



Разработка и сертификация средств защиты СУБД

Андрей Гусаков

Апрель 2026 г.

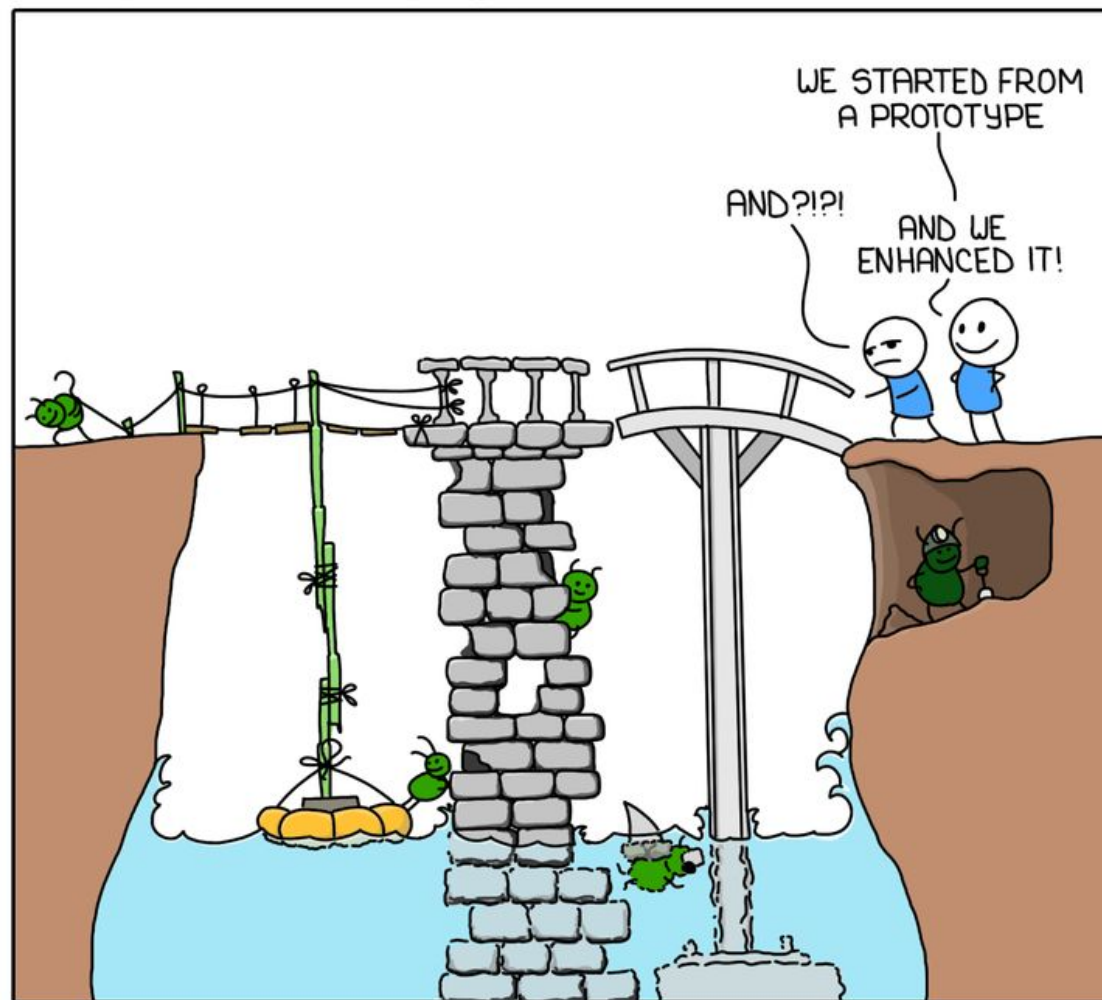
Проблема – не используются доступные средства защиты СУБД

Помимо проблем разделения труда и ответственности между отделами ИТ и ИБ существуют проблема юридического пробела в законодательных документах ФСТЭК

Имеются требования к разработчикам СУБД по наличию средств защиты, но отсутствуют требования к разработчикам приложений по обязательному их применению

В итоге задачи ИБ игнорируются или вместо промышленных решений применяются сделанные «на коленке»

PRODUCTION READY



Правильная стратегия – опора на прошедшие сертификационные испытания механизмы обеспечения ИБ

Это значительно облегчает дальнейшую аттестацию ваших ИС

Требования по безопасности информации к СУБД утверждены приказом ФСТЭК России от 14 апреля 2023 г. № 64. Они включают требования по безопасности информации, предъявляемые к:

- уровню доверия СУБД;
- операционной системе, в среде которой функционирует СУБД;
- управлению доступом в СУБД;
- идентификации и аутентификации пользователей в СУБД;
- контролю целостности в СУБД;
- регистрации событий безопасности в СУБД;
- резервному копированию и восстановлению в СУБД;
- обеспечению доступности СУБД;
- очистке памяти в СУБД;
- производительности СУБД;
- ограничению программной среды в СУБД

А в редакции приказа ФСТЭК России от 30 июня 2025 г. № 230) определен **Порядок проведения сертификации процессов безопасной разработки программного обеспечения средств защиты информации**



Сертифицированные редакции СУБД Postgres Pro

Standard

Современная СУБД, включает все новые функции PostgreSQL и полезные доработки от компании

Enterprise

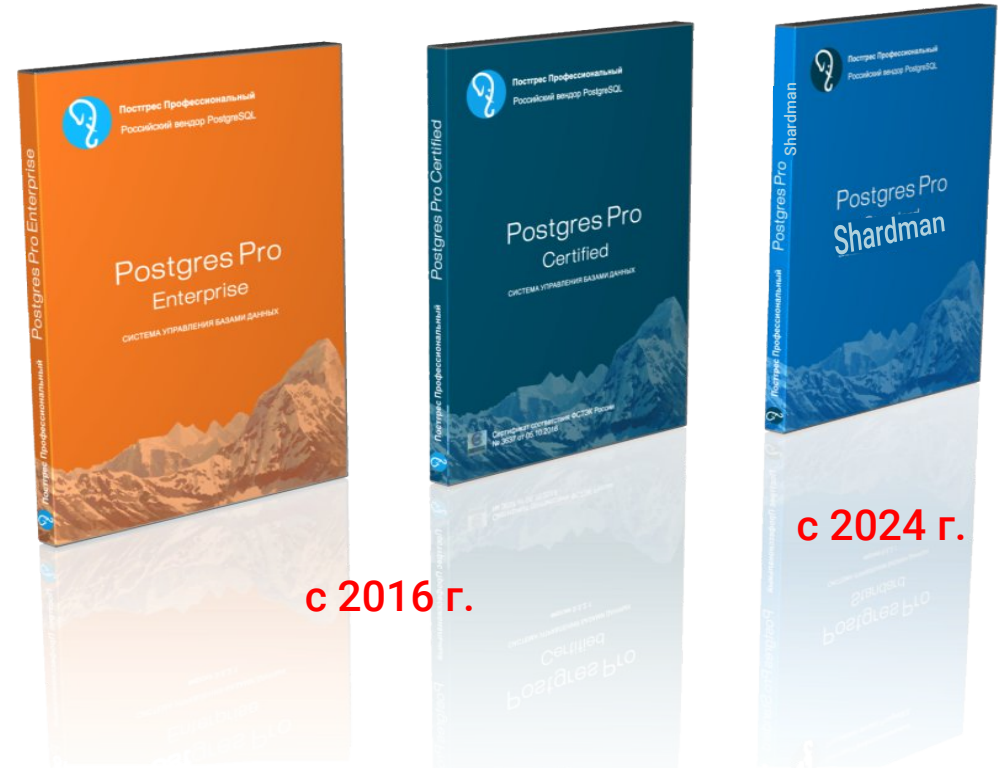
Enterprise для 1С

Наиболее полнофункциональная СУБД с высокой производительностью и масштабируемостью

Shardman

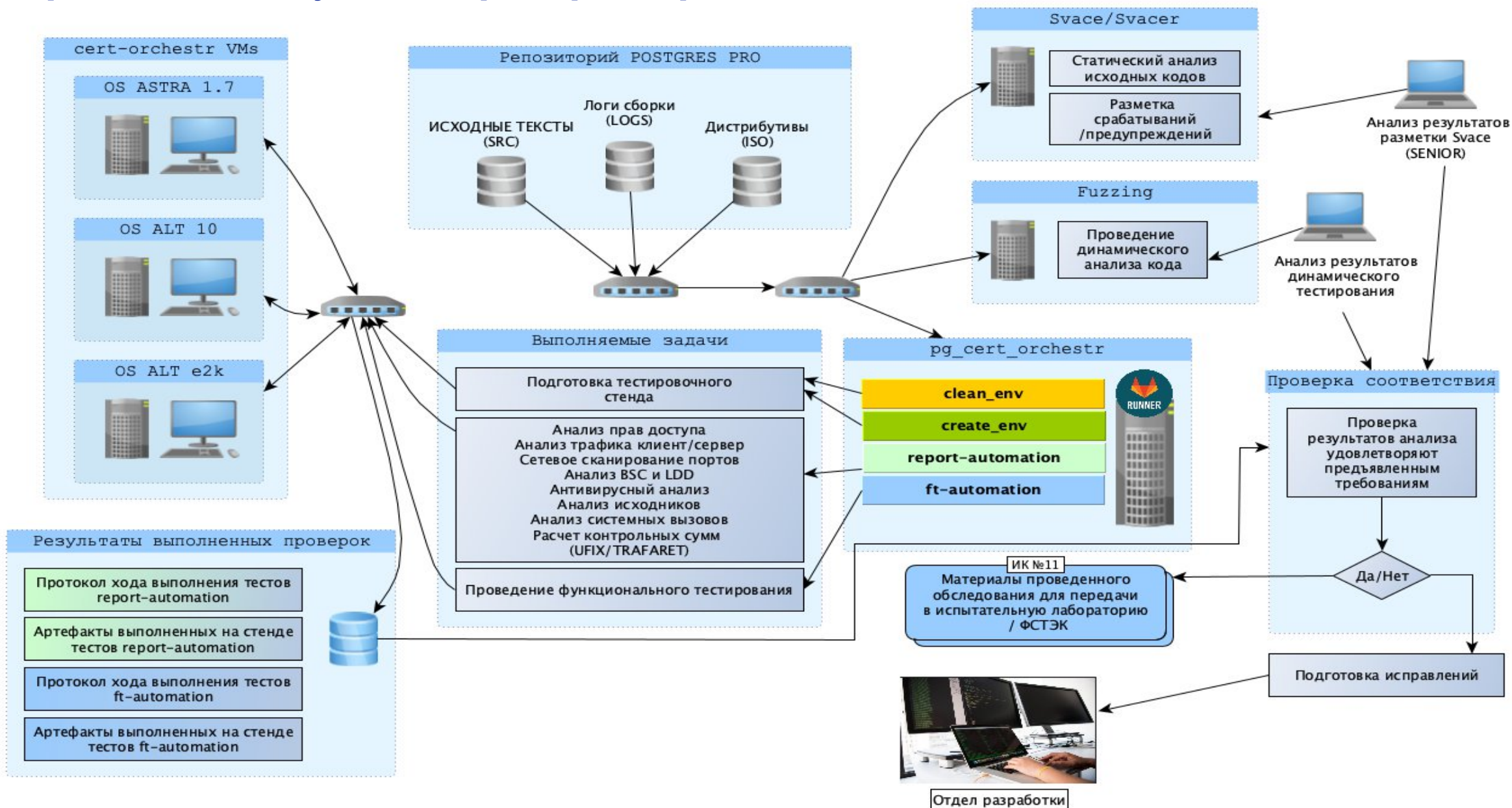
Распределенная СУБД, предоставляющая строгие гарантии целостности данных

соответствуют «Требованиям по безопасности информации к СУБД» ФСТЭК России самого высокого для защиты конфиденциальной информации четвертого класса защиты и уровня доверия



с ежеквартальным обновлением в рамках инспекционного контроля

Процесс выпуска сертифицированных обновлений...



...упрощается после получения нами сертификата РБПО

Эволюция разработки средств ИБ

Компания Postgres Professional успешно доказала наличие ресурсов, знание технологий и зрелость процессов

Цель сертификации – сохранив безопасность ПО, снизить издержки разработчиков и ускорить доставку обновлений пользователям



СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ



СЕРТИФИКАТ СООТВЕТСТВИЯ № 7

Выдан: 21 октября 2025 г.
Действителен до: 21 октября 2030 г.

Настоящий сертификат удостоверяет, что процессы безопасной разработки, реализованные обществом с ограниченной ответственностью «Постгрес Профессиональный» (ООО «Постгрес Профессиональный»), соответствуют требованиям национального стандарта ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования», утвержденного и введенного в действие приказом Федерального агентства по техническому регулированию и метрологии от 24 октября 2024 г. № 1504-ст.

Сертификат выдан на основании результатов сертификации, проведенной органом по сертификации федерального государственного бюджетного учреждения науки Институт системного программирования им. В.П. Иванникова Российской академии наук (аттестат аккредитации от 24.05.2024 № СИ RU.0001.01БИ00.А009) - экспертное заключение от 26.09.2025.

ПЕРВЫЙ ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ



В.Лютиков

Где можно использовать наши сертифицированные редакции

Системы управления базами данных, соответствующие 4 классу защиты, применяются:

- в значимых объектах критической информационной инфраструктуры 1 категории значимости,
- в государственных информационных системах 1 класса защищенности,
- в автоматизированных системах управления производственными и технологическими процессами 1 класса защищенности,
- в информационных системах персональных данных при необходимости обеспечения 1 уровня защищенности персональных данных,
- в информационных системах общего пользования II класса

Приказ ФСТЭК РФ от 11.04.2025 N 117 даёт преимущество решениям обладателей РБПО-сертификатов

Либо организация-оператор ГИС или ИС ЗОКИИ сама реализует меры по ГОСТ Р 56939-2024, либо использует ПО от доверенного поставщика (дословно – «привлекает подрядную организацию» с сертификатом)

«В случае самостоятельной разработки оператором (обладателем информации) программного обеспечения, предназначенного для использования в информационных системах, должны быть реализованы меры, предусмотренные разделами 4 и 5 ГОСТ Р 56939-2024.

В случае привлечения оператором (обладателем информации) для разработки программного обеспечения подрядной организации по решению руководителя (ответственного лица) в техническое задание на разработку программного обеспечения могут быть включены требования по разработке безопасного программного обеспечения в соответствии с ГОСТ Р 56939-2024» (см. п. 50)



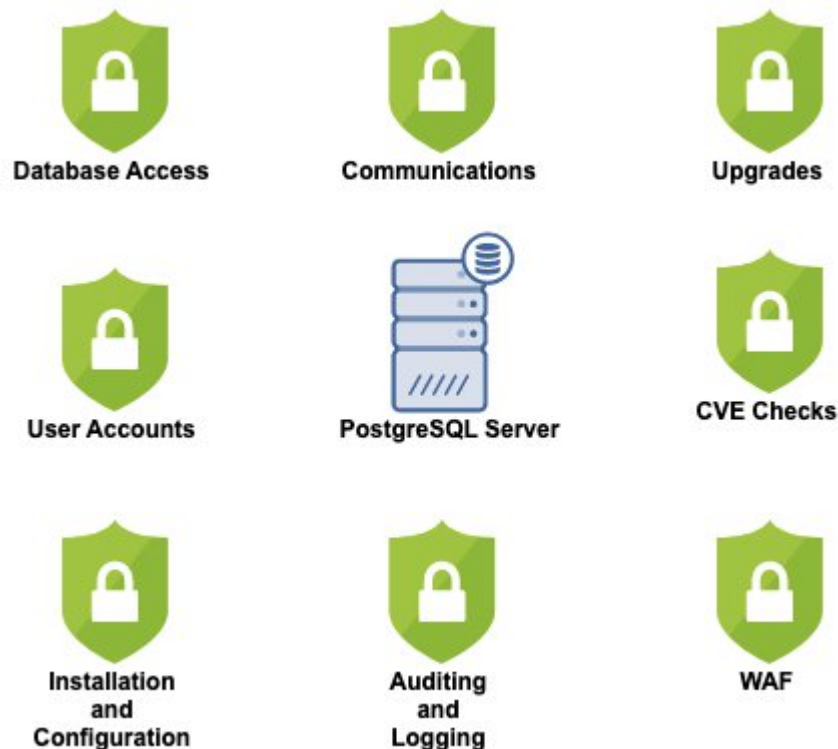


Механизмы реализации требований ФСТЭК по безопасности информации к СУБД

PostgreSQL-сообщество предлагает множество решений ИБ и выпускает исправления для найденных уязвимостей

Наши продукты опираются на базовый функционал по защите СУБД

Аспекты ИБ, которые необходимо учитывать



- Ролевая модель управления привилегиями с наследованием прав
- Row Level Security и представления
- Безопасность подключений и контроль доступа (диапазон IP, порты, таймауты, SSL, ограничение числа подключений)
- Идентификация и аутентификация клиентов (пароли, LDAP, cert, Kerberos, OAuth)
- Встроенный аудит (журнал событий)
- Встроенная криптозащита (пароли, столбцы, на стороне клиента)

Операционные системы, в среде которых функционирует СУБД

Требование:

Система управления базами данных должна функционировать в среде сертифицированной операционной системы, имеющей класс защиты не ниже класса защиты СУБД

Реализация:

Двоичные пакеты Postgres Pro предоставляются для следующих систем:

- **Linux** для архитектуры **x86-64**:
 - Astra Linux Special Edition 1.7/1.8
 - Альт СП 8/8.2/8.4, Альт СП релиз 10
 - МосОС 15
 - РЕД ОС 7.3/8
 - РОСА «ХРОМ» 2021.1
- **Linux** для архитектуры процессоров **Эльбрус**:
 - Альт СП 8 для e2k/e2kv4
 - Альт СП релиз 10 для e2k/e2kv4
 - Astra Linux Special Edition «Ленинград» 8.1 для e2k-8c



Управление доступом в СУБД

Требование:

Ролевой метод управления доступом должен быть реализован для следующих ролей пользователей СУБД: администратор СУБД, администратор БД (администратор информационной системы), пользователь БД (пользователь информационной системы)...

Реализация:

- **Запрет использования УЗ суперпользователя СУБД** для повседневных операций путем делегирования его полномочий специальным ролям через predetermined роли и функции
- **Полный контроль** за администраторами через механизмы аудита

Минимальный набор прав обычного пользователя



Набор прав суперпользователя

- Создадим администратора БД для настройки конкретной БД

- Создадим администратора СУБД для настройки экземпляра СУБД

```
root: edit pg_hba.conf
auth type = reject
chown root & chmod 640
```

- Временно заблокируем суперпользователя с помощью администратора инфраструктуры

Управление доступом в СУБД

Дополнительно:

Администратор без доступа к данным (аналог Oracle Database Vault)

- Вводятся специальные роли для использования в защищенной схеме – ее владельца (доверенного администратора) и менеджера прав доступа
- Назначение схеме менеджера прав доступа превращает ее в защищенную
- Владелец схемы имеет доступ к ее объектам по умолчанию, но теперь администраторы и бизнес-пользователи могут получить доступ к ним только после явного разрешения от менеджера прав доступа
- Для контроля доступа используется стандартный механизм ACL

Поиск избыточных привилегий (Отчетность по способу получения и по реальному использованию привилегий)

- Подзадача в рамках Управления Жизненным Циклом Данных
- Отчёт выполняется путём сравнения всех выданных прав (включая доступ, полученный через другие роли) с реально использованными
- Использование прав определяется статистикой

Идентификация и аутентификация пользователей в СУБД

Требование:

При исчерпании установленного максимального количества неудачных попыток ввода неправильного пароля учетная запись пользователя ... / администратора БД / СУБД ... должна быть заблокирована СУБД с возможностью разблокировки администратором БД / СУБД или с возможностью автоматической разблокировки по истечении временного интервала

Пароль пользователя СУБД должен содержать не менее 8 символов при алфавите пароля не менее 70 символов

Реализация:

Управление политиками блокировок УЗ реализовано через **интегрированный в ядро СУБД механизм профилей**. Профиль ограничивает использование базы данных и устанавливает парольную политику для ролей. Выполнять команду CREATE PROFILE разрешено только суперпользователям БД или пользователям с правами роли pg_manage_profiles.

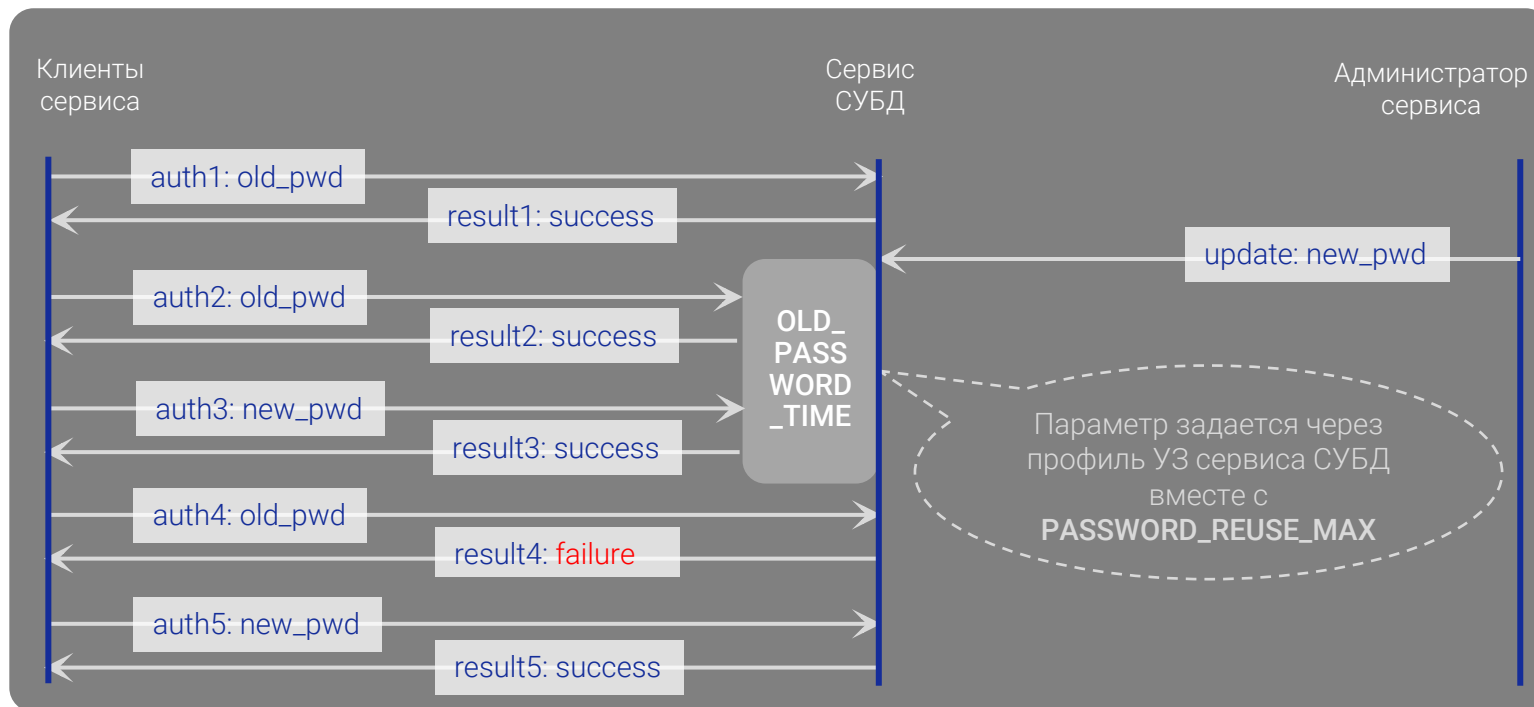
Параметры профиля ограничивают число неверных попыток входа, задают интервал хранения неудачных попыток, устанавливают минимальное количество символов в пароле, минимальное количество уникальных символов в пароле и включают проверку его сложности:

- Пароль содержит как минимум по одному символу из трёх перечисленных групп: строчные буквы, прописные буквы, цифры и специальные символы
- Пароль не содержит имя пользователя

Идентификация и аутентификация пользователей в СУБД

Дополнительно:

Отложенное изменение пароля (временное сосуществование старого и нового пароля при смене)



- Пароль может стать «старым», только если на момент установки нового пароля он ещё валиден
- В качестве параметров password_encryption поддерживаются md5 и scram-sha-256
- Клиент получает оповещение с предложением сменить пароль на новый

Контроль целостности в СУБД

Требование:

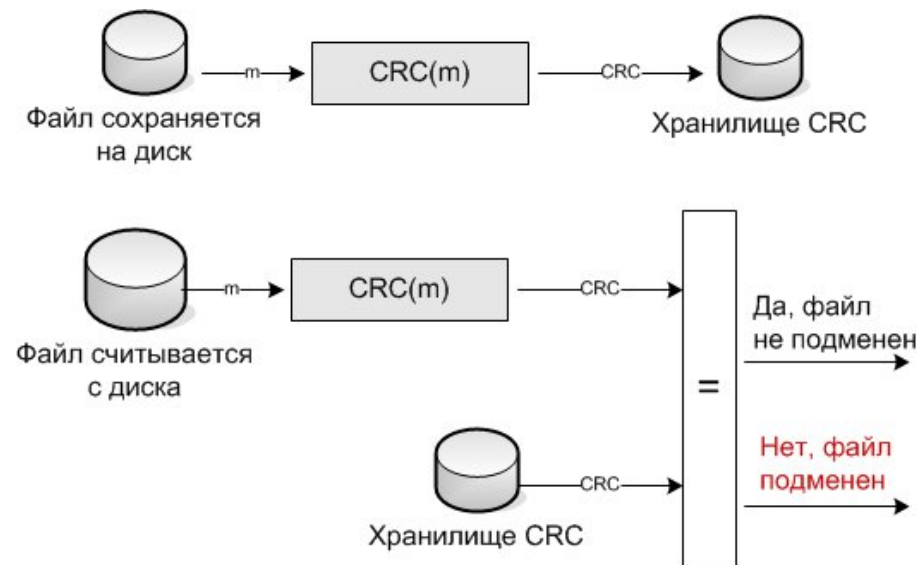
СУБД должна **контролировать** целостность конфигурации СУБД, конфигураций БД, процедур (программного кода) СУБД, процедур (программного кода), хранимых в БД, в процессе запуска СУБД самостоятельно или с применением сертифицированной ОС;

информировать администратора СУБД о нарушении целостности объектов контроля;

блокировать доступ пользователей СУБД и БД (за исключением администратора СУБД) к СУБД и БД при выявлении нарушения целостности объектов контроля.

Реализация:

- Утилита **pg_integrity_check** проводит **расчет контрольных сумм объектов контроля** с учетом содержимого файла, его атрибутов и времени изменения
- Имеются отдельные настройки для неизменяемых файлов (бинарники) и файлов, которые могут быть изменены администратором баз данных (конфигурационные файлы, системные таблицы, функции). Для первых контрольные суммы поставляются готовыми, для вторых необходимо провести расчеты при вводе в промышленную эксплуатацию
- Контроль целостности выполняется автоматически **при старте СУБД или по расписанию**; при несовпадении контрольных сумм требуется вмешательство администратора СУБД или инфраструктуры для принятия изменений или отката



Регистрация событий безопасности в СУБД

Требование:

СУБД должна обеспечивать регистрацию событий безопасности, связанных с функционированием СУБД и действиями пользователей СУБД...

Реализация:

Расширение **pg_proaudit** с

- Оптимизированным механизмом фильтрации событий – правило для аудирования определяется комбинацией параметров из:
 - Имени базы данных
 - Типа события (можно указать как конкретные команды, так и классы событий)
 - Типа объекта
 - Имени объекта
 - Имени роли (можно указать как конкретного пользователя, так и групповую роль)
- Высоким быстродействием благодаря параллельной обработке

Регистрация событий безопасности в СУБД

Дополнительно:

Различные форматы записи или перенаправления событий (CSV, CEF, syslog) для упрощения интеграции с SIEM-приложениями

Классы событий с исключением временных объектов

Обязательное маскирование паролей в журнале сервера для защиты конфиденциальных данных

Отслеживание продолжительности сессии и объема передаваемых данных (функционал DBFW)

Резервное копирование и восстановление в СУБД

Требование:

В СУБД должно обеспечиваться резервное копирование и восстановление конфигурации СУБД, баз данных и их конфигураций, в том числе атрибутов безопасности, самостоятельно или с применением сертифицированных операционной системы или средства резервного копирования.

Реализация:

Утилита **pg_probackup** обеспечивает управление локальным и удалённым резервным копированием и восстановлением кластеров баз данных Postgres Pro. Оно предназначено для регулярного создания резервных копий экземпляра Postgres Pro, позволяющих восстанавливать сервер в случае необходимости

В отличие от многих других российских вендоров, использующих рискованную с точки зрения сроков выпуска исправлений утилиту WAL-G, это – полноценная отечественная разработка

Дополнительно:

Реализована глубокая интеграция с комплексным решением для администрирования инфраструктуры баз данных Postgres Pro Enterprise Manager (**PPEM**), позволяющая выполнять все операции pg_probackup через графический интерфейс

Обеспечение доступности СУБД

Требование:

СУБД 4 класса защиты должна функционировать в отказоустойчивом кластере, обеспечивающем её доступность, за счет одновременного функционирования нескольких экземпляров СУБД

Комментарий:

Отказоустойчивость – это не просто параллельная работа нескольких экземпляров СУБД; это:

- физическая репликация, которая может включать каскадную, которая в свою очередь может быть как синхронной, так и асинхронной,
- автоматическое обнаружение сбоя узлов,
- механизм аварийного переключения узлов в случае сбоя,
- фиксация изменения конфигурации кластера;

Реализация:

- Расширение **BiHA** (Built-in High Availability) с доработками ядра, утилитой управления и процессом координации узлов обеспечивает отказоустойчивость и автоматическое восстановление после отказа узлов
- В отличие от многих других российских вендоров, использующих рискованные с точки зрения сроков выпуска исправлений Stolon или Patroni, это – полноценная отечественная разработка

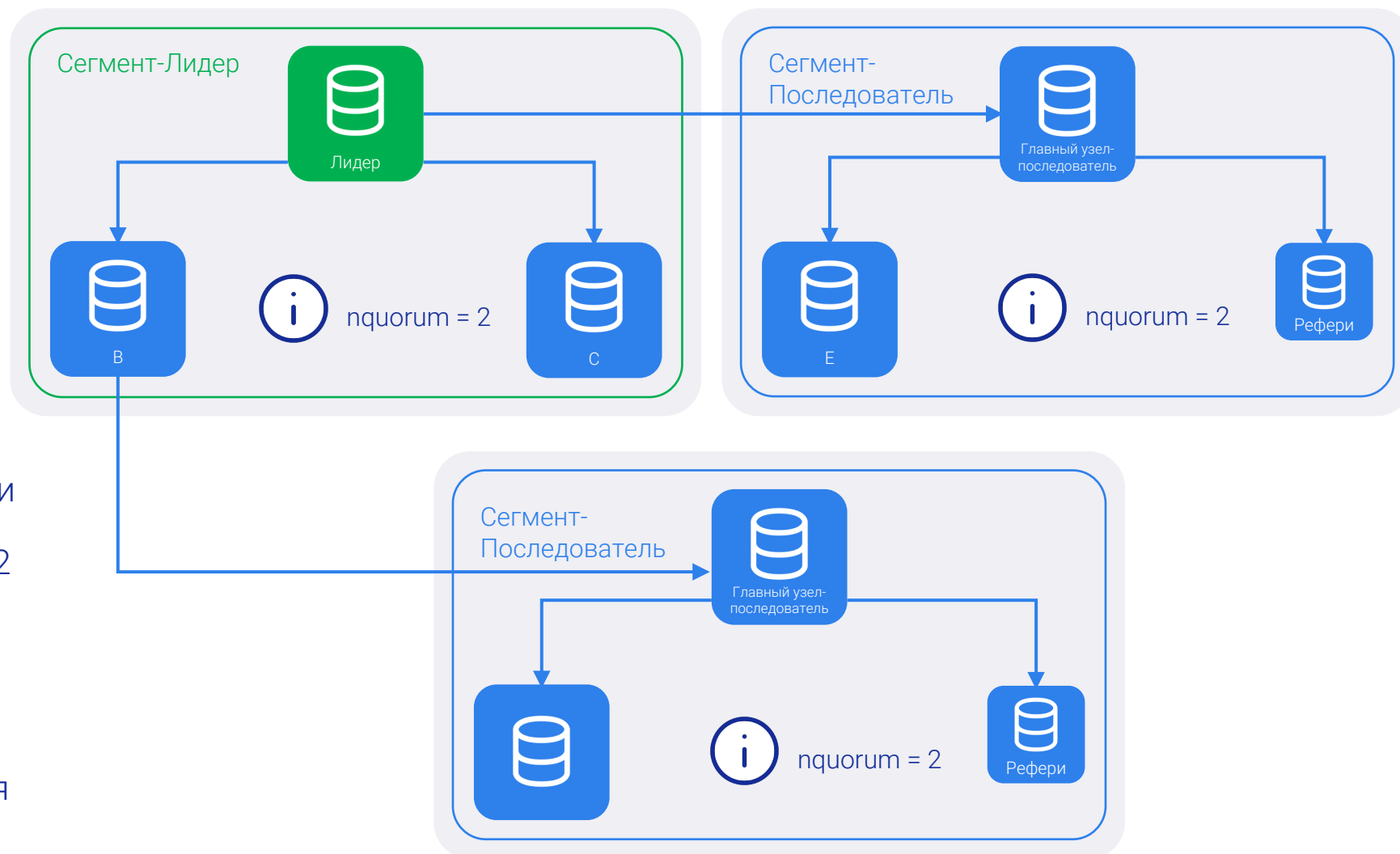
Обеспечение доступности СУБД

Реализация:

Многоуровневый катастрофоустойчивый кластер (GDBiHA)

- Каждый сегмент имеет собственную систему выборов
- Сегменты имеют свои параметры кворума и минимально количества нод
- Сегмент-последователь может стать автоматически Сегмент-лидером, только если сегментов более чем 2 (будет реализовано в будущей версии)

Не требующий лицензирования узел рефери используется для обеспечения кворума и накопления WAL



Обеспечение доступности СУБД

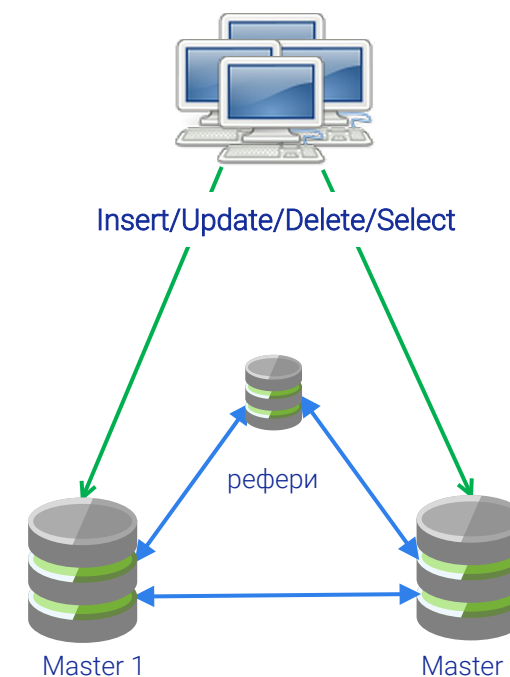
Дополнительно:

Proxima (Pooler, Proxy, Load Balancer):

- Proxima работает внутри экземпляров Postgres Pro на каждом узле кластера ViNA
- Любой узел может быть точкой входа в кластер с перенаправлением пишущей нагрузки на лидера, а читающей – на реплики
- Определение лидера ViNA происходит на лету
- В случае сбоя одного узла клиент может подключиться к Proxima на любом другом узле
- После обработки сбоя Proxima перенаправляет соединения на новый лидер ViNA

Мультимастер (минимизация простоев):

- Основан на логической репликации
- Все узлы доступны на запись
- Масштабирование на чтение
- Управление транзакциями
- Гарантия синхронности данных на всех узлах



Очистка памяти в СУБД

Требование:

СУБД 4 класса защиты должна обеспечивать удаление БД и журналов, а также удалять объекты доступа базы данных, используемые СУБД, путем перезаписи модифицированных **участков** объектов файловой системы при выполнении операции удаления

Комментарий:

Многие другие российские вендоры делегируют эту задачу ОС; но команды Linux `wipe` или `shred` можно использовать только для **удаление файлов** баз данных и журналов **целиком!**

В отличие от них, наше решение работает с сегментами памяти внутри объектов, не освобожденных СУБД и не переданных ОС

Реализация:

Немного разные решения используются для

- Удаления **фрагментов файлов** с дисков
- Очистки **страниц** (Multiversion Concurrency Control → VACUUM)
- Очистки **блоков памяти** в ОЗУ (MemoryContexts)
- Очистки **файлов WAL** (удаление или перезапись **сегментов**)

Это – полноценная отечественная разработка

Производительность СУБД

Требование:

СУБД должна обеспечивать производительность со следующими параметрами:

- количество пользовательских сессий, поддерживаемых параллельно;
- количество обрабатываемых стандартных запросов в единицу времени;
- количество транзакций в единицу времени;
- задержка в выполнении стандартного запроса, определенного в документации СУБД;
- количество экземпляров СУБД, которые могут совместно работать в режиме балансировки нагрузки.

Реализация:

Среди множества решений необходимо выделить:

Улучшенный **механизм проверки блокировок**, не оказывающий отрицательного влияния на производительность

AQO – использование машинного обучения для оптимизации запросов по стоимости их выполнения

plantuner – возможность добавлять поддержку указаний для планировщика, позволяющих отключать или подключать определённые индексы при выполнении запроса

pg_wait_sampling – возможность периодического сбора статистики по событиям ожидания

pgpro_stats – возможность трассировки сеансов приложений основе фильтров, которые запускают протоколирование выполнения запросов

Ограничение программной среды в СУБД

Требование:

СУБД 4 класса защиты должна запрещать создание процедур (программного кода), хранимых в БД, пользователям БД (пользователям информационной системы); ... выявлять и блокировать загрузку в адресное пространство СУБД программного обеспечения, целостность которого нарушена

Реализация:

Для запрета создания хранимых процедур и функций в БД необходимо **управлять правами доступа** на уровне схем и языков процедур:

- Отзовите право CREATE на схеме у роли public;
- Запретите использование (USAGE) языков процедур (например, plpgsql, plpython3u);
- Явно предоставьте эти права доверенным ролям (например, администраторам БД).

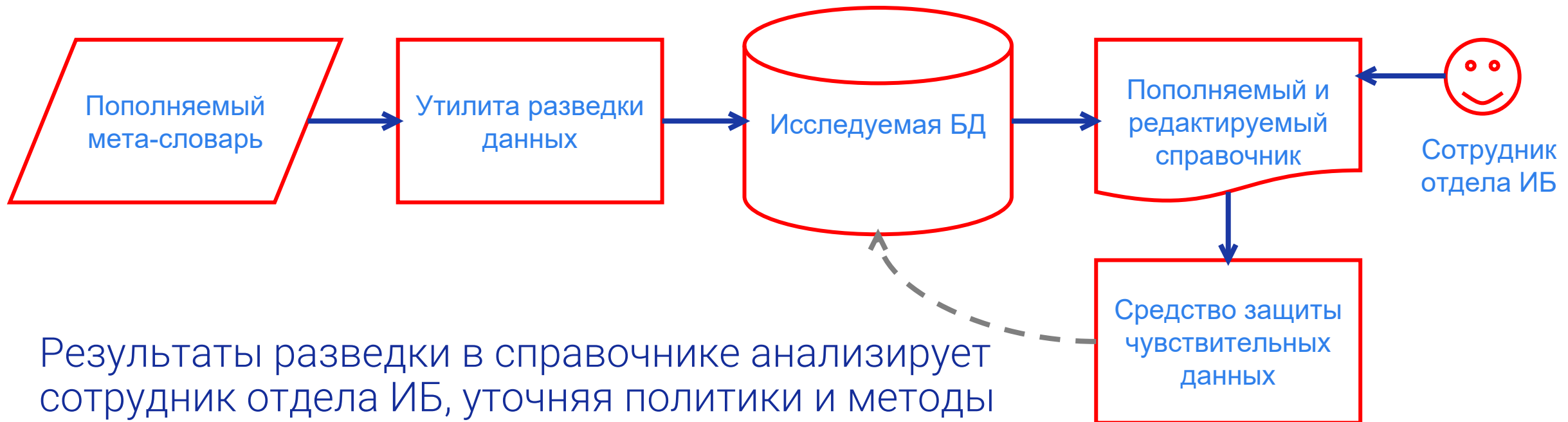
Используйте утилиту **pg_integrity_check** для **расчета контрольных сумм** процедур (программного кода), хранимых в БД



Механизмы обеспечения информационной безопасности в сертифицированных редакциях СУБД вне требований ФСТЭК

Утилита для поиска чувствительной информации

Для разведки используется мета-словарь, содержащий маски для проверки имен и содержимого полей по набору регулярных выражений и константным значениям (названия организаций, фамилии и т. д.)



Результаты разведки в справочнике анализирует сотрудник отдела ИБ, уточняя политики и методы защиты (в отношении каких схем или таблиц, ролей, статическое или динамическое маскирование и т.п.)

Защита данных методом обезличивания

Требования определены Приказом Роскомнадзора от 19.06.2025 № 140 и Постановлением Правительства РФ от 1 августа 2025 г. № 1154

Во многих случаях раскрытие данных СУБД нежелательно, и для защиты коммерческих или персональные сведений их надо заменить либо фейковой, либо частичной информацией
Оригинал при этом остается нетронутым

pgpro_anonymizer – расширение для маскирования или замены конфиденциальных данных внутри экземпляра PostgresPro

В проекте используется декларативный подход к анонимизации. Вы можете объявлять правила маскирования, используя язык описания данных (DDL), и задавать свою стратегию анонимизации внутри определения таблицы

Используются следующие основные стратегии:

- **Динамическое** маскирование изменяет представление реальных данных, не модифицируя их. Некоторые пользователи могут читать только замаскированные данные, а другие могут получить доступ к исходной версии
- **Статическое** маскирование полностью заменяет выгружаемую конфиденциальную информацию несвязанными данными. После такой обработки исходные данные не могут быть восстановлены

Защита данных в состоянии покоя методом прозрачного преобразований (TDE)

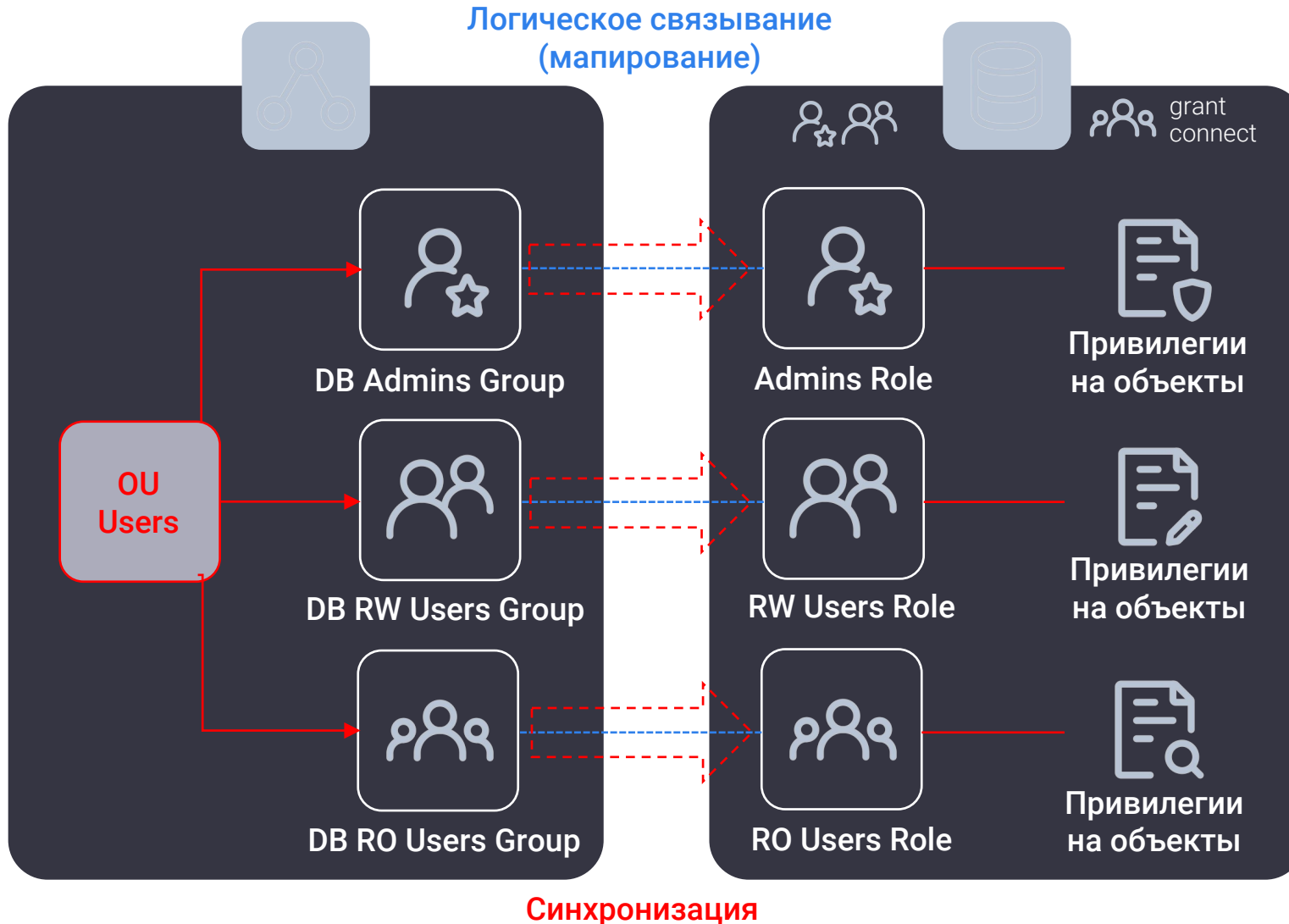
Выделенное табличное пространство и оптимальные алгоритмы минимизируют влияние на производительность

Все поставляемые в составе сервера СУБД утилиты работают с защищенными данными СУБД точно так же, как с незащищенными

Имеется интеграция с сертифицированными отечественными KMS



Синхронизация ролей и привилегий СУБД с группами LDAP



На базе расширения **Idap2pg** происходит периодический опрос состава выделенных групп каталога, сравнение с составом связанных групповых ролей СУБД и формирование набора применяемых к СУБД изменений (CREATE, DROP и ALTER)

Обфускация кода хранимых функций и процедур

Что хочется предотвратить:

Несанкционированные правки кода

Лишние вопросы о тех или иных решениях в коде

Как добавляется защита:

Encode (`convert_to` (<текст создания функции или любой произвольный текст>, 'UTF8'), <алгоритм (например, 'base64' или XOR кодирование по фиксированному hardcoded ключу)>) + сжатие

Как СУБД понимает, что код защищен:

Реализована механика экранирования текста меткой `$_PGPROwrapped_` с двух сторон. Экранированный таким образом текст воспринимается, как скрипт в base64. Он сначала раскодируется, а затем выполняется.

```

$_PGPROwrapped_ $U0VMRUNUIDE7Cg==$_PGPROwrapped_ ;
?column? |
-----+
      1 |

```

Планы

pgpro_tde:

Повышение производительности

Защита временных таблиц

Интеграция с решениями провайдеров СКЗИ

PREM:

Сертификация в составе СУБД

Добавление специализированной консоли Администратора ИБ

Мониторинг SQL-трафика (DAM) и анализ запросов

Выявление нарушений и аномалий (UBA/UEBA)

Образование:

Обновление курса “PGPRO. Возможности Postgres Pro Enterprise” на базе 16 версии

Выпуск специализированных книжек по обеспечению ИБ в СУБД

Дополнительные материалы

Обучающие видео по теме ИБ см. на postgrespro.ru/video/how-to :

- Как минимизировать угрозы со стороны суперпользователя
- Ограничение доступа привилегированных пользователей к данным
- Как снизить риски раскрытия конфиденциальной информации

Скрипты для самостоятельного прохождения сценариев из How-to по безопасности СУБД на postgrespro.ru/materials

Недавние **доклады и вебинары** :

- «Новые возможности для обеспечения безопасности и защиты данных» на pgproday.ru/pgprotechday
- «Организация защиты данных в Postgres Pro: пошаговая инструкция» на pgconf.ru/260120
- «Решение вопросов ИБ в приложениях 1С, развернутых на СУБД Postgres Pro» на pgconf.ru/vebinarr/talks с отдельным 20-минутным видео с описанием демо-стенда и демонстрацией

 PostgresPro

См. ежегодное
исследование рынка СУБД
от Центра Стратегических
Разработок



**Спасибо за
внимание!**



presales@postgrespro.ru