System DB Crypto Storage

Построение защищенных хранилищ данных на основе СУБД Firebird v3.0

ООО «Сайфер БИС»
Влад Ковтун
Леонид Белясник

Суть проблемы

Обеспечение конфиденциальности данных хранящихся в БД:

- Персональных данных
- Чувствительных данных (медицинских, банковских и т.д.)

Суть проблемы

Согласно требований:

- КСЗИ
- ISO/IEC 27001:2013
- PCI-DSS
- HIPAA
- FERPA

Существующие подходы

- Шифрование соединения
- Шифрование файлов БД
  - Шифрование всего раздела (уровень ФС)
  - Шифрование указанных файлов (уровень ФС)
  - Использование специальных инструментов (BitLocker, TrueCrypt и другие)
- Шифрование данных в БД (TDE)
  - **Прозрачное шифрование пространства таблиц, постранично**
- Шифрование полей в БД (AL)
  - На основе паролей в SQL

Существующие решения

Что предлагается в мире СУБД:

- Oracle DB Enterprise (TDE, AL)
  - Ключ в файле
  - Ключ на устройстве
- Microsoft SQL Server Enterprise (TDE, AL)
  - Ключ в файле
  - Ключ на устройстве
- MongoDB Enterprise (TDE, AL)
  - Ключ в файле
  - Ключ на устройстве
  - Основан на OpenSSL

Существующие решения

Что предлагается в мире СУБД:

- MySQL Enterprise (TDE, AL)
  - Ключ в файле
  - Ключ на устройстве
- MySQL/MariaDB/Percona (AL)
  - Пароль в SQL/DB
- PostgreSql (AL)
  - Используется pgcrypt (plugin общего назначения)
  - Пароль в SQL/DB
- SQLite

Что предлагаем мы?

- СУБД Firebird v3.0
  - Промышленная СУБД
  - Бесплатная
  - Открытый исходный код
  - Большие объемы данных
  - Высокая стабильность
  - Поддержка шифрования БД
  - Поддержка шифрования канала
  - Личная система управления пользователями
  - Работа оффлайн с шифрованными БД

Детали реализации

- Что потребовалось?
  - На Firebird C++API реализованы расширения:
    - Расширение-хранитель секретного ключа (KeyHolder)
    - Расширение шифрования данных (DbCrypt)
- Что получили
  - Зашифровывание/расшифровывание БД с помощью запроса SQL

```
ALTER DATABASE ENCRYPT WITH "plugin_name" KEY "key_name"
ALTER DATABASE DECRYPT
```

  - Шифрование в фоновом служебном потоке
  - Возможность управления ключами

Детали реализации

- Протокол безопасной передачи ключа
  - DbCrypt plugin → KeyHolder plugin:
    - Прошу передать мне ключ
  - KeyHolder plugin:
    - Шифрует ключ (с учётом данных от DbCrypt)
  - KeyHolder plugin → DbCrypt plugin:
    - Зашифрованный ключ
  - DbCrypt plugin:
    - Расшифровует и проверяет ключ
    - Готов к работе

Детали реализации

- Что подлежит зашифрованию:
  - Страницы данных, blob и индексов (кроме заголовка страницы) - зашифрованы, включая системные таблицы
  - Вспомогательные страницы не зашифрованы (не содержат конфиденциальной информации)
  - Проверка корректности ключа производится с помощью сравнения хеша фиксированных данных с образцом хранящимся в заголовке
  - Особо важные данные защищены дополнительной MAC

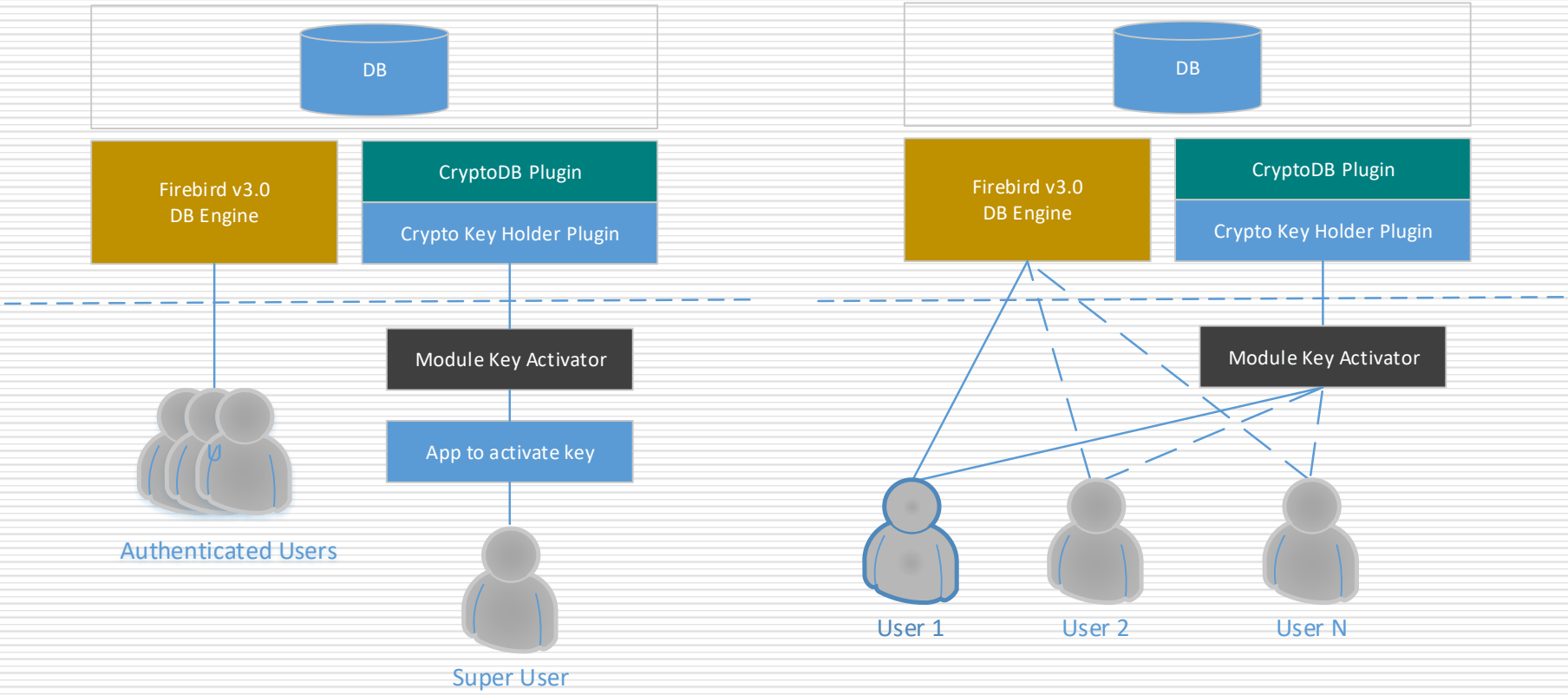
Что предлагается?

- Средства, разработанные для сторонних разработчиков, позволяющие защитить используемую их приложением БД от несанкционированного доступа:
  - Plugin для доступа к ключу
  - Plugin для шифрования БД
  - Модуль активации с описанием интерфейса для использования в разрабатываемом ПО
  - Поддержка сетевого и Embedded режима

Варианты использования

- Предустановленные данные:
  - Поддержка шифрования БД, предназначенных для передачи и дальнейшего использования другим лицом
  - Доступ возможен только по ключу
- Внедрение в готовое решение:
  - Без особых изменений в основное приложение, можно обеспечить конфиденциальность данных в БД
  - Не тратить время на разбор подходов и алгоритмов обеспечения конфиденциальности
  - Не тратить время на знакомство с C++ API Firebird и написание плагинов

Архитектура решения



Готовое решение

- Систему шифрования БД для СУБД Firebird 3
  - Plugin для доступа к ключу
  - Plugin для шифрования БД
  - Сервер активации ключей
  - Клиент генерации контейнеров ключей и управления ими.

Решаемые задачи

- Безопасное хранение секретного ключа БД
  - Хранится в зашифрованном виде в файловом контейнере
  - Есть возможность хранить в контейнере только пароль к защищённому носителю
  - Активация доступна только двум ответственным лицам
  - Число ответственных лиц не ограничено
  - Число используемых ключей системой не ограничено
- Шифрование данных
  - После того, как ключ был активирован, система работает автоматически и не требует участия человека
  - Число зашифрованных БД системой не ограничено

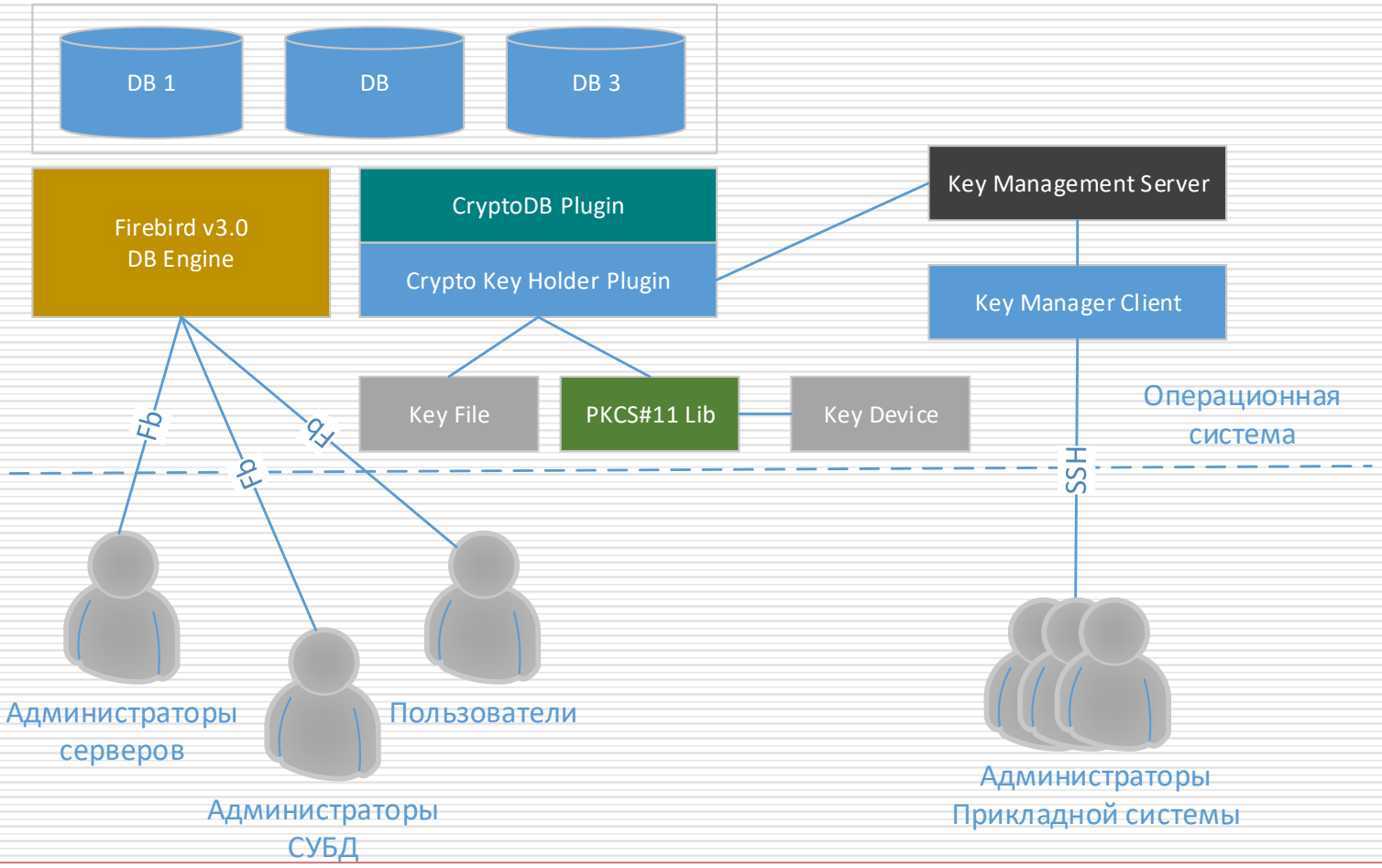
Решаемые задачи

- Безопасное использование секретного ключа БД
  - Доступ к секретному ключу обеспечивает три элемента системы
  - Обмен информацией между элементами обеспечивается шифрованием на сессионных ключах
  - Объекты доступа к ключу создаются динамически и в зависимости от настроек живут не более организованной сессии
  - Только во время запуска процесса шифрования ключ преобразуется и готов к использованию

Решаемые задачи

- Применение системы
  - Есть возможность хранить неограниченное количество контейнеров секретных ключей и при этом шифровать в разных режимах неограниченное количество баз данных
  - Обслуживающему персоналу сервера, на котором развёрнута система шифрования БД недоступны хранимые данные
  - Можно отдавать на хранение БД с чувствительными данными в аутсорсинг
  - Защита БД от физического похищения
  - Может использоваться в модели SaaS

Архитектура решения



Криптографические алгоритмы

- Для шифрования данных используются:
  - ДСТУ 7624:2014 (ECB, CBC, CFB, OFB, CTR)
  - ГОСТ 28147-89 (ECB, CBC, CFB, OFB, CTR)
  - AES (ECB, CBC, CFB, OFB, CTR)
  - TDEA (ECB, CBC, CFB, OFB, CTR)
- В основе лежит библиотека «Шифр+» v2.0 (на этапе получения экспертного заключения)

Поддерживаемые платформы

СУБД Firebird v3.0 поддерживает:

- Windows
  - x86
  - x86-64
- Linux
  - x86
  - x86-64
- Android (experimental)
  - ARM
  - ARM64

Условия эксперимента

Сервер:

- CPU: Intel Core i7-2600 CPU @ 3,40GHz
- CPU Cores: 4 x 3,41 GHz (with HT - 8)
- HDD: 40GB
- RAM: 4096 MB
- OS: Centos 7 x86-64
- Linux v.: 3.10.0-327.36.1.e17.x86_64
- СУБД: Firebird v3.0.2 x86-64

Условия эксперимента

Клиент:

- CPU: Intel Core i5-6400 CPU @ 2,70GHz
- CPU Cores: 4 x 2,7 GHz
- HDD: SATA III 2000GB
- RAM: 8 GB
- OS: Windows 10 (64-bit)
- Клиент СУБД: IBExpert v.2017.4.24.1
- NET: Gigabit Ethernet

Условия эксперимента

- БД:
  - 7 таблиц, 28 индексов, 5 blob полей, 19 представлений, 5 триггеров, 1 генератор, 1 функция, 1 пользователь
  - Размер: 1008000 KB (~ 1 ГБ)
- Шифры:
  - AES-NI-256
  - ГОСТ 28147-89 (ДКЕ №1)
  - ДСТУ 7624:2014 (256/256)

Зашифровывание

Первичное полное зашифровывание БД размером 1 Гб и последующее полное расшифровывание, МБ/с. Время в секундах.

Algorithm-Mode	Производит., МБ/с		Время, с	
	Encrypt	Decrypt	Encrypt	Decrypt
AES-NI-256-OFB	109.14	110.131	9.01934	8.93823
AES-NI-256- CTR	101.696	101.882	9.67954	9.66193
ГОСТ 28147-OFB	46.4388	46.2943	21.1973	21.2634
ГОСТ 28147- CTR	44.7567	44.7679	21.9939	21.9884
ДСТУ 7624-256-OFB	66.1892	63.6726	14.8721	15.4599
ДСТУ 7624-256-CTR	66.0562	63.5132	14.9021	15.4987

Производительность СУБД

- Алгоритм 1:
  - SQL-скрипт создает пустую БД
  - SQL-скрипт и Blob производится операция вставки большого количества записей (более 320000)
  - создаётся резервная копия
  - замеры времени операций с данными на незашифрованной БД (выборка, изменение, удаление)

Производительность СУБД

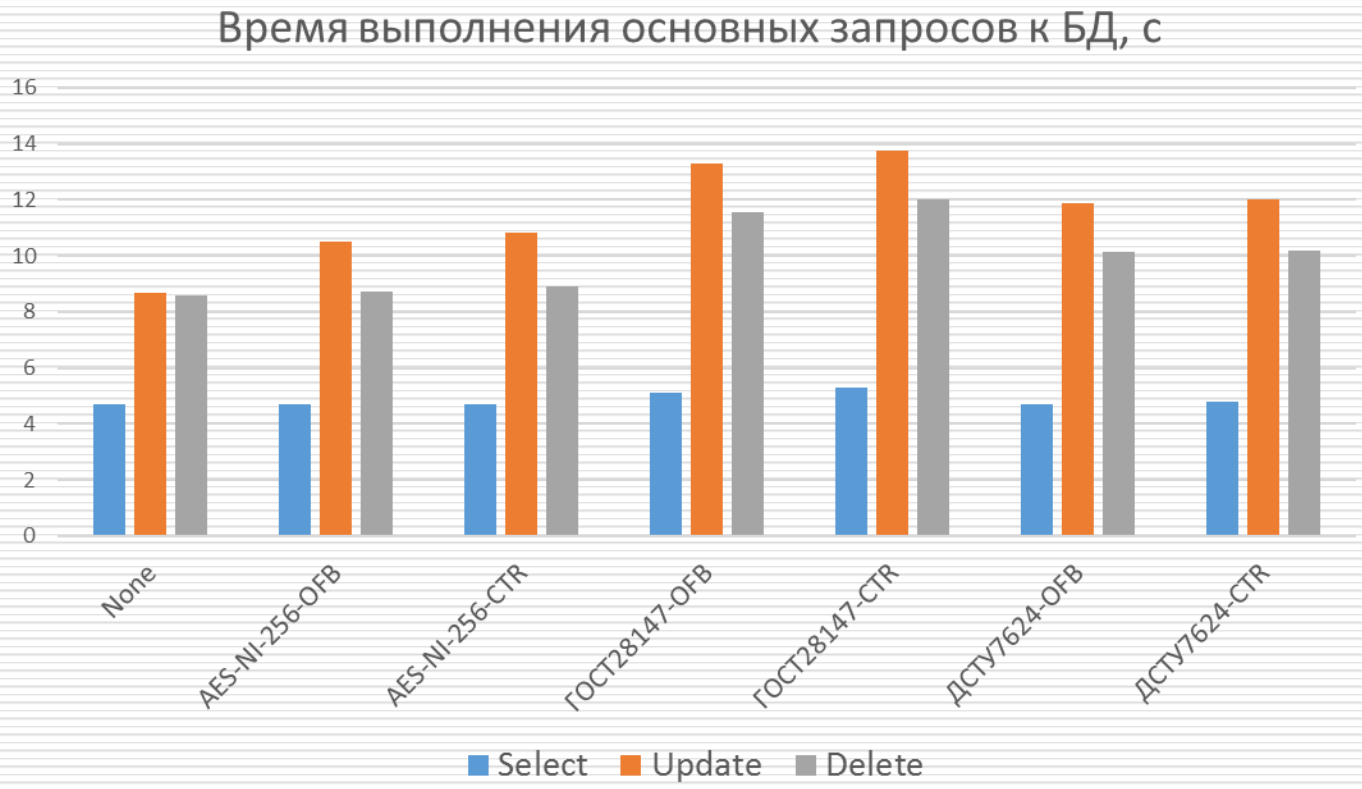
- Алгоритм 2:
  - создается пустая БД
  - **шифруется одним из алгоритмов в одном из режимов**
  - производится операция вставки большого количества записей
  - создаётся резервная копия
  - замеры времени операций с данными в зашифрованной БД

Производительность СУБД

Operation	Bulk Insert	Backup	Select	Update	Delete
None	25:23.610	00:17.000	00:04.688	00:08.672	00:08.578
AES-NI-256-OFB	25:43.922	00:26.000	00:04.719	00:10.516	00:08.734
AES-NI-256-CTR	26:09.344	00:25.000	00:04.703	00:10.843	00:08.890
ГОСТ28147-OFB	26:40.375	00:37.000	00:05.109	00:13.297	00:11.563
ГОСТ28147-CTR	25:49.547	00:36.000	00:05.31	00:13.766	00:12.000
ДСТУ7624-256-OFB	25:58.890	00:31.000	00:04.703	00:11.890	00:10.150
ДСТУ7624-256-CTR	25:54.969	00:33.000	00:04.782	00:12.000	00:10.172

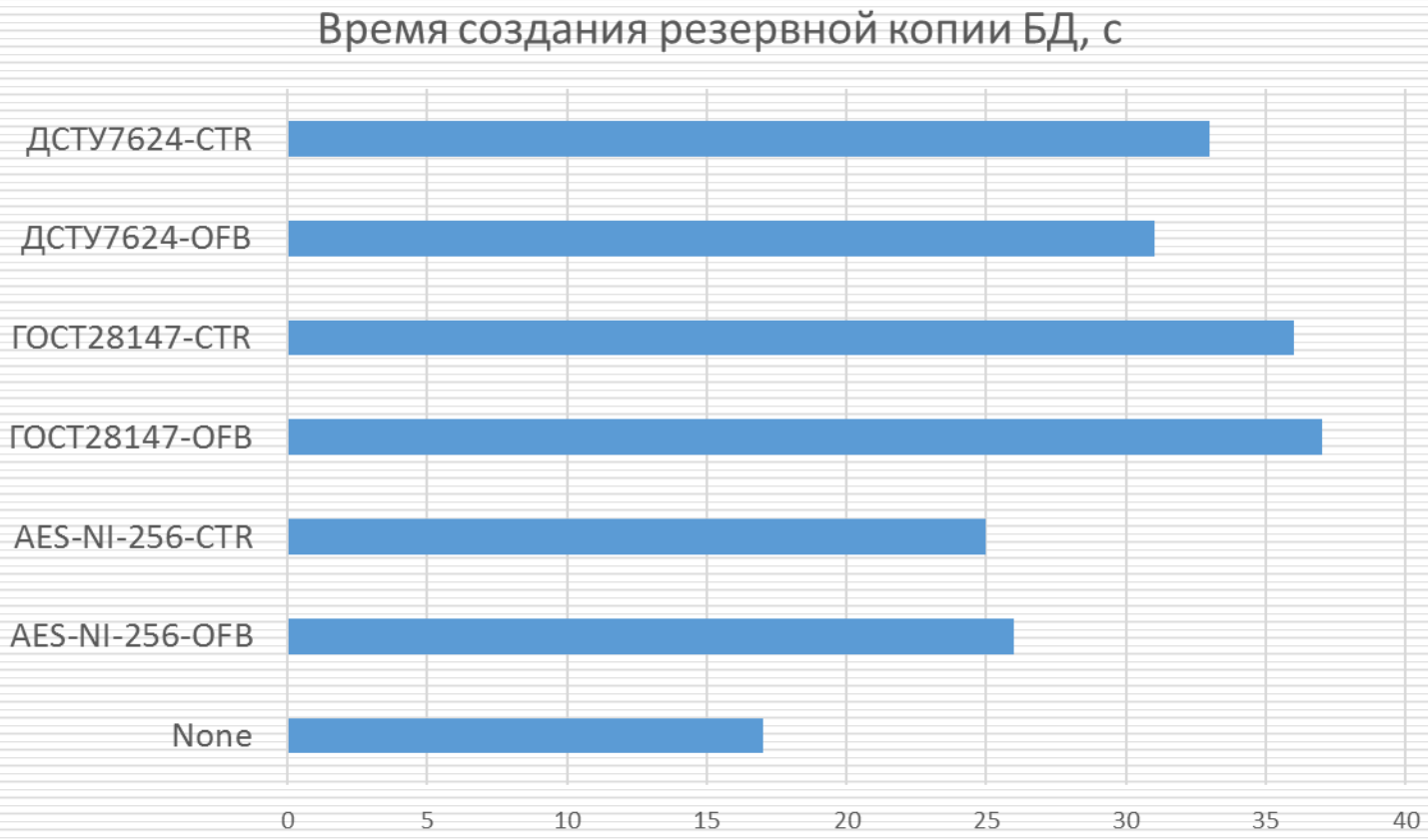
Время указано в формате mm:ss.fff

Производительность СУБД



Производительность СУБД

Производительность СУБД



Вопросы?

Спасибо за внимание!

ООО «Сайфер БИС»

Влад Ковтун
Леонид Белясник

email: vk@cipher.kiev.ua, lb@cipher.kiev.ua
www: http://cipher.kiev.ua