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

БЕЗОПАСНОСТЬ И БЫСТРОДЕЙСТВИЕ

СЕРТИФИКАЦИЯ СУБД PostgreSQL В СОСТАВЕ ОС СН "Astra Linux Special Edition"

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.

ПЕРЕЧЕНЬ ПРОГРАММНЫХ СРЕДСТВ СУБД В СОСТАВЕ ОС СН "Astra Linux Special Edition"

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.

ДОРАБОТКА СУБД PostgreSQL ДЛЯ ОБЕСПЕЧЕНИЯ ТРЕБОВАНИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ

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).

РАЗЛИЧИЯ В РАЗГРАНИЧЕНИИ ДОСТУПА

Обычная СУБД PostgreSQL

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

Доработанная СУБД PostgreSQL

ПРИМЕР ФОРМИРОВАНИЯ МАНДАТНЫХ МЕТОК РАЗГРАНИЧЕНИЯ ДОСТУПА К ДАННЫМ

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

ПРИМЕР ОБЛАСТИ ВИДИМОСТИ ДАННЫХ ПРИ МАНДАТНОМ РАЗГРАНИЧЕНИИ ДОСТУПА

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}
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}

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

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

ПРИМЕР РЕАЛИЗАЦИИ МАНДАТНОГО РАЗГРАНИЧЕНИЯ ДОСТУПА

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	Таблица-2 {2,0x1} CCR = On
Запись {3,0x0}	Запись
Запись {2,0x8}	Запись
Запись {1,0x0}	Запись
Запись {0,0x0}	Запись
Запись {3,0x0}	Запись
Запись {2,0x0}	Запись
Запись {1,0x0}	Запись
Запись {0,0x0}	Запись

CCR (Container clearance required) - учет мандатных атрибутов контейнера

ПРИМЕР РЕАЛИЗАЦИИ МАНДАТНОГО РАЗГРАНИЧЕНИЯ ДОСТУПА

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

ПРИМЕР РЕАЛИЗАЦИИ МАНДАТНОГО РАЗГРАНИЧЕНИЯ ДОСТУПА

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

ПРИМЕР РЕАЛИЗАЦИИ МАНДАТНОГО РАЗГРАНИЧЕНИЯ ДОСТУПА

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

ПРИМЕР РЕАЛИЗАЦИИ МАНДАТНОГО РАЗГРАНИЧЕНИЯ ДОСТУПА

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

ПРИМЕР РЕАЛИЗАЦИИ МАНДАТНОГО РАЗГРАНИЧЕНИЯ ДОСТУПА

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

РЕГИСТРАЦИЯ СОБЫТИЙ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

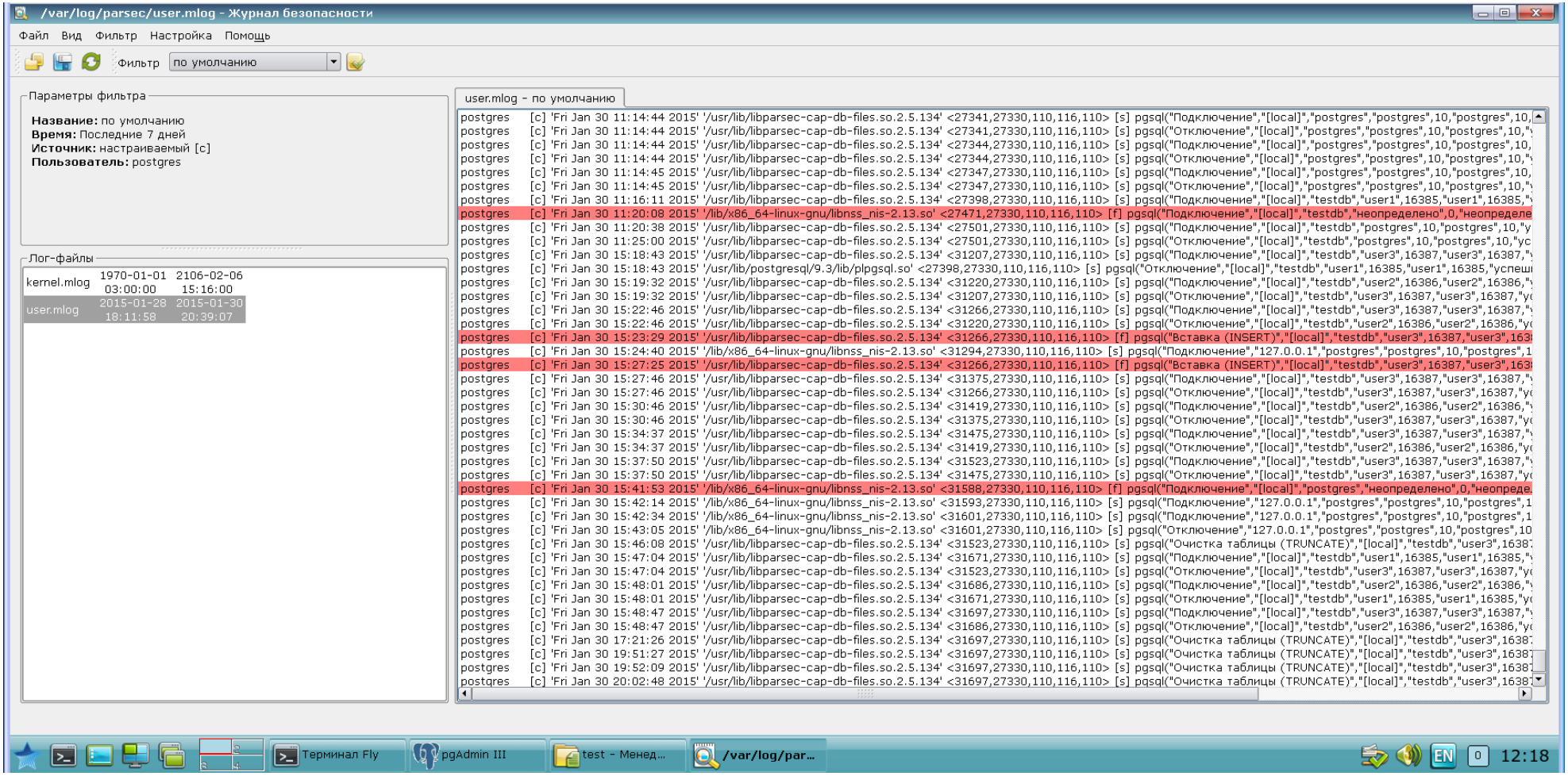
Средства аудита доработанной СУБД PostgreSQL обеспечивают регистрацию следующих событий:

- 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.

ЖУРНАЛ РЕГИСТРАЦИИ СОБЫТИЙ БЕЗОПАСНОСТИ



ОЦЕНКА УВЕЛИЧЕНИЯ ОБЪЕМА БАЗЫ ДАННЫХ

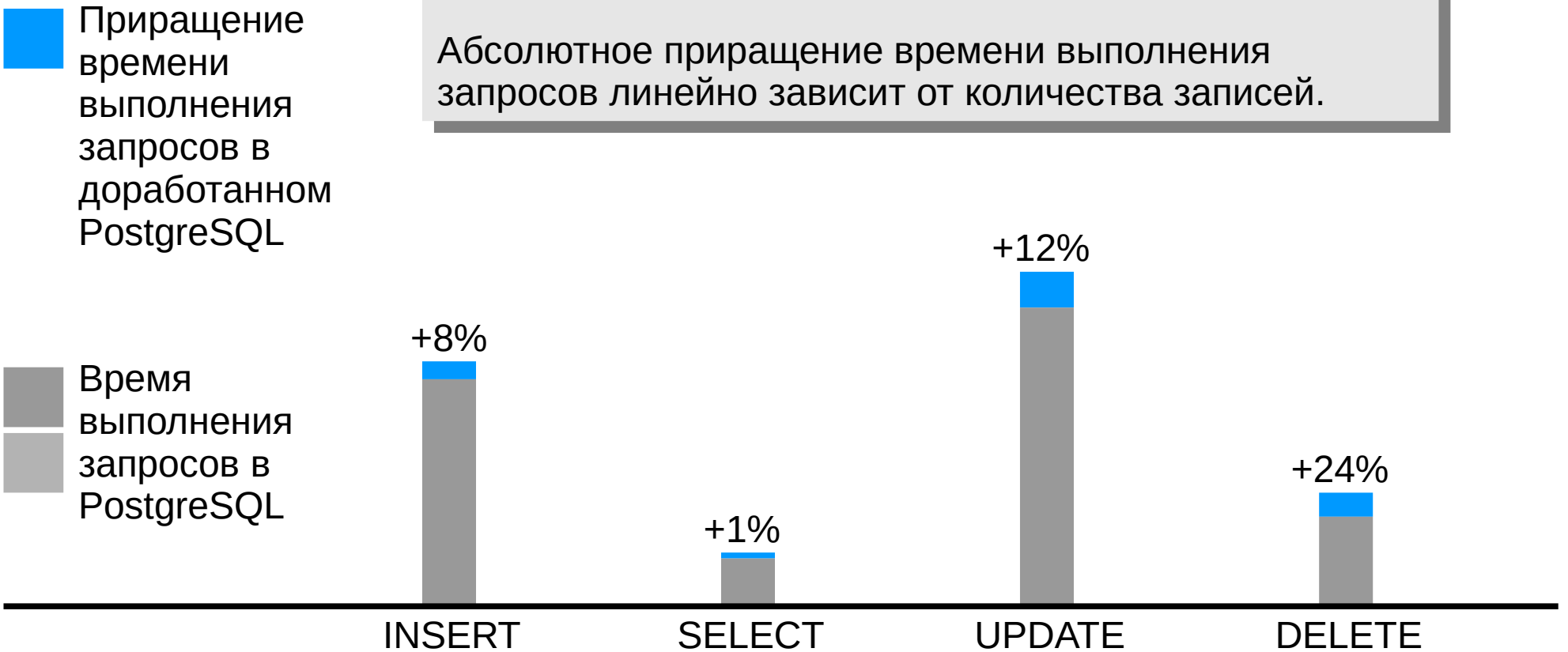
Пример расчета увеличения размера таблицы:

- 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 x 1000000 ≈ 9МБ.

ИЗМЕНЕНИЕ СКОРОСТИ ВЫПОЛНЕНИЯ ОСНОВНЫХ ОПЕРАЦИЙ ПРИ МАНДАТНОМ РАЗГРАНИЧЕНИИ ДОСТУПА К ЗАПИСЯМ

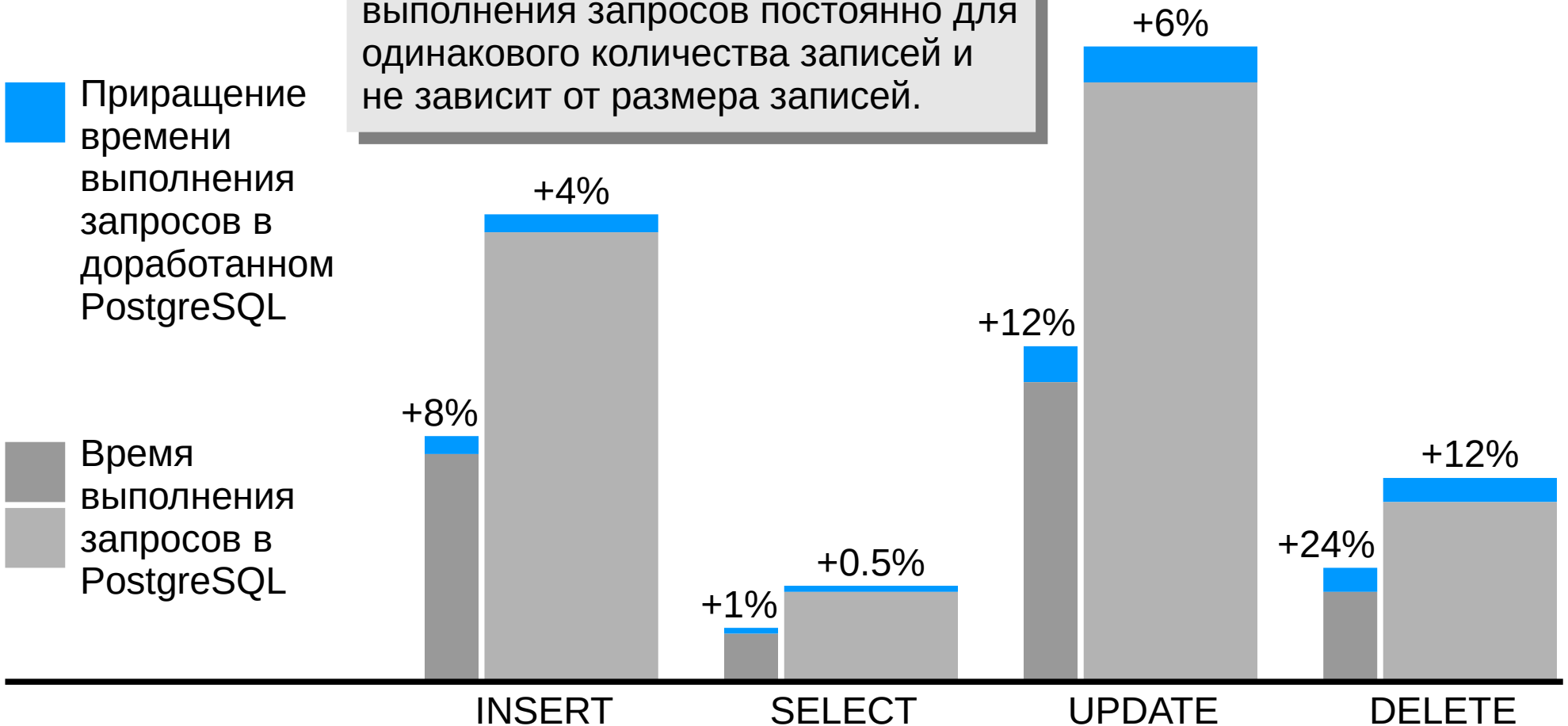
В таблицах с записями малого размера приращение времени выполнения запросов наиболее заметно.

Абсолютное приращение времени выполнения запросов линейно зависит от количества записей.



ИЗМЕНЕНИЕ СКОРОСТИ ВЫПОЛНЕНИЯ ОСНОВНЫХ ОПЕРАЦИЙ ПРИ МАНДАТНОМ РАЗГРАНИЧЕНИИ ДОСТУПА К ЗАПИСЯМ

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



www.rusbitech.ru

СПАСИБО ЗА ВНИМАНИЕ!

www.astralinux.ru