ШИФРОВАНИЕ В СУБД «КВАНТ-ГИБРИД»

СЗИ: СС ФСТЭК № 4691 от 12 июля 2023 г.
СКЗИ: СС ФСБ № СФ/124-4721 от 15 января 2024 г.

Презентация к докладу конференции CNews СУБД: технологии, миграция и администрирование 2026

Турканов И.Ф.

СУБД «Квант-гибрид»

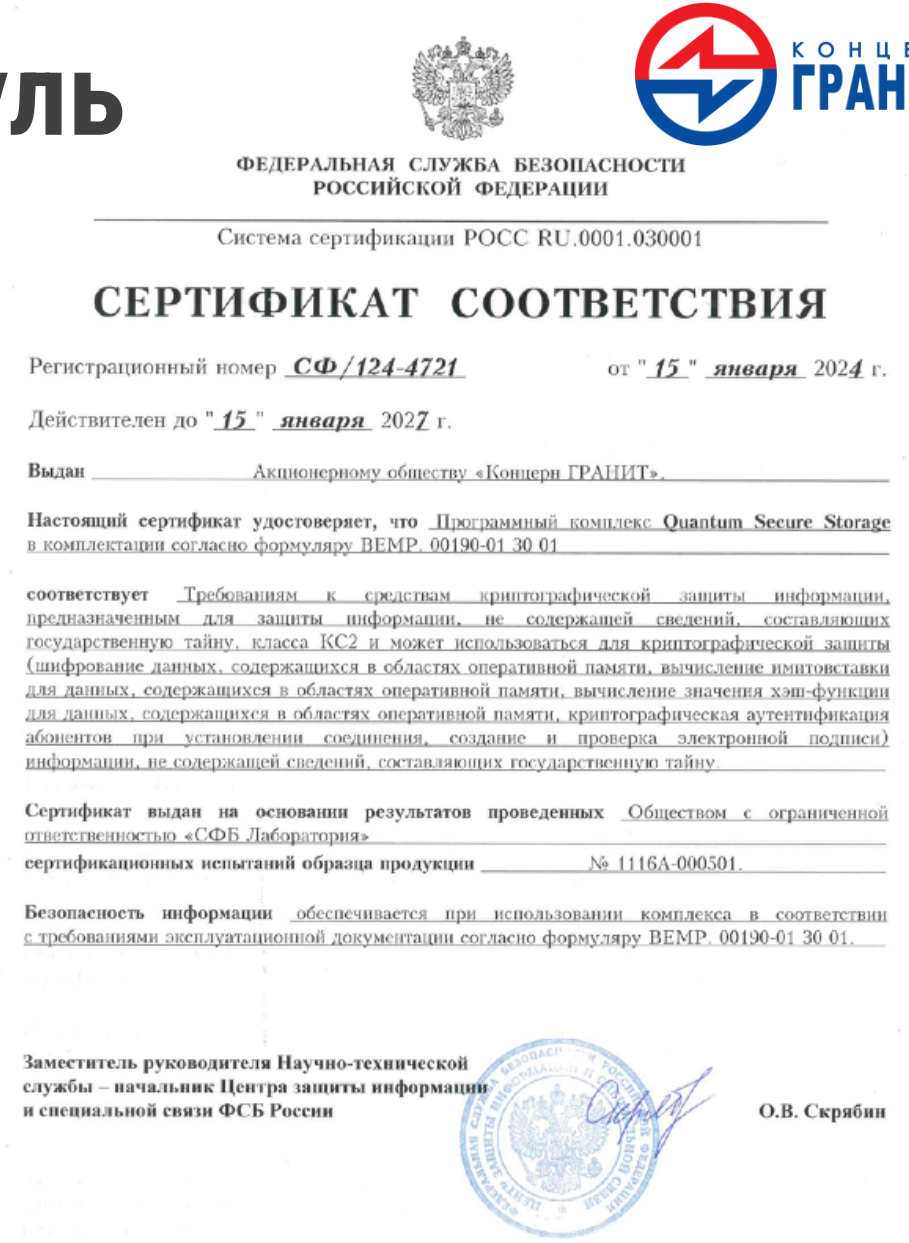
Наш продукт представляет собой коммерческий форк открытого программного обеспечения PostgreSQL (https://www.postgresql.org/).

Компания ведет разработку и постоянное совершенствование продукта уже более семи лет. Основные направления модификации - увеличение стабильности, повышение безопасности, расширение функциональности и быстродействия.

Одной из отличительных особенностей продукта является шифрование на уровне ядра СУБД.

Криптографический модуль

Криптографический модуль QSS ориентирован на российский рынок, он реализует набор национальных российских криптографических стандартов (ГОСТ). В нем используется блочный шифр Кузнечика, хэш-функция Стрибог и алгоритмы цифровой подписи ГОСТ 34.10-2018, основанные на эллиптических кривых. Продукт успешно прошел криптографическую сертификацию в Федеральной службе безопасности (ФСБ).



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-4721 от "15" января 2024 г.

Действителен до "15" января 2027 г.

Выдан Акционерному обществу «Концерн ГРАНИТ».

Настоящий сертификат удостоверяет, что Программный комплекс Quantum Secure Storage в комплектации согласно формуляру ВЕМР. 00190-01 30 01

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС2 и может использоваться для криптографической защиты (шифрование данных, содержащихся в областях оперативной памяти, вычисление имитовставки для данных, содержащихся в областях оперативной памяти, вычисление значения хэш-функции для данных, содержащихся в областях оперативной памяти, криптографическая аутентификация абонентов при установлении соединения, создание и проверка электронной подписи) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «СФБ Лаборатория» сертификационных испытаний образца продукции № 1116А-000501.

Безопасность информации обеспечивается при использовании комплекса в соответствии с требованиями эксплуатационной документации согласно формуляру ВЕМР. 00190-01 30 01.

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России О.В. Скрябин

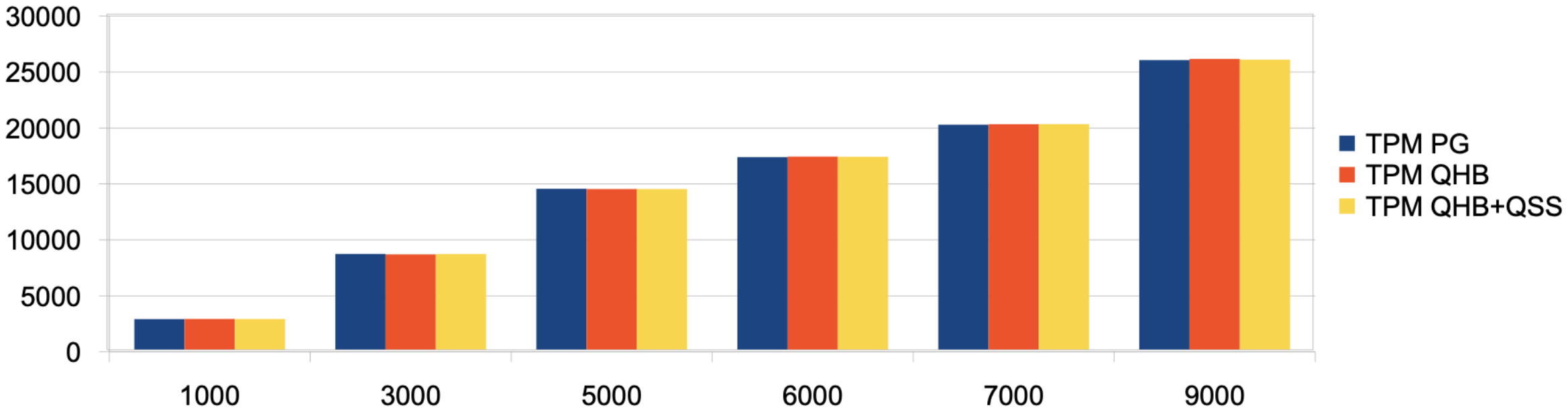
Криптографический модуль

КОНЦЕРН ГРАНИТ

Шифровать данные можно как всей базы данных, так и только выделенных таблиц. Если таблица объявляется как шифрованная, то все данные, относящиеся к ней и хранимые на дисках, будут всегда зашифрованы. Данные таблицы расшифровываются только тогда, когда попадают в оперативную память, в буферный кеш. При изменении и вытеснении из буферного кеша, данные снова зашифровываются.

Также, утилита бинарного резервного копирования, как для полных копий, так и для инкрементальных, будет работать с зашифрованными данными.

Графики производительности с шифрованием и без



При увеличении объема буферного кеша падение производительности за счет утилизации ресурсов шифрованием нивелируется (даже для очень слабых машин как в данном тесте)

PostgreeSQL и уязвимости

Свежие данные только за февраль 2026 года рисуют картину высокой активности вокруг безопасности PostgreSQL. За короткий промежуток времени было зафиксировано множество критических уязвимостей:

- **Удаленное выполнение кода (RCE)-**Наибольшая угроза представляющая критические уязвимости, позволяющих атакующему выполнить произвольный код на сервере .
- **Повышение привилегий через расширения-**позволяет обычному пользователю стать суперпользователем.
- **Атаки через цепочку поставок-**создают риск внедрения вредоносного кода во время восстановления из бэкапа.
- **Утечка информации и обход ACL-**позволяет пользователю читать выборочные данные (гистограммы, списки популярных значений) из статистики оптимизатора, обходя при этом права доступа к представлениям (views) и политики защиты строк (row security).

PostgreeSQL и уязвимости

Такая концентрация критических проблем за короткий срок говорит о том, что поверхность для атак на системы с PostgreSQL в начале 2026 года была значительной, а риск компрометации данных — высоким

Это ведет к потенциальной возможности реализации разведывательных и диверсионных миссий, таких как утечка, уничтожение или изменение данных, а также вывод систем управления базами данных из строя. Особенно с привлечением злоумышленниками и специальными службами недружественных государств преступного ИИ.

Поверхность атаки

КОНЦЕРН ГРАНИТ

В **СУБД «Квант-гибрид»** достигается существенное снижение поверхности атаки за счет применения комплекса мер, таких как:

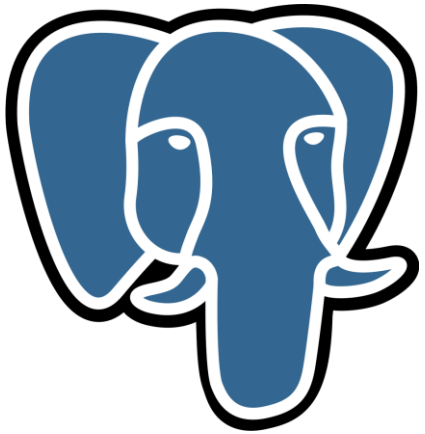
- **Шифрование** (даже в случае доступа и утечки данных сами данные не будут скомпрометированы, а атака будет бесполезной)
- **Рефакторинг кода ядра** (в настоящее время 20% переписано на языка RUST- это снижение завуалированных недекларированных возможностей исходного PostgreeSQL)
- **Применение языка RUST** для написания расширений (устранение утечки памяти, гонки данных, висящих ссылок , эффективное использование памяти и современных мультипроцессорных архитектур)
- **Модули и Утилиты собственной разработки** бэкапирования, кластеризации, балансировки, менеджера кэша дисковых блоков, и др.

OpenSource «сообщество»

Министерство войны США

Агентство Передовых Оборонных Исследовательских Проектов США,

Калифорнийский университет в Беркли



PostgreSQL Global Development Group (PGDG)

PostgreSQL Community Association of Canada (PGCAC)

Перечень иностранных и международных организаций, деятельность которых признана нежелательной на территории Российской Федерации

- № п/п 339 (02.03.2026)
- Номер распоряжения Минюста России о включении в перечень 272-р
- Дата принятия решения Генеральной прокуратурой Российской Федерации 16.02.2026
- **University of California, Berkeley (UC Berkeley, «Калифорнийский университет в Беркли»), США**
- Дата обнародования информации о признании деятельности организации нежелательной на территории Российской Федерации 03.03.2026
- Статус Включена

СПАСИБО ЗА ВНИМАНИЕ

Россия, 119019, г. Москва, ул. Гоголевский бульвар, д. 31, стр. 2, эт. 2, пом.1
т. 8 (495) 642-9742, ф. 8 (499) 558-1529
office@granit-concern.ru, granit-concern.ru