PostgresPro

От комплаенса к реальной эффективности

Живая система – лучший аргумент
на аудите РБПО

Мария Матвейчук

Postgres Professional сегодня

PostgresPro

Сертификат РБПО №7

соответствие ГОСТ Р 56939-2024 процессов безопасной разработки ПО

ТОП-5

в мире по вкладу в PostgreSQL

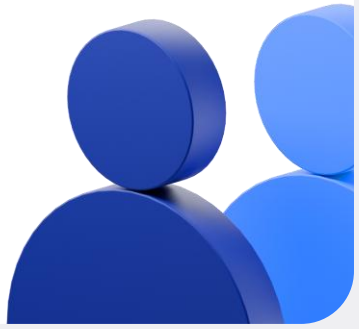
(100+ патчей ежегодно)

№1

в России среди разработчиков СУБД по данным ЦСР (2024)

500+

специалистов в команде, включая Major Contributors PostgreSQL



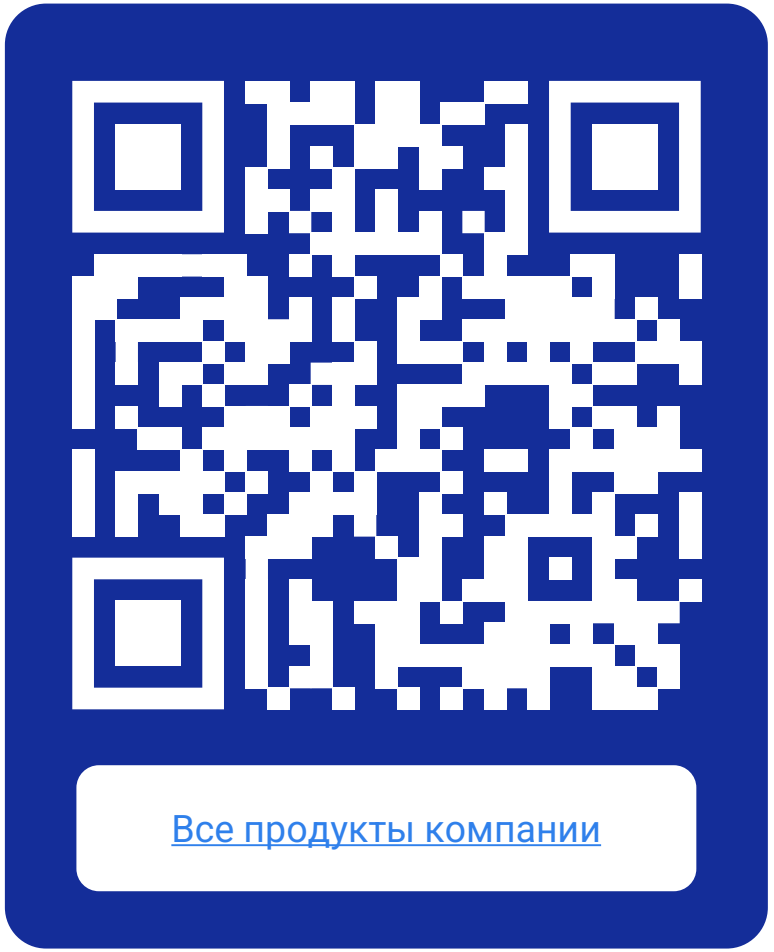
3000+ заказчиков

крупнейшие госкомпании, банки, телеком, критическая инфраструктура

Основные направления Postgres Professional

PostgresPro

- СУБД
- Машины баз данных
- Масштабирование
- Аналитика больших данных
- Миграция и репликация
- ИИ-решения
- Управление и резервное копирование
- Услуги



Все продукты компании

PostgresPro

Душно, но важно

Почитаем ГОСТ Р 56939-2024: вдруг кто-то не читал

РБПО – разработка безопасного программного обеспечения

PostgresPro

01. Соответствие стандартам и нормам

ГОСТ Р 56939-2024
Приказ ФСТЭК России от 01.12.2023 №240 (в ред. от 30.06.2025 № 230)

02. Единая утвержденная методология

Руководство по безопасной разработке.
Регламенты по процессам РБПО

03. Интеграция в культуру и инструменты

CI/CD, SAST, SCA, AV, Git, Proxy, управление задачами и проектами

PostgresPro

Раздел 4

Общие требования к разработке безопасного ПО

Общие требования

Безопасная среда разработки

Пункт 4.13

Защита критичной информации

Пункт 4.17

Вовлеченность руководства. Ресурсы

Пункт 4.5

Системный подход

ГОСТ Р ИСО/МЭК 12207-2010

Пункт 4.2–4.3

Орг&Тех меры

МЕРЫ ЗАЩИТЫ В ГИС.
МЕТОДИКА ВУ И НДВ

Пункт 4.6

PostgresPro

А у нас дедлайны и релизы

Как объяснить о важности РБПО и заинтересовать программистов

+100 к карме и чистый код

Уходит рутина

Инструменты работают – программиста не дергают

Прозрачность

Чёткие процессы и распределённая ответственность

Чистый код

Безопасно = аккуратно

Экономия времени

Отдых по выходным

Карьерный рост

Безопасный код – база. + 100 к карме, карьере и зарплатной вилке

PostgresPro

Видимо, измеримо, рассказано

Лайфхаки с пройденного аудита

Всего 10 очных встреч, остальное — удаленно

PostgresPro

1. Организационная встреча

Знакомство команд: разработчик ↔ аудитор

Вы презентуете: компания, продукты, оргструктура, ответственные роли

2. Согласование графика

2–3 встречи в неделю, процессы миксом

3. Перерыв — 1 неделя

Аудиторы изучают:

- Руководство по безопасной разработке
- Политику ИБ (артефакт ГОСТ Р 56939-2016)
- Полноту предоставленных артефактов

4. Технические проверки

Встречи по процессам

Артефакты на старте

- Презентация о компании и продуктовой линейке
- Схема организационной структуры компании
- Штатное расписание с указанием вакансий
- Доступ в защищенное хранилище с артефактами реализации процессов

Дорожная карта проверок

PostgresPro

Пункт 19 приказа ФСТЭК России от 01.12.2023 N 240 в ред. от 30.06.2025 N 230

* артефакт ГОСТ Р 56939-2016

Документ, который все ищут

Пункт 5.1 приказа ФСТЭК России от 01.12.2023 N 240 в ред. от 30.06.2025 N 230

* артефакт ГОСТ Р 56939-2016

О проверках

PostgresPro

* артефакт ГОСТ Р 56939-2016

Из интересного…

PostgresPro

01. Организация встреч

02. Фиксация результатов

03. Регламенты vs живая система

04. Визуализация – ключ к пониманию

05. Прослеживаемость устранения ошибок

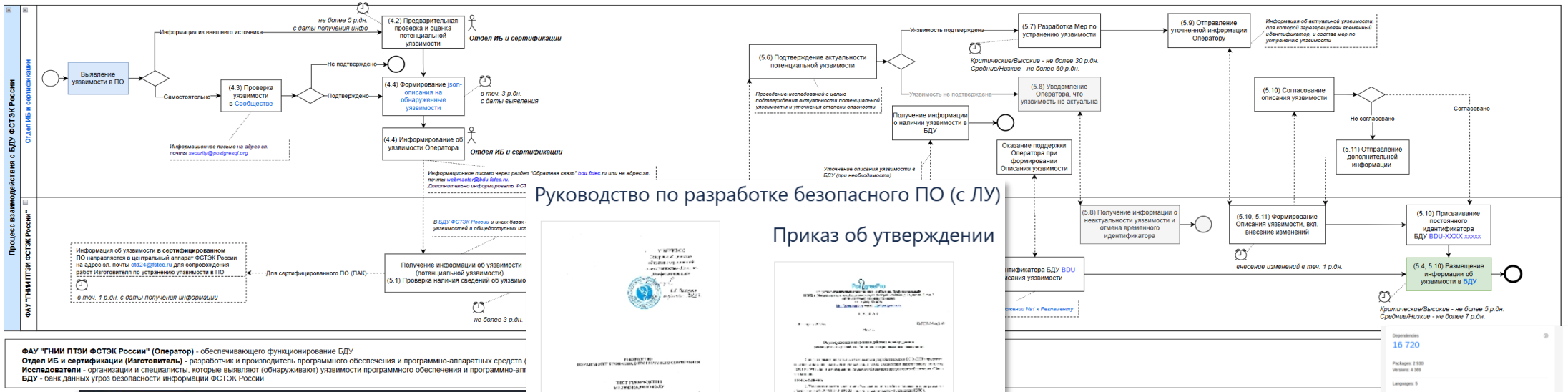
06. Гибкость в описании процессов

07. Следите за обновлениями регулятора

08. IDEF0. РБПО.РФ

Наши красивые скриншоты

PostgresPro

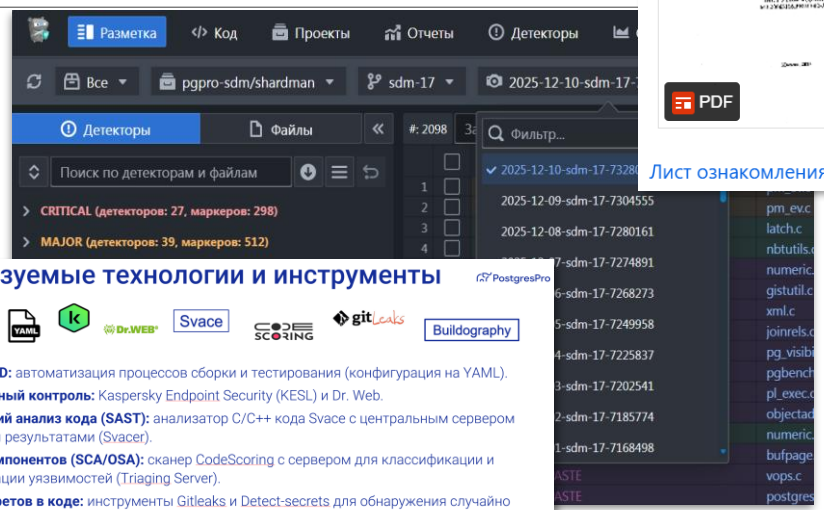


ФАУ "ГНИИ ПТЗИ ФСТЭК России" (Оператор) - обеспечивающего функционирование БДУ
Отдел ИБ и сертификации (Изготовитель) - разработчик и производитель программного обеспечения и программно-аппаратных средств (
Исследователи - организации и специалисты, которые выявляют (обнаруживают) уязвимости программного обеспечения и программно-апп
БДУ - банк данных угроз безопасности информации ФСТЭК России

Руководство по разработке безопасного ПО (с ЛУ)

Приказ об утверждении

Лист ознакомления в И



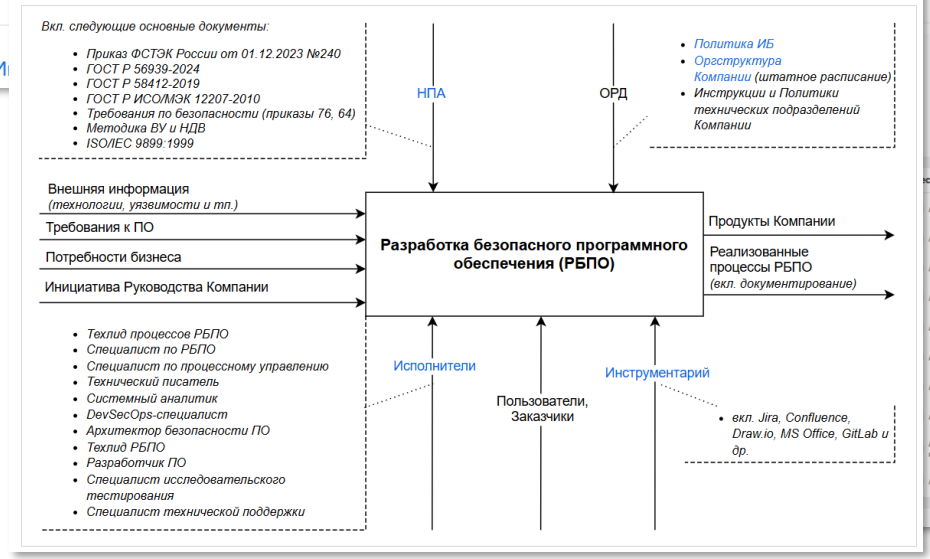
Используемые технологии и инструменты

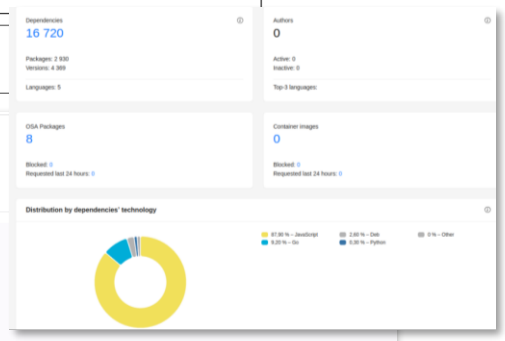
PostgresPro

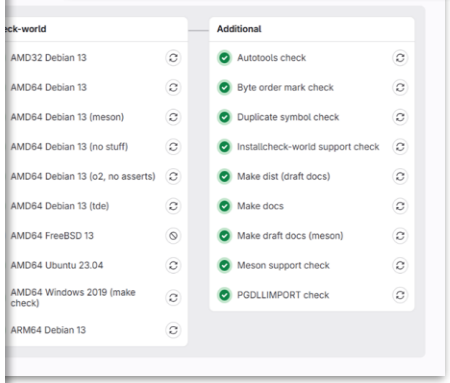
GitLab CI · YAML · Kaspersky · Dr.WEB · Svace · CODE SCORING · gitLeaks · Buildography

1. **GitLab CI/CD:** автоматизация процессов сборки и тестирования (конфигурация на YAML).
2. **Антивирусный контроль:** Kaspersky Endpoint Security (KESL) и Dr. Web.
3. **Статический анализ кода (SAST):** анализатор C/C++ кода Svace с центральным сервером управления результатами (Svacer).
4. **Анализ компонентов (SCA/OSA):** сканер CodeScoring с сервером для классификации и приоритизации уязвимостей (Triaging Server).
5. **Поиск секретов в коде:** инструменты Gitleaks и Detect-secrets для обнаружения случайно закоммиченных ключей, паролей и т.д.
6. **Идентификация артефактов сборки:** инструмент Buildography для анализа состава и происхождения сборочных зависимостей.
7. **Обнаружение protestware:** кастомный скрипт для поиска в исходном коде признаков вредоносной функциональности, связанной с протестной активностью.
8. **и другие.**

Схема IDEF0 процесса РБПО







PostgresPro

Спасибо за внимание!