




СУБД PostgreSQL
ИЗ ДИСТРИБУТИВА ОПЕРАЦИОННОЙ СИСТЕМЫ
СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ
"Astra Linux Special Edition"
ДЛЯ ОБРАБОТКИ СВЕДЕНИЙ,
СОСТАВЛЯЮЩИХ ГОСУДАРСТВЕННУЮ ТАЙНУ

БЕЗОПАСНОСТЬ И БЫСТРОДЕЙСТВИЕ

Система сертификации	Номер сертификата	Дата выдачи	Срок действия
 Минобороны России	№ 1339	24.09.2010 г.	15.09.2018 г.
 ФСТЭК России	№ 2557	27.01.2012 г.	27.01.2018 г.
 ФСБ России	№ СФ/014-2234	04.10.2013 г.	04.10.2018 г.

ОС СН "Astra Linux Special Edition" сертифицирована на соответствие:

- 3 классу защищенности СВТ от НСД;
- 2 уровню контроля отсутствия НДВ.

В состав сертифицированного дистрибутива

ОС СН "Astra Linux Special Edition" 1.4

включены следующие программные средства СУБД:

- СУБД PostgreSQL 9.3.3;
- расширение PostGIS 2.1.1;
- патч для технологической платформы 1С-Предприятие 8;
- программное средство администрирования pgAdmin III 1.18.1;
- программное средство репликации Slony-I 2.1.4.

Все программные средства, включаемые в состав ОС СН "Astra Linux Special Edition" должны соответствовать требованиям нормативных документов по защите информации ФСБ, ФСТЭК и Минобороны России.

В дополнение к имеющимся средствам защиты в СУБД PostgreSQL встраиваются средства защиты информации, обеспечивающие:

- мандатное разграничение доступа;
- регистрацию событий безопасности (аудит).

Обычная СУБД PostgreSQL

Объекты и метаданные	Дискреционное разграничение доступа	Мандатное разграничение доступа
База данных	+	+
Схема	+	+
Таблица	+	+
Поле (столбец)	+	
Запись		+
Функция	+	+

Доработанная СУБД PostgreSQL

Виды данных и уровни доступа		Подразделения и категории доступа				
		Общий доступ	Отдел 1	Отдел 2	Отдел 3	Руководство
		0x0 (0000)	0x1 (0001)	0x2 (0010)	0x4 (0100)	0x8 (1000)
Государственная тайна	3	{3,0x0}	{3,0x1}	{3,0x2}	{3,0x4}	{3,0x8}
Конфиден- циальные	2	{2,0x0}	{2,0x1}	{2,0x2}	{2,0x4}	{2,0x8}
Служебная тайна	1	{1,0x0}	{1,0x1}	{1,0x2}	{1,0x4}	{1,0x8}
Общий доступ	0	{0,0x0}	{0,0x1}	{0,0x2}	{0,0x4}	{0,0x8}

Диапазон значений иерархических уровней доступа: от 0 до 255

Диапазон значений неиерархических категорий доступа: 64 двоичных разряда

Область видимости данных для пользователя с мандатной меткой {2,0x9} (1001)

Виды данных и уровни доступа		Подразделения и категории доступа				
		Общий доступ	Отдел 1	Отдел 2	Отдел 3	Руководство
		0x0 (0000)	0x1 (0001)	0x2 (0010)	0x4 (0100)	0x8 (1000)
Государственная тайна	3	{3,0x0}	{3,0x1}	{3,0x2}	{3,0x4}	{3,0x8}
Конфиденциальные	2	{2,0x0}	{2,0x1}	{2,0x2}	{2,0x4}	{2,0x8}
Служебная тайна	1	{1,0x0}	{1,0x1}	{1,0x2}	{1,0x4}	{1,0x8}
Общий доступ	0	{0,0x0}	{0,0x1}	{0,0x2}	{0,0x4}	{0,0x8}

{0,0x0} - мандатная метка минимального доступа к данным

{3,0xF} - мандатная метка максимального доступа к данным

Область видимости пользователя с мандатной меткой {3,0xF}

База данных {3,0xF} CCR = Off

Схема {3,0xF} CCR = Off

Таблица-1 {3,0xF} CCR = Off

Запись {3,0x0}

Запись {2,0x8}

Запись {1,0x0}

Запись {0,0x0}

Запись {3,0x0}

Запись {2,0x0}

Запись {1,0x0}

Запись {0,0x0}

Таблица-2 {2,0x1} CCR = On

Запись

Запись

Запись

Запись

Запись

Запись

Запись

Запись

CCR (Container clearance required) - учет мандатных атрибутов контейнера

Область видимости пользователя с мандатной меткой {3,0x0}

База данных {3,0xF} CCR = Off

Схема {3,0xF} CCR = Off

Таблица-1 {3,0xF} CCR = Off

Запись {3,0x0}

Запись {2,0x8}

Запись {1,0x0}

Запись {0,0x0}

Запись {3,0x0}

Запись {2,0x0}

Запись {1,0x0}

Запись {0,0x0}

Таблица-2 {2,0x1} CCR = On

Запись

Запись

Запись

Запись

Запись

Запись

Запись

Запись

Область видимости пользователя с мандатной меткой {2,0x9}

База данных {3,0xF} CCR = Off

Схема {3,0xF} CCR = Off

Таблица-1 {3,0xF} CCR = Off

Запись {3,0x0}

Запись {2,0x8}

Запись {1,0x0}

Запись {0,0x0}

Запись {3,0x0}

Запись {2,0x0}

Запись {1,0x0}

Запись {0,0x0}

Таблица-2 {2,0x1} CCR = On

Запись

Запись

Запись

Запись

Запись

Запись

Запись

Запись

Область видимости пользователя с мандатной меткой {2,0x8}

База данных {3,0xF} CCR = Off

Схема {3,0xF} CCR = Off

Таблица-1 {3,0xF} CCR = Off

Запись {3,0x0}

Запись {2,0x8}

Запись {1,0x0}

Запись {0,0x0}

Запись {3,0x0}

Запись {2,0x0}

Запись {1,0x0}

Запись {0,0x0}

Таблица-2 {2,0x1} CCR = On

Запись

Запись

Запись

Запись

Запись

Запись

Запись

Запись

Область видимости пользователя с мандатной меткой {2,0x1}

База данных {3,0xF} CCR = Off

Схема {3,0xF} CCR = Off

Таблица-1 {3,0xF} CCR = Off

Запись {3,0x0}

Запись {2,0x8}

Запись {1,0x0}

Запись {0,0x0}

Запись {3,0x0}

Запись {2,0x0}

Запись {1,0x0}

Запись {0,0x0}

Таблица-2 {2,0x1} CCR = On

Запись

Запись

Запись

Запись

Запись

Запись

Запись

Запись

Область видимости пользователя с мандатной меткой {0,0x0}

База данных {3,0xF} CCR = Off

Схема {3,0xF} CCR = Off

Таблица-1 {3,0xF} CCR = Off

Запись {3,0x0}

Запись {2,0x8}

Запись {1,0x0}

Запись {0,0x0}

Запись {3,0x0}

Запись {2,0x0}

Запись {1,0x0}

Запись {0,0x0}

Таблица-2 {2,0x1} CCR = On

Запись

Запись

Запись

Запись

Запись

Запись

Запись

Запись

Средства аудита доработанной СУБД PostgreSQL обеспечивают регистрацию следующих событий:

- использование идентификационного и аутентификационного механизма;
- запрос на доступ к защищаемому ресурсу;
- создание, уничтожение и изменение объектов СУБД;
- действия по изменению правил разграничения доступа.

Для каждого события регистрируется следующая информация:

- дата и время;
- объект доступа к которому применяется регистрируемое действие;
- субъект, осуществляющий регистрируемое действие;
- тип события;
- результат завершения события.

/var/log/parsec/user.mlog - Журнал безопасности

Файл Вид Фильтр Настройка Помощь

Фильтр по умолчанию

Параметры фильтра

Название: по умолчанию
Время: Последние 7 дней
Источник: настраиваемый [C]
Пользователь: postgres

Лог-файлы

kernel.mlog	1970-01-01 03:00:00	2106-02-06 15:16:00
user.mlog	2015-01-28 18:11:58	2015-01-30 20:39:07

user.mlog - по умолчанию

```

postgres [c] 'Fri Jan 30 11:14:44 2015' '/usr/lib/libparsec-cap-db-files.so.2.5.134' <27341,27330,110,116,110> [s] pgsq("Подключение", "[local]", "postgres", "postgres", 10, "postgres", 10,
postgres [c] 'Fri Jan 30 11:14:44 2015' '/usr/lib/libparsec-cap-db-files.so.2.5.134' <27341,27330,110,116,110> [s] pgsq("Отключение", "[local]", "postgres", "postgres", 10, "postgres", 10,
postgres [c] 'Fri Jan 30 11:14:44 2015' '/usr/lib/libparsec-cap-db-files.so.2.5.134' <27344,27330,110,116,110> [s] pgsq("Подключение", "[local]", "postgres", "postgres", 10, "postgres", 10,
postgres [c] 'Fri Jan 30 11:14:44 2015' '/usr/lib/libparsec-cap-db-files.so.2.5.134' <27344,27330,110,116,110> [s] pgsq("Отключение", "[local]", "postgres", "postgres", 10, "postgres", 10,
postgres [c] 'Fri Jan 30 11:14:45 2015' '/usr/lib/libparsec-cap-db-files.so.2.5.134' <27347,27330,110,116,110> [s] pgsq("Подключение", "[local]", "postgres", "postgres", 10, "postgres", 10,
postgres [c] 'Fri Jan 30 11:14:45 2015' '/usr/lib/libparsec-cap-db-files.so.2.5.134' <27347,27330,110,116,110> [s] pgsq("Отключение", "[local]", "postgres", "postgres", 10, "postgres", 10,
postgres [c] 'Fri Jan 30 11:16:11 2015' '/usr/lib/libparsec-cap-db-files.so.2.5.134' <27398,27330,110,116,110> [s] pgsq("Подключение", "[local]", "testdb", "user1", 16385, "user1", 16385,
postgres [c] 'Fri Jan 30 11:20:08 2015' '/lib/x86_64-linux-gnu/libnss_nis-2.13.so' <27471,27330,110,116,110> [f] pgsq("Подключение", "[local]", "testdb", "неопределено", 0, "неопреде
postgres [c] 'Fri Jan 30 11:20:38 2015' '/usr/lib/libparsec-cap-db-files.so.2.5.134' <27501,27330,110,116,110> [s] pgsq("Подключение", "[local]", "testdb", "postgres", 10, "postgres", 10,
postgres [c] 'Fri Jan 30 11:25:00 2015' '/usr/lib/libparsec-cap-db-files.so.2.5.134' <27501,27330,110,116,110> [s] pgsq("Отключение", "[local]", "testdb", "postgres", 10, "postgres", 10,
postgres [c] 'Fri Jan 30 15:18:43 2015' '/usr/lib/libparsec-cap-db-files.so.2.5.134' <31207,27330,110,116,110> [s] pgsq("Подключение", "[local]", "testdb", "user3", 16387, "user3", 16387,
postgres [c] 'Fri Jan 30 15:18:43 2015' '/usr/lib/postgresql/9.3/lib/plpgsql.so' <27398,27330,110,116,110> [s] pgsq("Отключение", "[local]", "testdb", "user1", 16385, "user1", 16385,
postgres [c] 'Fri Jan 30 15:19:32 2015' '/usr/lib/libparsec-cap-db-files.so.2.5.134' <31220,27330,110,116,110> [s] pgsq("Подключение", "[local]", "testdb", "user2", 16386, "user2", 16386,
postgres [c] 'Fri Jan 30 15:19:32 2015' '/usr/lib/libparsec-cap-db-files.so.2.5.134' <31207,27330,110,116,110> [s] pgsq("Отключение", "[local]", "testdb", "user3", 16387, "user3", 16387,
postgres [c] 'Fri Jan 30 15:22:46 2015' '/usr/lib/libparsec-cap-db-files.so.2.5.134' <31266,27330,110,116,110> [s] pgsq("Подключение", "[local]", "testdb", "user3", 16387, "user3", 16387,
postgres [c] 'Fri Jan 30 15:22:46 2015' '/usr/lib/libparsec-cap-db-files.so.2.5.134' <31220,27330,110,116,110> [s] pgsq("Отключение", "[local]", "testdb", "user2", 16386, "user2", 16386,
postgres [c] 'Fri Jan 30 15:23:29 2015' '/usr/lib/libparsec-cap-db-files.so.2.5.134' <31266,27330,110,116,110> [f] pgsq("Вставка (INSERT)", "[local]", "testdb", "user3", 16387, "user3", 163
postgres [c] 'Fri Jan 30 15:24:40 2015' '/lib/x86_64-linux-gnu/libnss_nis-2.13.so' <31294,27330,110,116,110> [s] pgsq("Подключение", "127.0.0.1", "postgres", "postgres", 10, "postgres", 1
postgres [c] 'Fri Jan 30 15:27:25 2015' '/usr/lib/libparsec-cap-db-files.so.2.5.134' <31266,27330,110,116,110> [f] pgsq("Вставка (INSERT)", "[local]", "testdb", "user3", 16387, "user3", 163
postgres [c] 'Fri Jan 30 15:27:46 2015' '/usr/lib/libparsec-cap-db-files.so.2.5.134' <31375,27330,110,116,110> [s] pgsq("Подключение", "[local]", "testdb", "user3", 16387, "user3", 16387,
postgres [c] 'Fri Jan 30 15:27:46 2015' '/usr/lib/libparsec-cap-db-files.so.2.5.134' <31266,27330,110,116,110> [s] pgsq("Отключение", "[local]", "testdb", "user3", 16387, "user3", 16387,
postgres [c] 'Fri Jan 30 15:30:46 2015' '/usr/lib/libparsec-cap-db-files.so.2.5.134' <31419,27330,110,116,110> [s] pgsq("Подключение", "[local]", "testdb", "user2", 16386, "user2", 16386,
postgres [c] 'Fri Jan 30 15:30:46 2015' '/usr/lib/libparsec-cap-db-files.so.2.5.134' <31375,27330,110,116,110> [s] pgsq("Отключение", "[local]", "testdb", "user3", 16387, "user3", 16387,
postgres [c] 'Fri Jan 30 15:34:37 2015' '/usr/lib/libparsec-cap-db-files.so.2.5.134' <31475,27330,110,116,110> [s] pgsq("Подключение", "[local]", "testdb", "user2", 16386, "user2", 16386,
postgres [c] 'Fri Jan 30 15:34:37 2015' '/usr/lib/libparsec-cap-db-files.so.2.5.134' <31419,27330,110,116,110> [s] pgsq("Отключение", "[local]", "testdb", "user2", 16386, "user2", 16386,
postgres [c] 'Fri Jan 30 15:37:50 2015' '/usr/lib/libparsec-cap-db-files.so.2.5.134' <31523,27330,110,116,110> [s] pgsq("Подключение", "[local]", "testdb", "user3", 16387, "user3", 16387,
postgres [c] 'Fri Jan 30 15:37:50 2015' '/usr/lib/libparsec-cap-db-files.so.2.5.134' <31475,27330,110,116,110> [s] pgsq("Отключение", "[local]", "testdb", "user3", 16387, "user3", 16387,
postgres [c] 'Fri Jan 30 15:41:53 2015' '/lib/x86_64-linux-gnu/libnss_nis-2.13.so' <31588,27330,110,116,110> [f] pgsq("Подключение", "[local]", "postgres", "неопределено", 0, "неопреде
postgres [c] 'Fri Jan 30 15:42:14 2015' '/lib/x86_64-linux-gnu/libnss_nis-2.13.so' <31593,27330,110,116,110> [s] pgsq("Подключение", "127.0.0.1", "postgres", "postgres", 10, "postgres", 1
postgres [c] 'Fri Jan 30 15:42:34 2015' '/lib/x86_64-linux-gnu/libnss_nis-2.13.so' <31601,27330,110,116,110> [s] pgsq("Подключение", "127.0.0.1", "postgres", "postgres", 10, "postgres", 1
postgres [c] 'Fri Jan 30 15:43:05 2015' '/lib/x86_64-linux-gnu/libnss_nis-2.13.so' <31601,27330,110,116,110> [s] pgsq("Отключение", "127.0.0.1", "postgres", "postgres", 10, "postgres", 10
postgres [c] 'Fri Jan 30 15:46:08 2015' '/usr/lib/libparsec-cap-db-files.so.2.5.134' <31523,27330,110,116,110> [s] pgsq("Очистка таблицы (TRUNCATE)", "[local]", "testdb", "user3", 1638
postgres [c] 'Fri Jan 30 15:47:04 2015' '/usr/lib/libparsec-cap-db-files.so.2.5.134' <31671,27330,110,116,110> [s] pgsq("Подключение", "[local]", "testdb", "user1", 16385, "user1", 16385,
postgres [c] 'Fri Jan 30 15:47:04 2015' '/usr/lib/libparsec-cap-db-files.so.2.5.134' <31523,27330,110,116,110> [s] pgsq("Отключение", "[local]", "testdb", "user3", 16387, "user3", 16387,
postgres [c] 'Fri Jan 30 15:48:01 2015' '/usr/lib/libparsec-cap-db-files.so.2.5.134' <31686,27330,110,116,110> [s] pgsq("Подключение", "[local]", "testdb", "user2", 16386, "user2", 16386,
postgres [c] 'Fri Jan 30 15:48:01 2015' '/usr/lib/libparsec-cap-db-files.so.2.5.134' <31671,27330,110,116,110> [s] pgsq("Отключение", "[local]", "testdb", "user1", 16385, "user1", 16385,
postgres [c] 'Fri Jan 30 15:48:47 2015' '/usr/lib/libparsec-cap-db-files.so.2.5.134' <31697,27330,110,116,110> [s] pgsq("Подключение", "[local]", "testdb", "user3", 16387, "user3", 16387,
postgres [c] 'Fri Jan 30 15:48:47 2015' '/usr/lib/libparsec-cap-db-files.so.2.5.134' <31686,27330,110,116,110> [s] pgsq("Отключение", "[local]", "testdb", "user2", 16386, "user2", 16386,
postgres [c] 'Fri Jan 30 17:21:26 2015' '/usr/lib/libparsec-cap-db-files.so.2.5.134' <31697,27330,110,116,110> [s] pgsq("Очистка таблицы (TRUNCATE)", "[local]", "testdb", "user3", 1638
postgres [c] 'Fri Jan 30 19:51:27 2015' '/usr/lib/libparsec-cap-db-files.so.2.5.134' <31697,27330,110,116,110> [s] pgsq("Очистка таблицы (TRUNCATE)", "[local]", "testdb", "user3", 1638
postgres [c] 'Fri Jan 30 19:52:09 2015' '/usr/lib/libparsec-cap-db-files.so.2.5.134' <31697,27330,110,116,110> [s] pgsq("Очистка таблицы (TRUNCATE)", "[local]", "testdb", "user3", 1638
postgres [c] 'Fri Jan 30 20:02:48 2015' '/usr/lib/libparsec-cap-db-files.so.2.5.134' <31697,27330,110,116,110> [s] pgsq("Очистка таблицы (TRUNCATE)", "[local]", "testdb", "user3", 1638

```



Пример расчета увеличения размера таблицы:

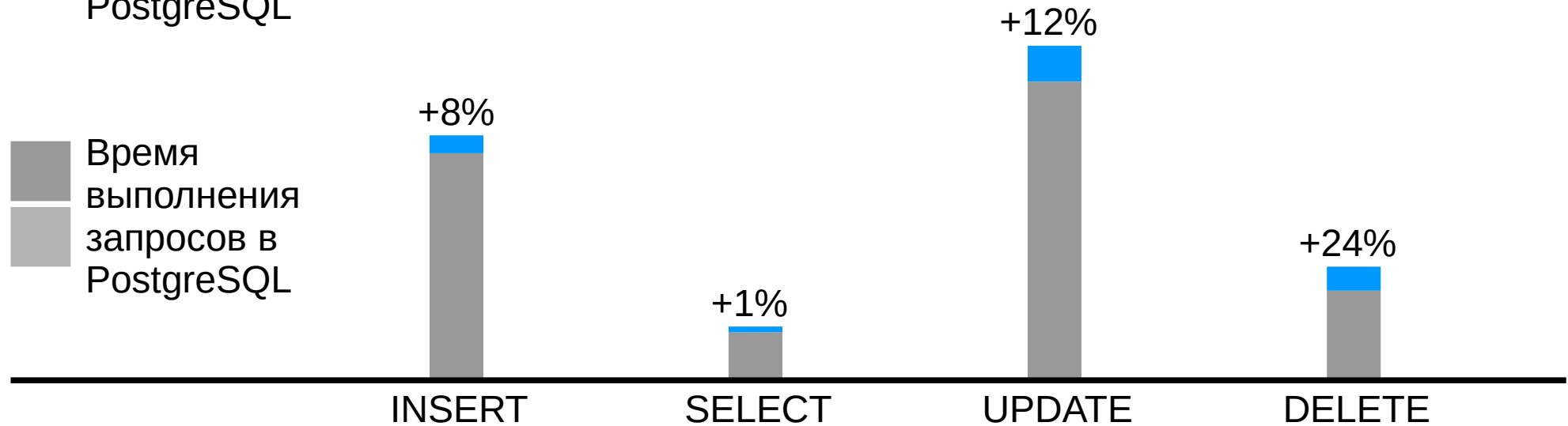
- размер мандатной метки таблицы: 9 байт;
- размер признака учета мандатных атрибутов: 1 байт;
- размер мандатной метки одной записи: 9 байт;
- увеличение размера таблицы с 1 млн. записей: $9 + 1 + 9 \times 1000000 \approx 9\text{МБ}$.

В таблицах с записями малого размера приращение времени выполнения запросов наиболее заметно.

Абсолютное приращение времени выполнения запросов линейно зависит от количества записей.

■ Приращение времени выполнения запросов в доработанном PostgreSQL

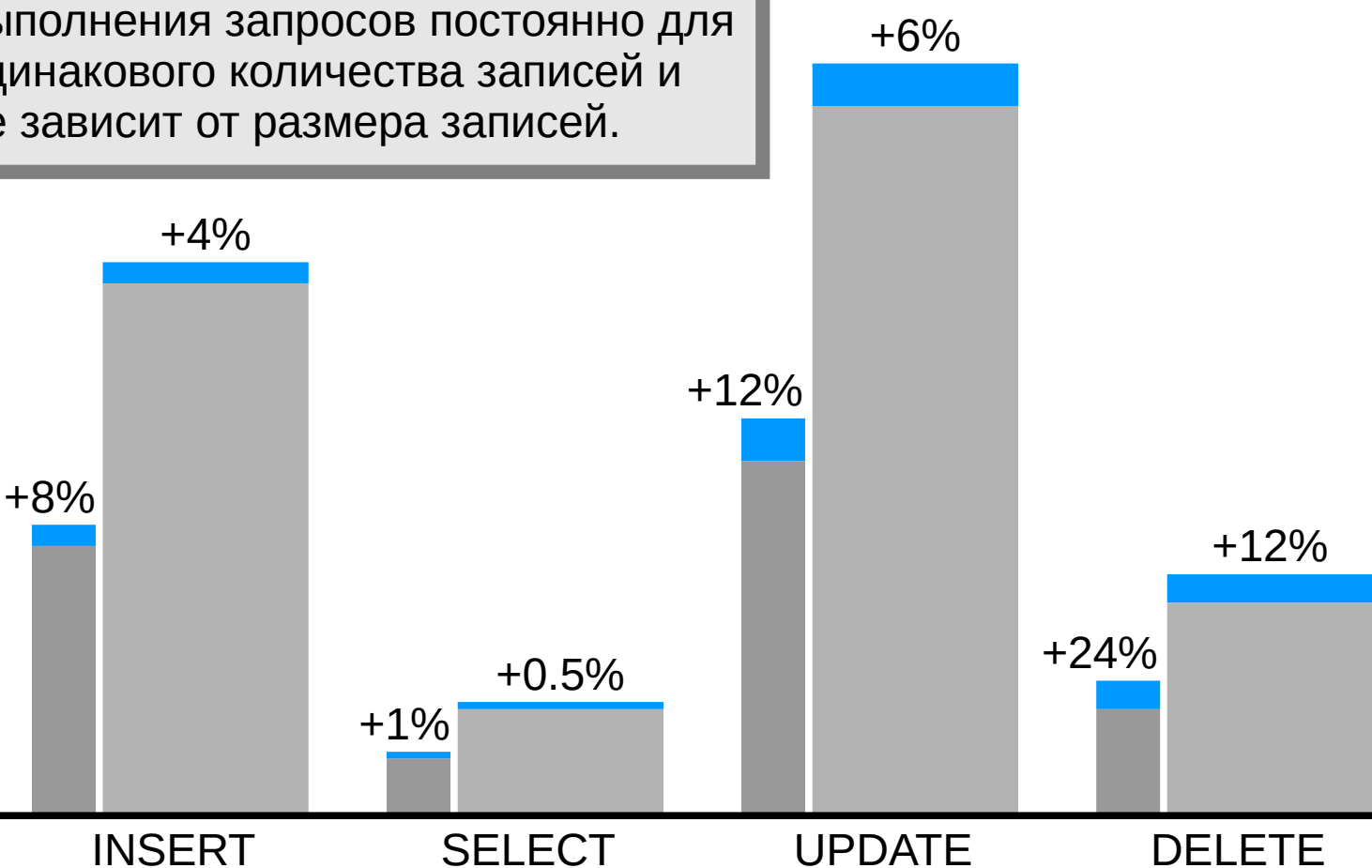
■ Время выполнения запросов в PostgreSQL



Абсолютное приращение времени выполнения запросов постоянно для одинакового количества записей и не зависит от размера записей.

■ Приращение времени выполнения запросов в доработанном PostgreSQL

■ Время выполнения запросов в PostgreSQL





НАУЧНО-ПРОИЗВОДСТВЕННОЕ ОБЪЕДИНЕНИЕ
РУССКИЕ БАЗОВЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

www.rusbitech.ru

СПАСИБО ЗА ВНИМАНИЕ!

www.astralinux.ru