РАСШИРЕННЫЕ ВОЗМОЖНОСТИ АУДИТА В СУБД «PostgreSQL» В ДИСТРИБУТИВЕ «Astra Linux Special Edition»

Дмитрий Воронин
ОАО «НПО РусБИТех»

ОПЕРАЦИОННАЯ СИСТЕМА СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ "Astra Linux Special Edition"

УЧАСТНИКИ ПРОЕКТА

- ОАО «НПО РусБИТех»
- Академия ФСБ
- ИСП РАН

СЗИ

запатентованы

СЕРТИФИЦИРОВАНА

- ФСБ России
- Минобороны России
- ФСТЭК Росии

ПОДДЕРЖИВАЕМОЕ ОБОРУДОВАНИЕ

Серверы

Рабочие станции

Моноблоки

Ноутбуки

Планшеты

Мейнфреймы

Банкоматы

Защищенные СВТ

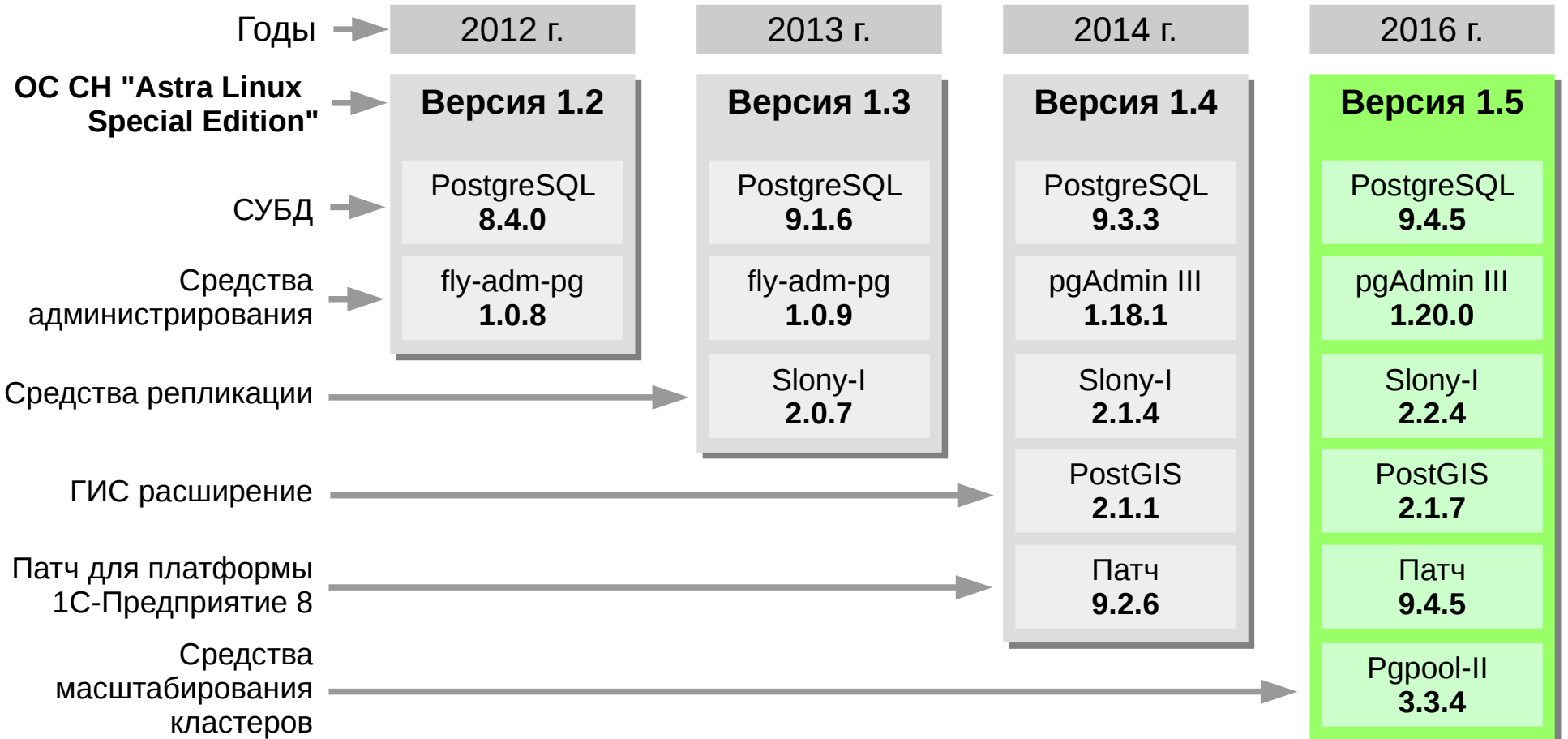
Смартфоны

Периферийное оборудование

Встраиваемые СВТ

Сетевое оборудование

РАЗВИТИЕ СРЕДСТВ СУБД «PostgreSQL» В СОСТАВЕ ОС СН «Astra Linux Special Edition»



ТРЕБОВАНИЯ НОРМАТИВНЫХ ДОКУМЕНТОВ К ПОДСИСТЕМЕ РЕГИСТРАЦИИ И УЧЕТА СОБЫТИЙ

Должны регистрироваться следующие события:

- Идентификация и аутентификация
- Запрос на доступ к объекту
- Создание и уничтожение объекта
- Изменения правил разграничения доступа

Параметры регистрации
Дата и время
Субъект (имя или идентификатор)
Объект
Тип доступа
Результат запроса на доступ

РЕАЛИЗАЦИЯ ТРЕБОВАНИЙ К ПОДСИСТЕМЕ РЕГИСТРАЦИИ И УЧЕТА СОБЫТИЙ

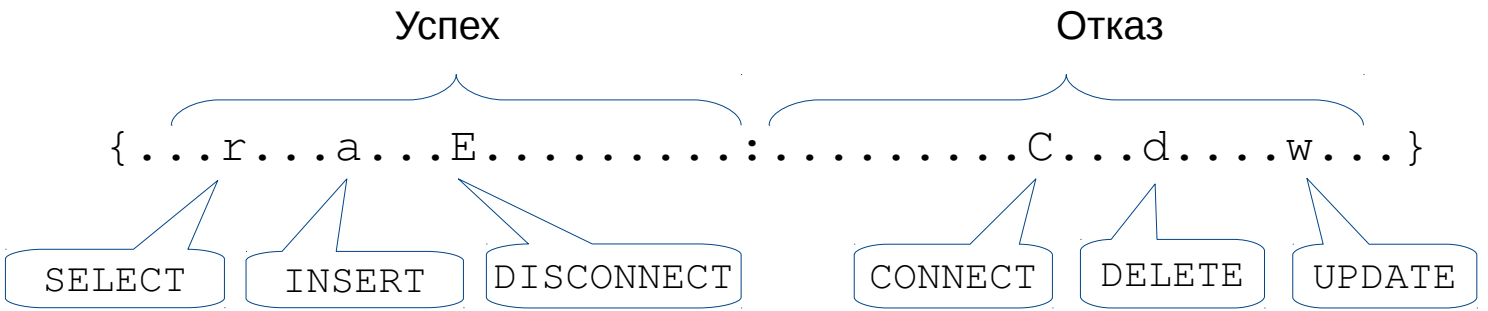
Базовый PostgreSQL

- регистрация входа и выхода пользователей
- регистрация отказа в доступе к защищаемому ресурсу

- регистрация создания и уничтожения объектов
- регистрация изменения правил разграничения доступа
- регистрация успешного доступа к защищаемому ресурсу

Доработанный PostgreSQL

- Регистрируемые события задаются маской аудита



- Порядок загрузки маски аудита

Пользователь	База данных
user1	testdb1
user1	ALL
ALL	testdb1
ALL	ALL

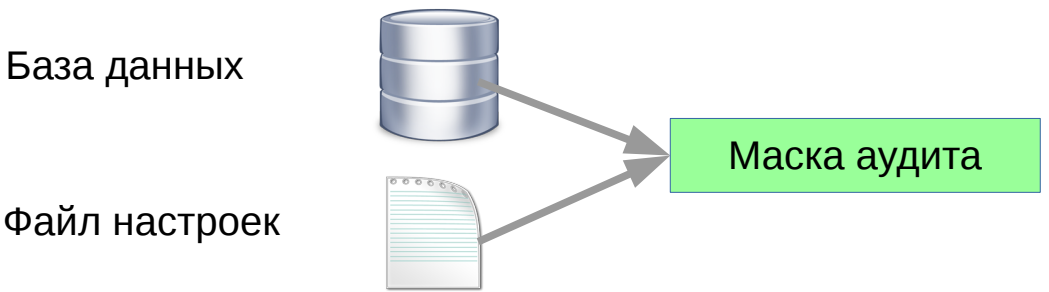
→ Маска аудита

ОСОБЕННОСТИ РЕАЛИЗАЦИИ

- Вывод сообщений в специальный журнал безопасности операционной системы
- Изменение маски аудита с помощью языка SQL

```
ALTER ROLE testuser
    IN DATABASE testdb SET ac_session_audit TO '{ace:ace}';
ALTER ROLE testuser
    IN DATABASE testdb RESET ac_session_audit;
```

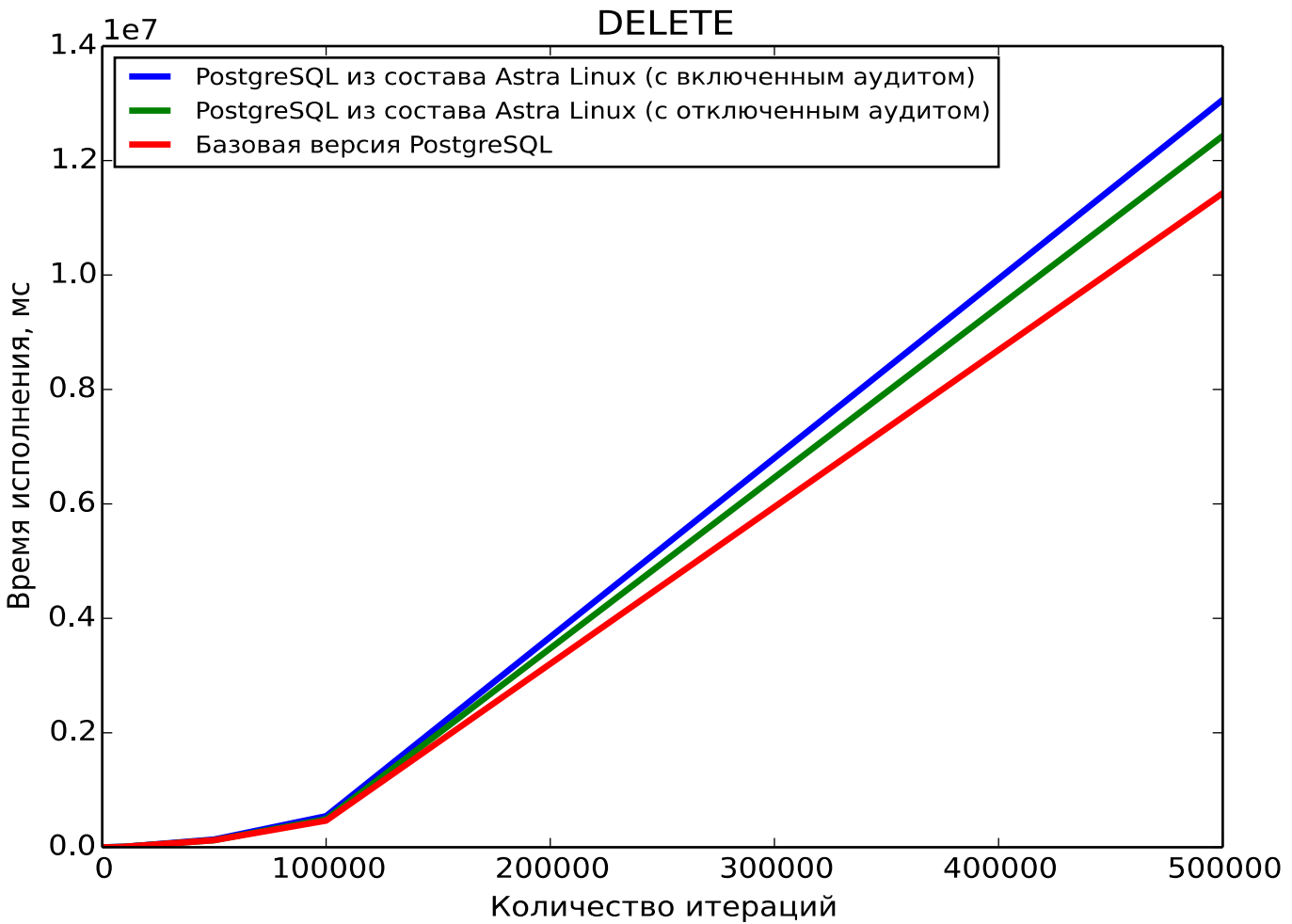
- Сочетание внешнего и внутреннего хранения настроек аудита



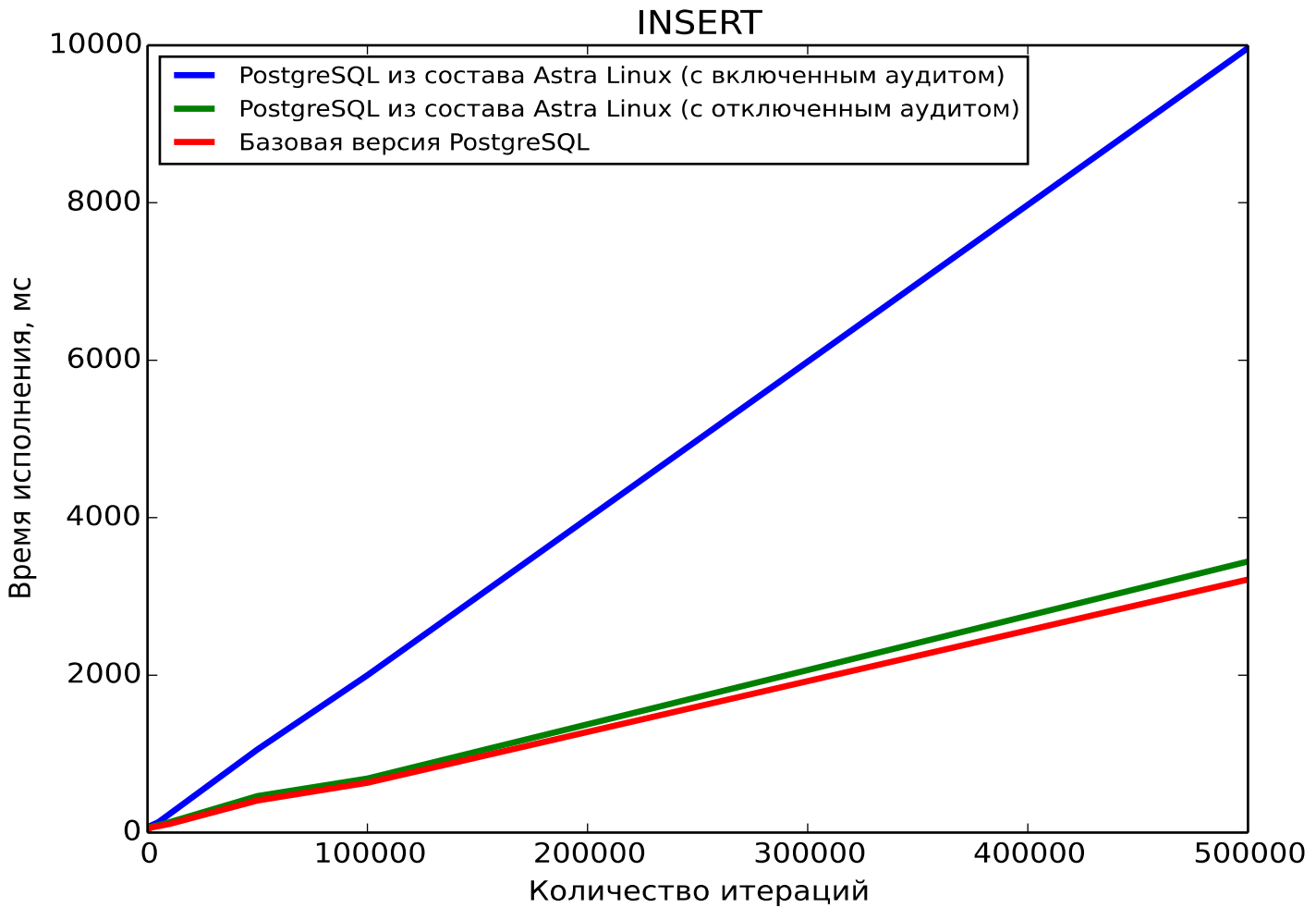
ФАКТОРЫ, ВЛИЯЮЩИЕ НА БЫСТРОДЕЙСТВИЕ

- Формирование параметров протоколирования для сессии (1 раз)
- Фиксация события по маске при доступе
- Получение необходимой информации для формирования сообщения (при доступе)
- Запись в системный журнал PostgreSQL (при доступе)
- Запись в специальный журнал безопасности операционной системы

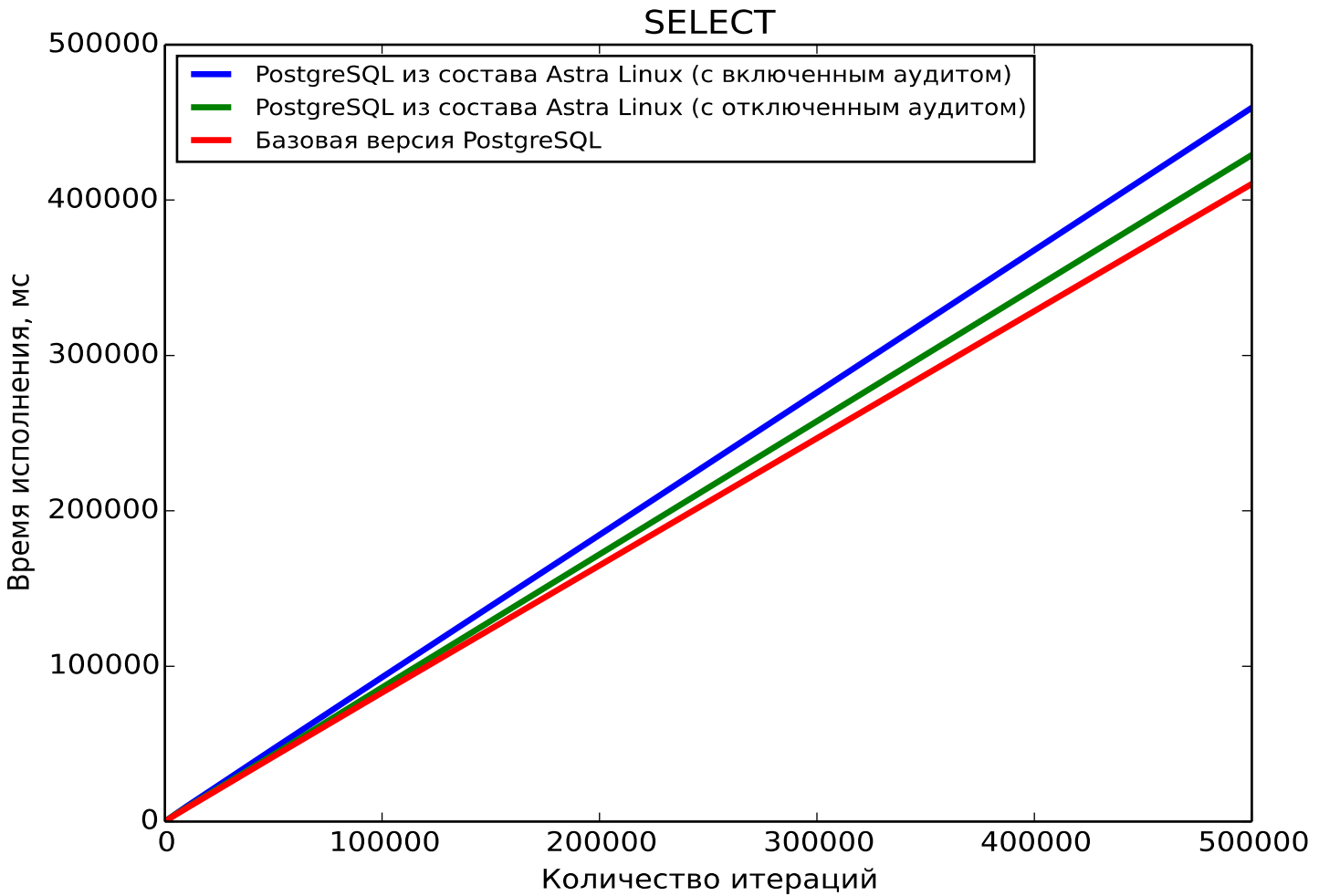
ВЛИЯНИЕ ПОДСИСТЕМЫ РЕГИСТРАЦИИ СОБЫТИЙ НА БЫСТРОДЕЙСТВИЕ СУБД «PostgreSQL»: DELETE



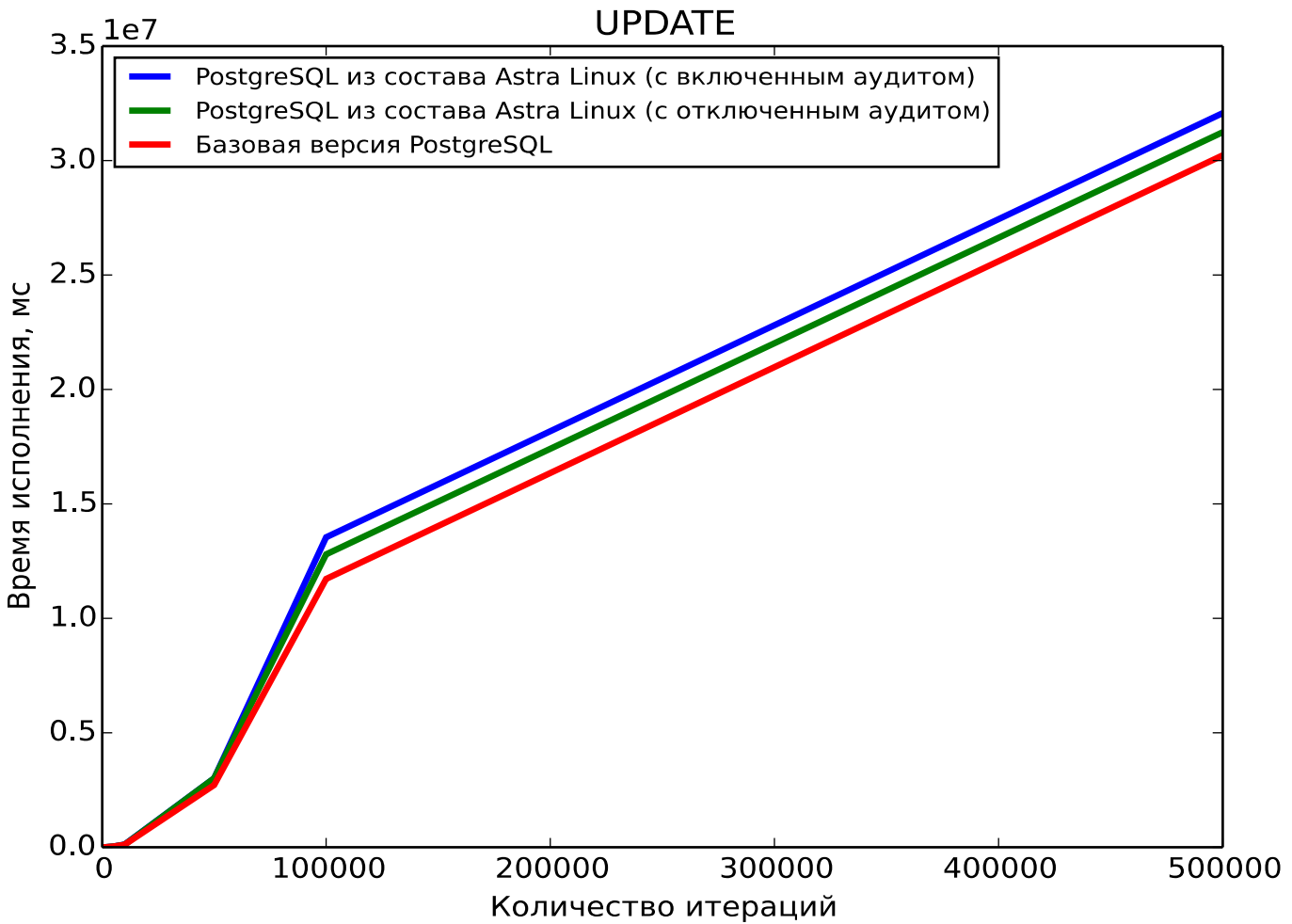
ВЛИЯНИЕ ПОДСИСТЕМЫ РЕГИСТРАЦИИ СОБЫТИЙ НА БЫСТРОДЕЙСТВИЕ СУБД «PostgreSQL»: INSERT



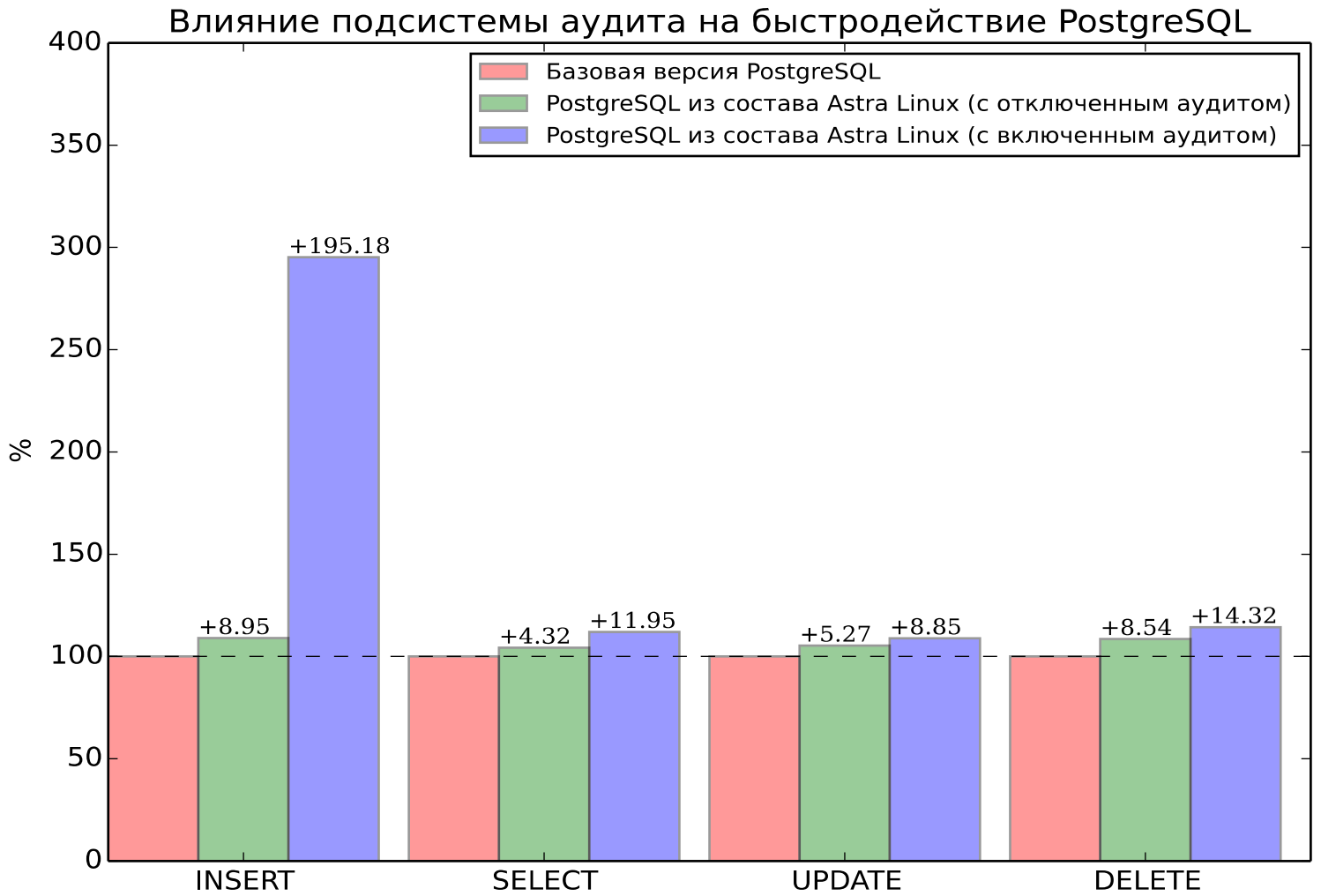
ВЛИЯНИЕ ПОДСИСТЕМЫ РЕГИСТРАЦИИ СОБЫТИЙ НА БЫСТРОДЕЙСТВИЕ СУБД «PostgreSQL»: SELECT



ВЛИЯНИЕ ПОДСИСТЕМЫ РЕГИСТРАЦИИ СОБЫТИЙ НА БЫСТРОДЕЙСТВИЕ СУБД «PostgreSQL»: UPDATE



ВЛИЯНИЕ ПОДСИСТЕМЫ РЕГИСТРАЦИИ СОБЫТИЙ НА БЫСТРОДЕЙСТВИЕ СУБД «PostgreSQL»



www.rusbitech.ru

СПАСИБО!

www.astralinux.ru