализаций
	Администратор PostgreSQL	<ul style="list-style-type: none"> <li>Снятие или ослабление проверок путем модификации политик доступа к объектам PostgreSQL</li> <li>Запрос данных из защищаемых объектов БД PostgreSQL через интерфейс запросов PostgreSQL</li> </ul>	Запрет на управление политиками доступа к пользовательским данным для пользователей без ролей или иных квалифицирующих признаков администратора безопасности

Сценарий	Участники	Действия	Контрмеры
	Администратор PostgreSQL	<ul style="list-style-type: none"> <li>Прямое выключение механизма защиты объектов PostgreSQL через удаление его из конфигурации, изменение списка загружаемых расширений для сессии или подключения, или отключения расширения</li> <li>Запрос данных из защищаемых объектов БД PostgreSQL через интерфейс запросов PostgreSQL</li> </ul>	<ul style="list-style-type: none"> <li>Безусловная загрузка расширений поддержки безопасности при запуске PostgreSQL</li> </ul> <p>и</p> <ul style="list-style-type: none"> <li>запрет установки списка расширений для сессии или подключения</li> </ul> <p>и</p> <ul style="list-style-type: none"> <li>Получение списка подгружаемых расширений из защищенного хранилища</li> </ul>
	Администратор PostgreSQL	<ul style="list-style-type: none"> <li>Подмена обработчиков механизма защиты объектов PostgreSQL через загрузку расширения-заглушки, не выполняющую проверки</li> <li>Запрос данных из защищаемых объектов БД PostgreSQL через интерфейс запросов PostgreSQL</li> </ul>	Запрет на загрузку расширений командами в PostgreSQL, только автоматическая загрузка по заранее составленному перечню, хранимому в защищенном хранилище
	Администратор PostgreSQL	<ul style="list-style-type: none"> <li>Понижение уровня механизма защиты через параметры настройки PostgreSQL (например, <code>sergsql.permissive</code>)</li> <li>Запрос данных из защищаемых объектов БД PostgreSQL через интерфейс запросов PostgreSQL</li> </ul>	<ul style="list-style-type: none"> <li>Отключение параметров, понижающих степень защиты</li> </ul> <p>или</p> <ul style="list-style-type: none"> <li>Перенос параметров, понижающих степень защиты, в защищенное хранилище</li> </ul>

Сценарий	Участники	Действия	Контрмеры
	Администратор PostgreSQL	<ul style="list-style-type: none"> <li>Создание роли ТУЗ приложения с заданным паролем</li> <li>Ожидание выдачи администратором безопасности прав на работу с защищаемыми данными роли ТУЗ приложения</li> <li>Запрос данных из защищаемых объектов БД PostgreSQL через интерфейс запросов PostgreSQL</li> </ul>	<ul style="list-style-type: none"> <li>Смена пароля ТУЗ приложения владельцем ТУЗ или неким приложением автоматически, после создания</li> </ul> <p>или</p> <ul style="list-style-type: none"> <li>Реализация поддержки двухфакторной аутентификации на PostgreSQL, при которой второй фактор аутентификации для ТУЗ приложения формируется администратором безопасности или автоматически</li> </ul> <p>или</p> <ul style="list-style-type: none"> <li>Администратор безопасности задает ограничение на адреса, с которых может подключаться ТУЗ приложения, в pg_hba.conf в защищенном хранилище. Администратор PostgreSQL не имеет доступа к серверам с адресами, с которых возможен коннект для учетной записи ТУЗ</li> </ul>

Сценарий	Участники	Действия	Контрмеры
	Администратор PostgreSQL	<ul style="list-style-type: none"> <li>Смена текущей роли сессии через инструкции SET ROLE или SET SESSION   LOCAL AUTHORIZATION, либо же через переменные окружения при запуске подключения к БД, на роль пользователя, имеющего доступ к пользовательским данным или роль администратора безопасности</li> <li>Запрос данных из защищаемых объектов БД PostgreSQL через интерфейс запросов PostgreSQL или наделение правами доступа к данным других учетных записей</li> </ul>	Запрет на смену роли в рамках сессии на защищаемые механизм защиты роли
	Администратор безопасности	<ul style="list-style-type: none"> <li>Понижение уровня механизма защиты через параметры настройки PostgreSQL (например, <code>sergsql.permissive</code>)</li> <li>Запрос данных из защищаемых объектов БД PostgreSQL через интерфейс запросов PostgreSQL</li> </ul>	<ul style="list-style-type: none"> <li>Отсутствие у администратора безопасности возможности перезапуска PostgreSQL</li> </ul> <p>и</p> <ul style="list-style-type: none"> <li>Отключение параметров, понижающих степень защиты</li> </ul> <p>или</p> <ul style="list-style-type: none"> <li>Сверка локальных параметров, относящихся к безопасности, с таковыми в защищенном хранилище при перезапуске PostgreSQL. При несовпадении выдается ошибка</li> </ul>

Сценарий	Участники	Действия	Контрмеры
	Администратор безопасности	<ul style="list-style-type: none"> <li>• Прямое выключение механизма защиты объектов PostgreSQL через удаление его из конфигурации, изменение списка загружаемых расширений для сессии или подключения, или отключения расширения</li> <li>• Запрос данных из защищаемых объектов БД PostgreSQL через интерфейс запросов PostgreSQL</li> </ul>	<ul style="list-style-type: none"> <li>• Безусловная загрузка расширений поддержки безопасности при запуске PostgreSQL</li> </ul> <p>и</p> <ul style="list-style-type: none"> <li>• запрет установки списка расширений для сессии или подключения</li> </ul> <p>и</p> <ul style="list-style-type: none"> <li>• Сверка списка загружаемых расширений из локальных настроек PostgreSQL со списком из защищенного хранилища при запуске PostgreSQL. При несовпадении выдается ошибка</li> </ul>
	Администратор безопасности	<ul style="list-style-type: none"> <li>• Снятие или ослабление проверок путем модификации политик доступа к объектам PostgreSQL</li> <li>• Запрос данных из защищаемых объектов БД PostgreSQL через интерфейс запросов PostgreSQL</li> </ul>	<ul style="list-style-type: none"> <li>▪ Отсутствие у учетных записей администраторов безопасности прав на обращение к защищаемым объектам PostgreSQL.</li> </ul> <p>и</p> <ul style="list-style-type: none"> <li>▪ Отсутствие у учетных записей администраторов безопасности прав на изменение привилегий в стандартной системе привилегий PostgreSQL</li> </ul>

Сценарий	Участники	Действия	Контрмеры
	Администратор безопасности	<ul style="list-style-type: none"> <li>Получение информации о логине ТУЗ приложений</li> <li>Установка и настройка собственного Directory Server/ RADIUS сервера/Kerberos сервера, занесение в него записи для ТУЗ с известным паролем</li> <li>Изменение информации в pg_hba.conf в защищенном хранилище, указание для логина ТУЗ аутентификации LDAP/ RADIUS/Kerberos на поддельном Directory Server</li> <li>Получение доступа к БД PostgreSQL как авторизованного на чтение данных пользователя</li> </ul>	<ul style="list-style-type: none"> <li>Верификация LDAP/ RADIUS/Kerberos серверов по списку из защищенного хранилища</li> </ul> <p>и</p> <ul style="list-style-type: none"> <li>Сверка списка разрешенных LDAP/ RADIUS/Kerberos серверов с аналогичным локальным списком экземпляра PostgreSQL, заполняемым администратором PostgreSQL</li> </ul>
	Администратор PostgreSQL или администратор приложения	<ul style="list-style-type: none"> <li>Создание триггера на добавление/изменение данных в защищаемой таблице/ представлении, выполняющего запись изменяемых или добавляемых данных в стороннюю, не защищаемую, таблицу</li> <li>Получение данных из не защищаемой таблицы</li> </ul>	Ограничение возможности создания триггеров на защищаемые таблицы и представления через механизм защиты, управляемый администраторами безопасности
	Администратор PostgreSQL или администратор приложения	<ul style="list-style-type: none"> <li>Создание правила на добавление/изменение данных в защищаемой таблице/ представлении, выполняющего запись изменяемых или добавляемых данных в стороннюю, не защищаемую, таблицу</li> <li>Получение данных из не защищаемой таблицы</li> </ul>	Ограничение возможности создания правил на защищаемые таблицы и представления через механизм защиты, управляемый администраторами безопасности

Сценарий	Участники	Действия	Контрмеры
	Владелец ТУЗ приложений	<ul style="list-style-type: none"> <li>Запрос данных из защищаемых объектов БД PostgreSQL через интерфейс запросов PostgreSQL с подключением под ТУЗ, для которого разрешено чтение защищаемых данных</li> </ul>	<ul style="list-style-type: none"> <li>Реализация поддержки двухфакторной аутентификации на PostgreSQL, при которой второй фактор аутентификации для ТУЗ приложения формируется администратором безопасности или автоматически, и задается для приложений администратором безопасности</li> </ul> <p>и</p> <ul style="list-style-type: none"> <li>Администратор безопасности задает ограничение на адреса, с которых может подключаться ТУЗ приложения, в pg_hba.conf в защищенном хранилище. Владелец ТУЗ приложений не имеет доступа к серверам с адресами, с которых возможен коннект для учетной записи ТУЗ</li> </ul>
Получение данных в расшифрованном виде через канал, не поддерживающий шифрование данных	Администратор PostgreSQL или Администратор бэкапирования	<ul style="list-style-type: none"> <li>Настройка логической репликации на источнике</li> <li>Создание подписки на базе получателя</li> <li>Получение расшифрованных данных через логическую репликацию</li> </ul>	<ul style="list-style-type: none"> <li>Шифрование данных логической репликации ключем шифрования WAL кластера HA</li> </ul> <p>или</p> <ul style="list-style-type: none"> <li>Отключение механизма логической репликации</li> </ul>

Сценарий	Участники	Действия	Контрмеры
	Администратор ОС	<ul style="list-style-type: none"> <li>Отключение параметра поддержки ssl в postgresql.conf, или отключение использования ssl для конкретных клиентов в файле pg_hba.conf</li> <li>Снимается трафик в открытом виде между клиентами и PostgreSQL</li> </ul>	<ul style="list-style-type: none"> <li>Запрет использования подключений клиентов без ssl</li> </ul> <p>или</p> <ul style="list-style-type: none"> <li>Хранение параметра ssl в защищенном хранилище и хранение pg_hba.conf в защищенном хранилище</li> </ul>
	Администратор безопасности	<ul style="list-style-type: none"> <li>Отключение параметра поддержки ssl в postgresql.conf, или отключение использования ssl для конкретных клиентов в файле pg_hba.conf</li> <li>Снимается трафик в открытом виде между клиентами и PostgreSQL</li> </ul>	<ul style="list-style-type: none"> <li>Администратор безопасности не имеет доступа к серверам и элементам сети, через которые проходит трафик взаимодействия с PostgreSQL</li> </ul> <p>и</p> <ul style="list-style-type: none"> <li>настройки ssl дублируются в защищенном хранилище и локальных файлах настройки PostgreSQL, настраиваемыми администратором PostgreSQL. При несовпадении параметров выдается ошибка при запуске PostgreSQL</li> </ul>