PostgresPro

Postgres Professional: путь от SDL к сертификации РБПО

Попов Валерий Викторович

Шаплов Николай Николаевич

О КОМПАНИИ

Postgres Pro – российский разработчик систем управления базами данных на основе PostgreSQL.

9 лет
на рынке с 2015 г.

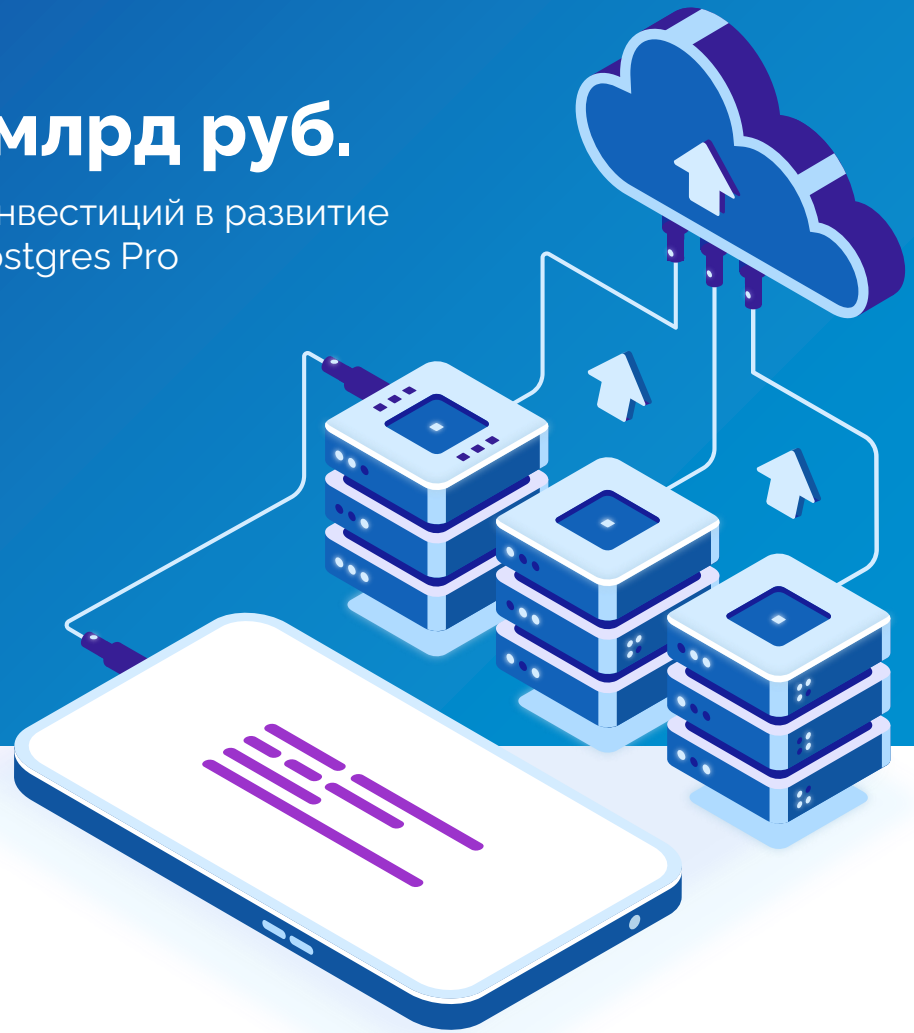
>20 лет
опыта в разработке PostgreSQL

>1,7 млрд руб.
объем инвестиций в развитие СУБД Postgres Pro

>250 чел.
штат компании

включая ведущих разработчиков и **коммитеров**

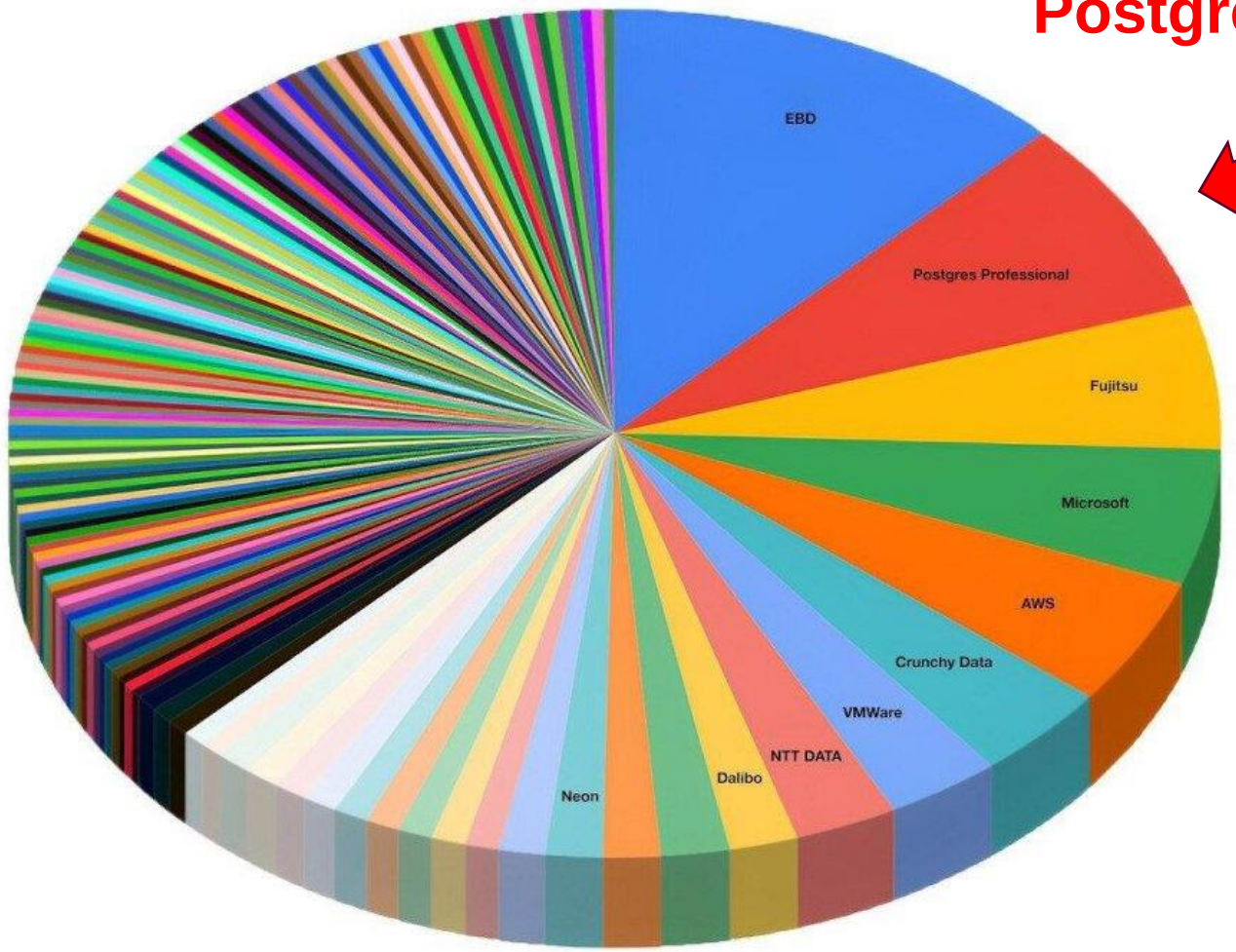
>100 патчей
направляют сотрудники компании ежегодно в международное сообщество PostgreSQL



Рейтинг контрибьютеров в PostgreSQL по данным Enterprise DB

PostgresPro

Postgres Professional



https://www.enterprisedb.com/blog/importance-of-giving-back-to-postgresql

EDB Postgres Professional Fujitsu Microsoft AWS Crunchy Data VMWare NTT DATA Dalibo Timescale HighGo Neon Cybertec Adjust
Credativ Google Kontur Materialize NTT Red Hat SRA OSS Yugabyte Aiven Instaclustr Loxodata pganalyze PostgreSQL Experts
AD Parts Analytics Engines Anastigmatix Apple Arcion Labs Arenadata Atos Avaya Axians NL Bank of China BCL Betsys Betterment
Bigbank Blacksmith Applications Braintree Caesars Digital Capital Rx Capsico Health CdC Citus Data Clearco Cockroach Labs Code Synthesis Tools
Codice Lieve Cofano Software Solutions Coinbase Conova Communications GmbH CrateDB CRSCube Data Egret dbi services Deutsche Telecom Dext
DockYard Doctolib DuckDB Labs EdgeDB End Point Corp Entelect EPAM Systems Fivetran Forest Management Institute Garner Gentoo
GLS Bank GTT HeteroDB HP IBM ILande Illuminated Computing Index Instructure Intel Intellasoft Intezer JackDB Jampp 58 more

СУБД POSTGRES PRO

Standard

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

Enterprise

Наиболее полнофункциональная СУБД с высокой производительностью и масштабируемостью

Shardman Сделано в 2023

Распределенная СУБД, предоставляющая строгие гарантии целостности данных

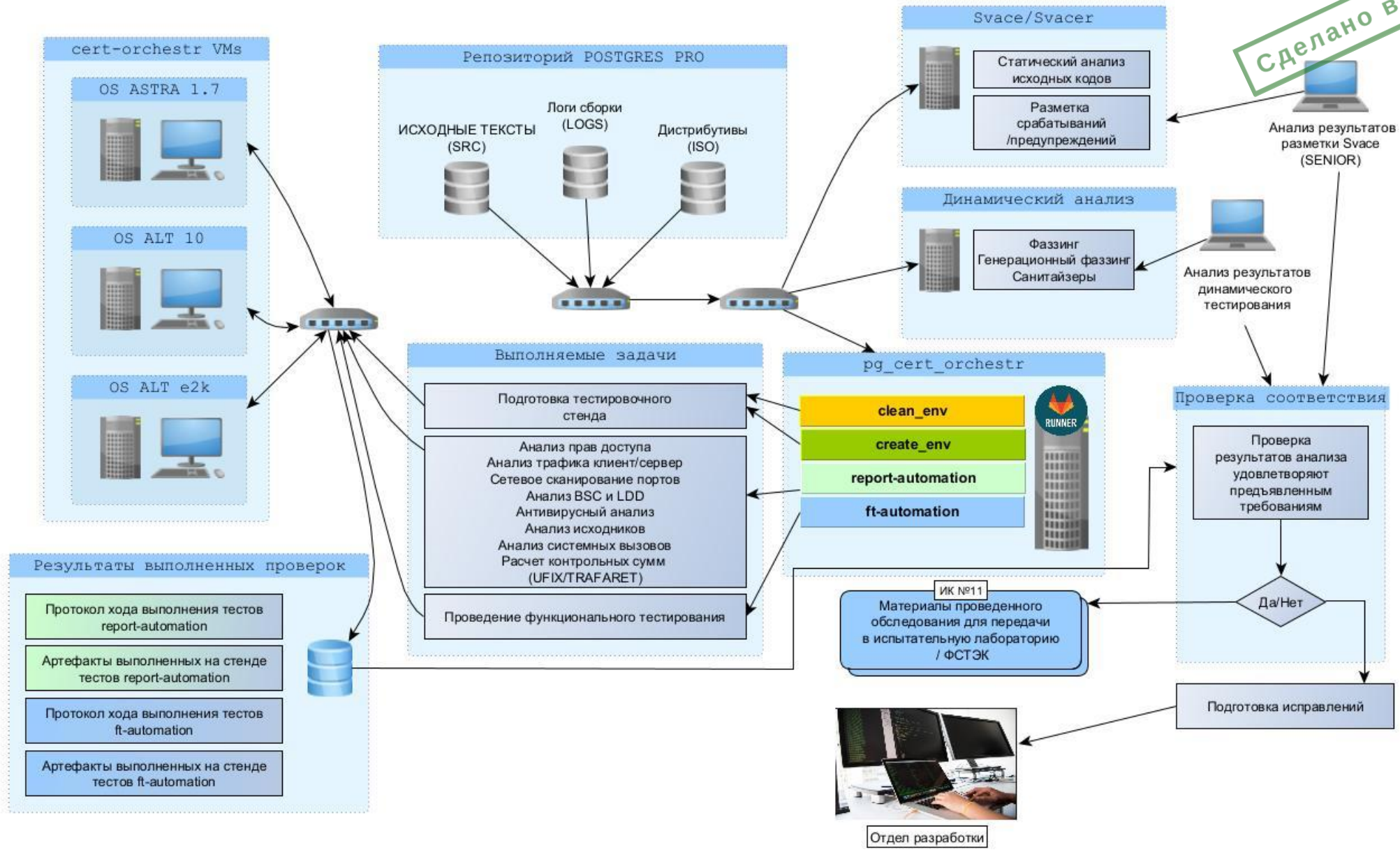
Certified

Сертифицированные ФСТЭК России версии Standard, Enterprise и Shardman. Требования к СУБД (4), УД(4)

ПРОЦЕСС ВЫПУСКА ОБНОВЛЕНИЙ

PostgresPro

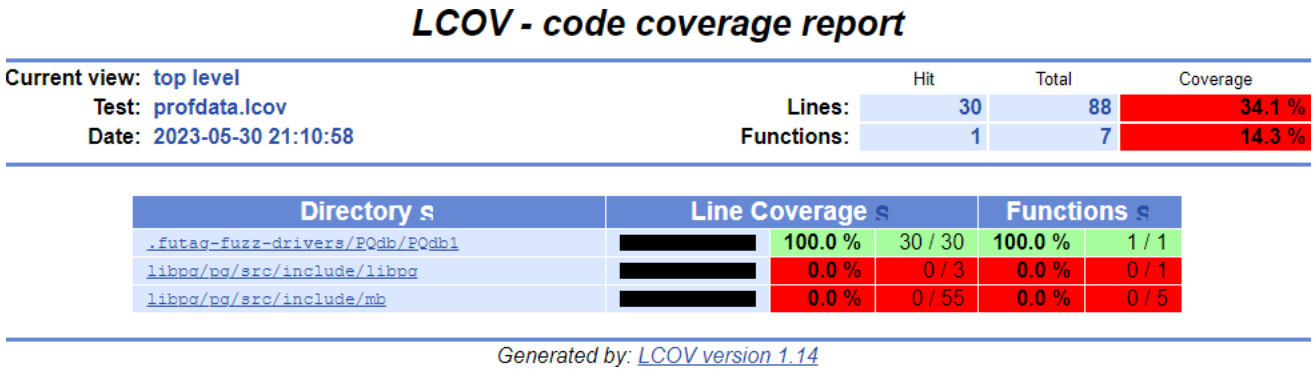
Сделано в 2023



Элемент проверки новых релизов (ИК)
Динамический анализ кода (фаззинг)

PostgresPro

- CRUSHER, SYDR-FUZZ, AFL++
- ГЕНЕРАЦИОННЫЙ ФАЗЗИНГ Sqlancer и Squirrel
- ФАЗЗИНГ СЕТЕВОГО ПРОТОКОЛА (libpq)
- ФАЗЗИНГ input-функций типов данных (28 типов: jsonb, int, line, varchar,…)
- ФАЗЗИНГ ОПЕРАЦИЙ НАД ТИПАМИ (128 операций: Structure Aware Fuzzing)
- FUTAG: автоматическая генерация целей для libpq

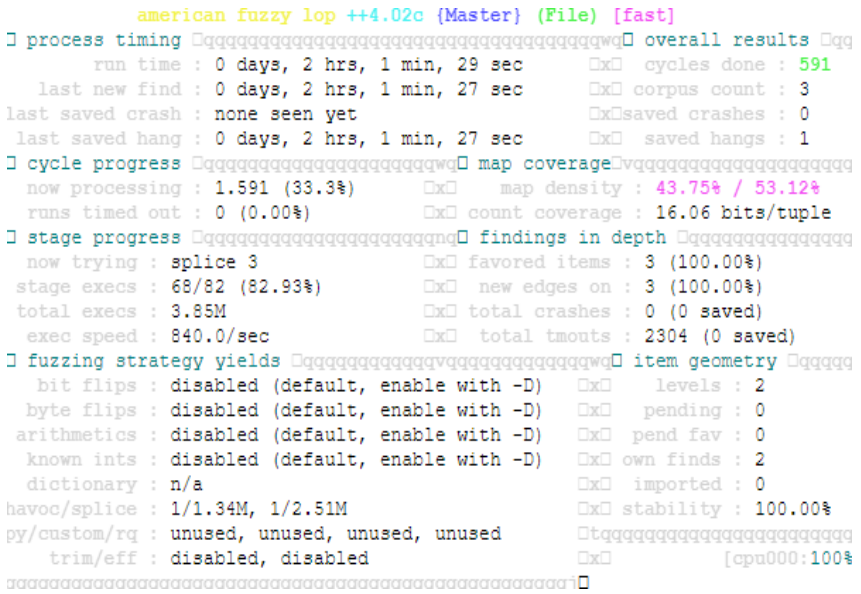


LCOV - code coverage report

Current view:	top level		Hit	Total	Coverage
Test:	profdata.lcov	Lines:	30	88	34.1 %
Date:	2023-05-30 21:10:58	Functions:	1	7	14.3 %

Directory	Line Coverage		Functions	
.futag-fuzz-drivers/PQdb/PQdb1	100.0 %	30 / 30	100.0 %	1 / 1
libpq/pg/src/include/libpq	0.0 %	0 / 3	0.0 %	0 / 1
libpq/pg/src/include/mb	0.0 %	0 / 55	0.0 %	0 / 5

Generated by: LCOV version 1.14



ФАЗЗИНГ СЕТЕВОГО ПРОТОКОЛА

PostgresPro

Эмулирование сетевого взаимодействия

Переопределение системных функций сетевого стека. Postgres работает в однопроцессном режиме, но вместо сети общается с фаззером.

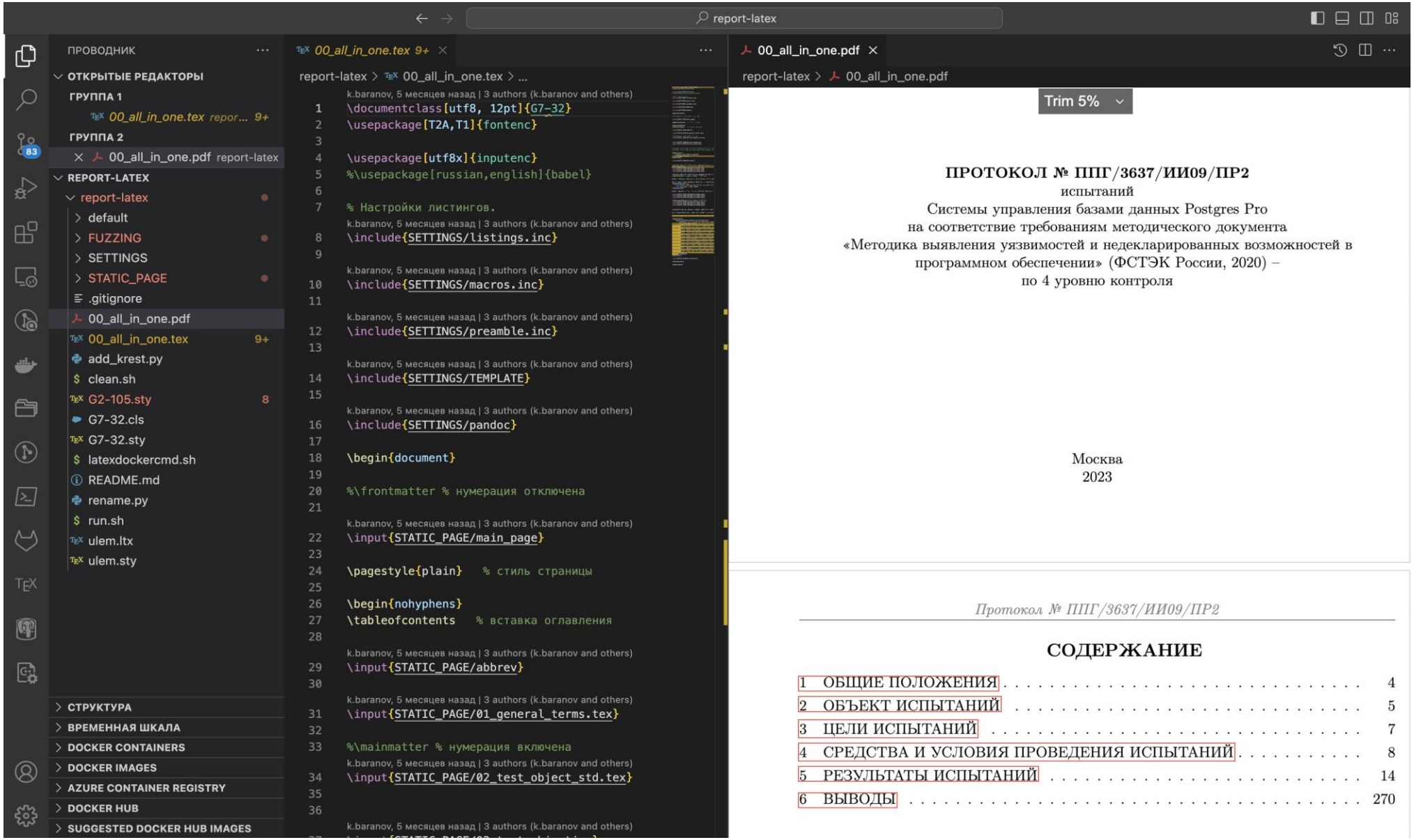
Фаззим стартовый пакет 1 (handshake) и стартовый пакет 2 – с паролем

Сделано в 2023

FUTAG

Автоматически выделены и были протестированы все функции libpq

Элемент проверки новых релизов (ИК)
Подготовка отчётных материалов (Протоколы)



PostgresPro

Фаззинг: Системный подход

(или куда подевалось время)

Фаззить надо так, чтобы это было легко и привычно, как «почистить зубы»

Система автоматизации

Фаззинг — большое количество очень похожих действий, отличающихся большим количеством мелких нюансов.

- Обычные ci-скрипты не очень удобно;
- Избегаем дублирования кода;
- Грубая нюансировка — конфиги;
- Кастомное поведение удобно реализовывать через систему наследования ООП.

- **Поверхность патча**
- **Простота портирования**

Новые версии исследуемой программы выходят регулярно. Важно не тратить много времени на портирование фаззинг-врезок и фаззинг-модулей.

PostgresPro

- **Единый каталог целей**
- **Простота добавления цели**

- Если у вас нет единой точки хранения информации о запускаемых целях, списки неизбежно разъедутся и наступит хаос;
- Добавление новой цели должно быть рутинной процедурой, потребляющей минимум ресурсов.

Сделано в 2023

In Progress...

PostgresPro

• Сводные таблицы результатов
• Простота воспроизведения

- Что там нафаззилось - интересно смотреть в первый раз. На десятый не интересно совсем. Чтобы не пропустить важные результаты, отчет для инженера должен быть простым, содержательным и наглядным.
- Для срабатываний:
  - Собрать максимум отладочной информации автоматически
  - Сделать напоминалку как запускать руками
  - Как добиться аналогичного эффекта на большом postgres’е (SQL, netcat)

Процедура передачи бага

Найденный баг должен быть праздником для фаззингиста. Если приходится биться за то, чтобы найденный баг взяли в работу, если багу никто не рад, фаззингист не захочет ничего находить.

Протестировать
СУБД Postgres Pro:

117036, Москва, ул. Дмитрия Ульянова, 7А

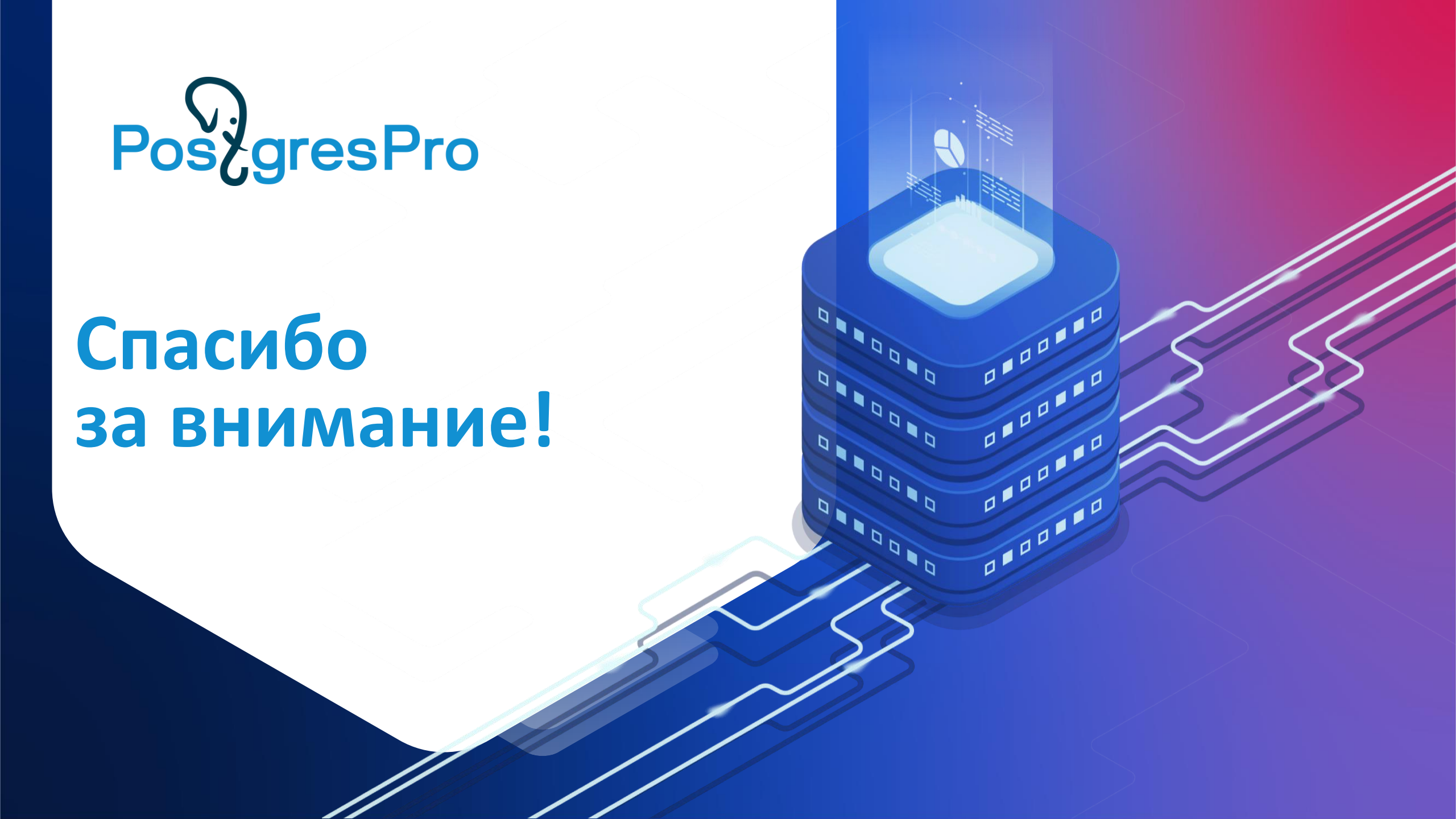
8 (495) 150-06-91

sales@postgrespro.ru

postgrespro.ru

PostgresPro

Спасибо за внимание!



PostgresPro

Q&A