



Создание защищённых систем на основе PostgreSQL Pro и Кристо БД

#защитаинформации
#импортозамещение
#системауправлениябазамиданных
#переходныйпериод
#управлениебазамиданных
#шифрованиеинформации
#сжатиеданныхнауровнеблоков
#высокаяпроизводительность
#отечественноепо

PROFESSIONAL
Postgres

Аладдин

О чём мы сегодня расскажем!

План мероприятия

- 🎯 Платформа СУБД PostgresPro
- 🎯 Система защиты информации Кристо БД
- 🎯 Железные аргументы в пользу защиты информации
- 🎯 Жизненный цикл системы с точки зрения СУБД и СЗИ
- 🎯 Критерии выбора платформы СУБД и СЗИ
- 🎯 Что такое защищённая база данных?
- 🎯 Импортзамещение и переход на СУБД PostgresPro
- 🎯 Принципы безопасного перехода из старой в новую СУБД



СУБД PostgresPro

Краткое представление платформы

Postgres Pro – это наиболее динамично развивающаяся отечественная система управления базами данных. Разработана на платформе открытой и востребованной СУБД PostgreSQL

1. Postgres Pro = PostgreSQL + корпоративные функции
2. Производительность
3. Надёжность
4. Безопасность
5. Объём доработок более 120 человеко-лет



Крипто БД

Система защиты информации в СУБД

Крипто БД – это средство защиты конфиденциальности информации обрабатываемой в базе данных PostgreSQL.

Надёжная защита информации в СУБД

- Сертифицированное СКЗИ для защиты данных в базе;
- Возможность шифрования отдельных столбцов;
- Применение метода "прозрачного" шифрования;

Разграничение прав доступа пользователей

- Реализация двухфакторной аутентификации;

Аудит и мониторинг действий пользователей

- Ведение учёта доступа к данным в защищённом журнале.



ИНТЕРЕСНЫЙ ВОПРОС

Мнения экспертов мероприятия

1. Зачем вообще нужно защищать информацию в СУБД?

Возражения, страхи и предубеждения

- “Мы не обрабатываем великие секреты в СУБД”;
- “Моя система очень сложная”;
- “Защита нарушит стабильность системы”;
- “СУБД чёрный ящик, доступ только у разработчиков”.



ИНТЕРЕСНЫЙ ВОПРОС

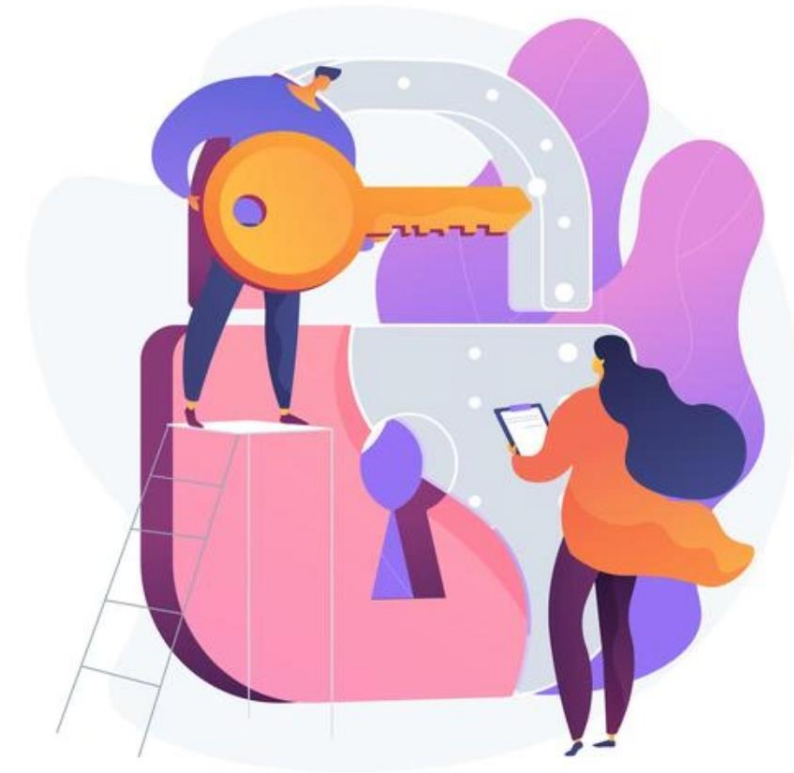
Ответы и мнения экспертов мероприятия

1. Зачем вообще нужно защищать информацию в СУБД?

Железные аргументы в пользу защиты информации

- Масштабные утечки реализуются именно в СУБД;
- Любой компании необходимо разграничение доступа;
- Необходимость защиты от Администратора СУБД;
- Выполнение требований ФСТЭК (ГИС, ПДн, КИИ..).

Аксиома: Если деятельность организации существенно зависит от обрабатываемой ею информации (считай от своих ИС и СУБД), то избегать выполнение требований государства в области защиты информации просто опасно. Результатом бездействия может стать приостановка деятельности или существенные штрафы и конечно значительный репутационные ущерб организации.



ИНТЕРЕСНЫЙ ВОПРОС

Ответы и мнения экспертов мероприятия

2. Как соотносить защищённую базу данных и ЖЦ?

ЖЦ: Это совокупность стадий жизнедеятельности информационной системы. Понятие помогает структурировать подходы к построению и эксплуатации информационных систем.

Жизненный цикл информационной системы

- формирование требований (концепции);
- проектирование технических решений;
- внедрение (ввод системы в эксплуатацию);
- эксплуатация (сопровождение проекта);
- вывод из эксплуатации.



ИНТЕРЕСНЫЙ ВОПРОС

Ответы и мнения экспертов мероприятия

3. Критерии выбора платформы СУБД и СЗИ

Свойства продукта влияющие на выбор базы данных

- Перспективность использования (политические, технологические риски);
- Распространённость продукта;
- Совокупный опыты рынка в применении платформы;
- Соответствие стандартам;
- Наличие продукта в реестре отечественного ПО;
- Профессиональная техническая поддержка;
- Соответствие Требованиям ФСТЭК России



ИМПОРТОЗАМЕЩЕНИЕ

Распространённые заблуждения

Существующие ИТ-системы



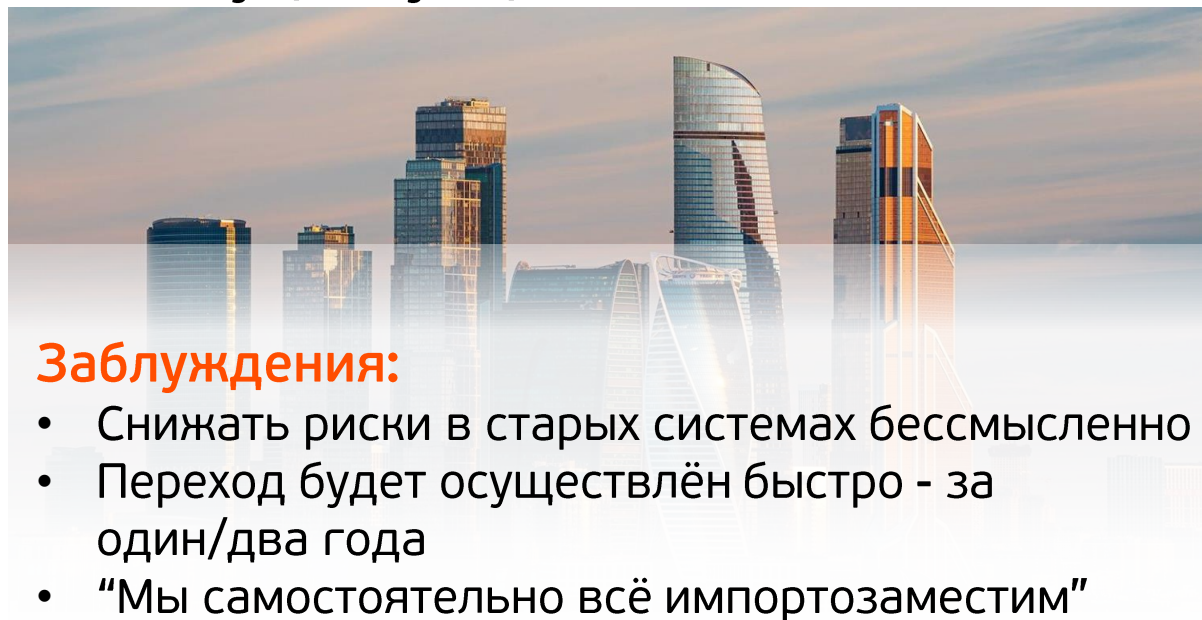
Импортозамещение ИТ-систем



ИМПОРТОЗАМЕЩЕНИЕ

Распространённые заблуждения

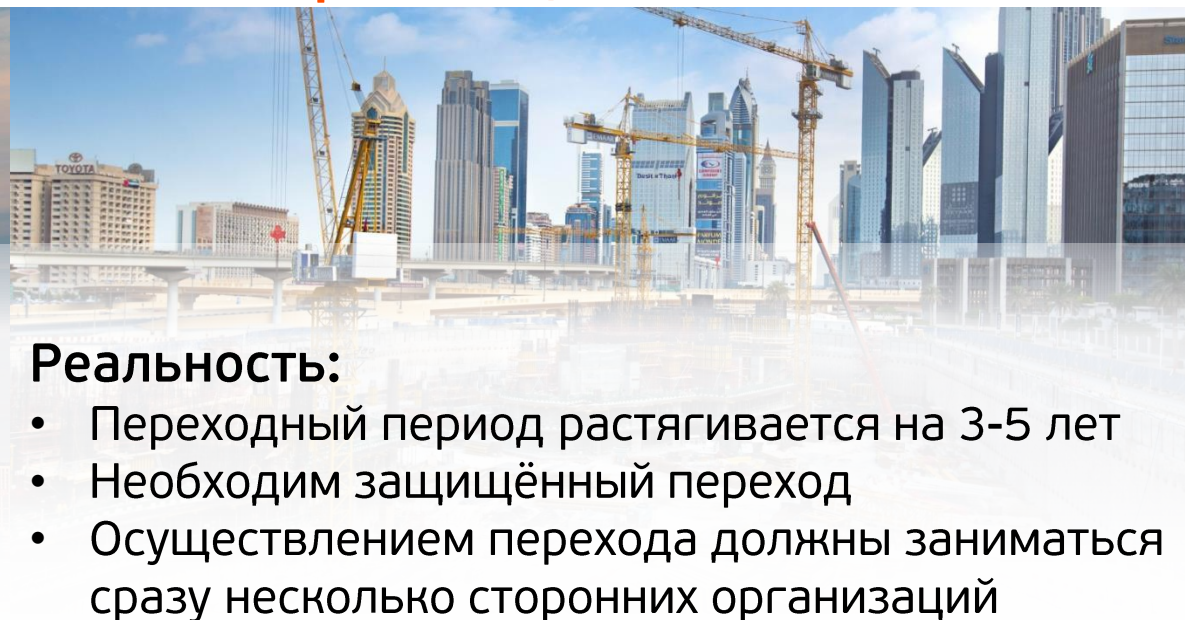
Существующие ИТ-системы



Заблуждения:

- Снижать риски в старых системах бессмысленно
- Переход будет осуществлён быстро - за один/два года
- “Мы самостоятельно всё импортозаместим”

Импортозамещение ИТ-систем



Реальность:

- Переходный период растягивается на 3-5 лет
- Необходим защищённый переход
- Осуществлением перехода должны заниматься сразу несколько сторонних организаций

ИМПОРТОЗАМЕЩЕНИЕ

Безопасность данных в переходном периоде

Питательная среда для угроз ИБ

- Перенос данных из “старой” СУБД в новую, не защищённую;
- Бесконтрольное участие сторонних организаций;
- Большая длительность переходного периода;
- небезопасный вывод “старой” СУБД из эксплуатации.

Как следствие:

- Отсутствие контроля доступа к переносимым данным;
- Архитектура новой системы не учитывает требования ИБ;
- Отложенные проблемы производительности СУБД;
- Сверхвысокие риски утечки больших объёмов информации.



ИМПОРТОЗАМЕЩЕНИЕ – БАЗОВЫЙ ПЛАН

Практика поэтапной реализации мероприятий



Адаптация

Первичный переход на отечественное прикладное ПО с сохранением на компьютерах ОС Windows



Интеграция

Формирование инфраструктуры переходного периода. Создание гибридных систем управления Win/Linux



Полный переход

Полноценный ввод в эксплуатацию бизнес-приложений и электронных сервисов на отечественном ПО, ОС и СУБД

ИНТЕРЕСНЫЙ ВОПРОС

Ответы и мнения экспертов мероприятия

4. Как осуществить переход на СУБД PostgresPro?

Факторы успешного перехода на новую платформу СУБД PostgresPro

- СУБД - центральное и ключевое место любой информационной системы;
- Миграция СУБД - один из ключевых этапов плана импортозамещения;
- Лучшая миграция - это реинжиниринг для полноценного использования возможностей СУБД;
- Продуманный план миграции, заблаговременная оценка её стоимости и затрат времени;
- Организация постоянного тестирования переносимой системы;
- Учёт того, что перенос данных существенно проще переноса функциональности.



ИНТЕРЕСНЫЙ ВОПРОС

Ответы и мнения экспертов мероприятия

5. Как решить задачи по защите данных при переходе?

Безопасная база данных помогает снять основные риски – наш подход:

- Необходимо защитить исходную СУБД
 - это повысит контроль доступа к ценной информации в старой информационной системе
- Необходимо предусмотреть и реализовать защиту в новой СУБД
 - это позволит изначально предусмотреть оптимальные характеристики производительности, “работающую” ролевую модель, информационную модель системы и т.п.
- Необходимо разработать меры контроля процедуры миграции информации из старой в новую СУБД



ИНТЕРЕСНЫЙ ВОПРОС

Ответы и мнения экспертов мероприятия

Рабочие кейсы защищённой СУБД?

#1: Предотвращение утечек

- Защита информации в СУБД при взломах информационных систем

#2: Защита от “админа”

- Предотвращение доступа со стороны привилегированных пользователей

#3: Контроль доступа к информации

- Разграничение прав доступа пользователей к защищаемой информации

#4: Защита архивов

- Защита резервных копий и архивов СУБД

#5: Маскирование данных

- Маскирование и деперсонализация информации в СУБД

#6: Надёжное уничтожение данных

- Предотвращение возможности восстановления удалённой информации

#7: Независимый аудит

- Аудит фактов доступа пользователей к защищаемой информации



ИТОГИ

Выводы экспертов

Импортозамещение

- Практическое выполнение задач перехода это уже не насущная необходимость – это жёсткое требование времени.

Защищённая СУБД

- Это органичное, адекватное и своевременное техническое решение на базе платформ СУБД PostgresPro и СЗИ Кripto БД.

Применимость защищённой СУБД

- Защищённая база данных обладает максимальной применимостью при решении целого ряда задач информационной безопасности.



КОММУНИКАЦИИ

Контактная информация докладчиков

Суховей Д.В.

+7(916) 550-11-78

d.sukhovey@aladdin.ru

www.aladdin.ru



Панченко И.Е.

+7(910) 433-98-46

i.panchenko@postgrespro.ru

www.postgrespro.ru



Додохов А.Л.

+7(903) 585-94-34

a.dodokhov@aladdin.ru

www.aladdin.ru

