СКЗИ «Шифр-X.509»

Масштабирование, резервируемость, диагностика, репликация и резервное хранение данных

ООО «Сайфер ЛТД», к.т.н. Влад Ковтун

Содержание

- Краткая характеристика и архитектура
- Масштабирование
- Резервирование
- Диагностика
- Резервное хранение данных

Назначение системы

Система криптографической защиты информации «Шифр-X.509» предназначена для управления персональными ключами и сертификатами электронной цифровой подписи и шифрования информации, согласно стандарта X.509

Криптографическое ядро системы

Программное изделие «Шифр+»
(библиотеки криптографических
преобразований Win32, Java)

Требования к ЦСК

- Высокая производительность – масштабируемость и репликация данных
- Высокая надежность – резервируемость и репликация данных
- Корректность – диагностика
- Восстановление после сбоев – резервирование данных и репликация

СКЗИ «Шифр-X.509»

ОСОБЕННОСТИ ПОСТРОЕНИЯ

Архитектура

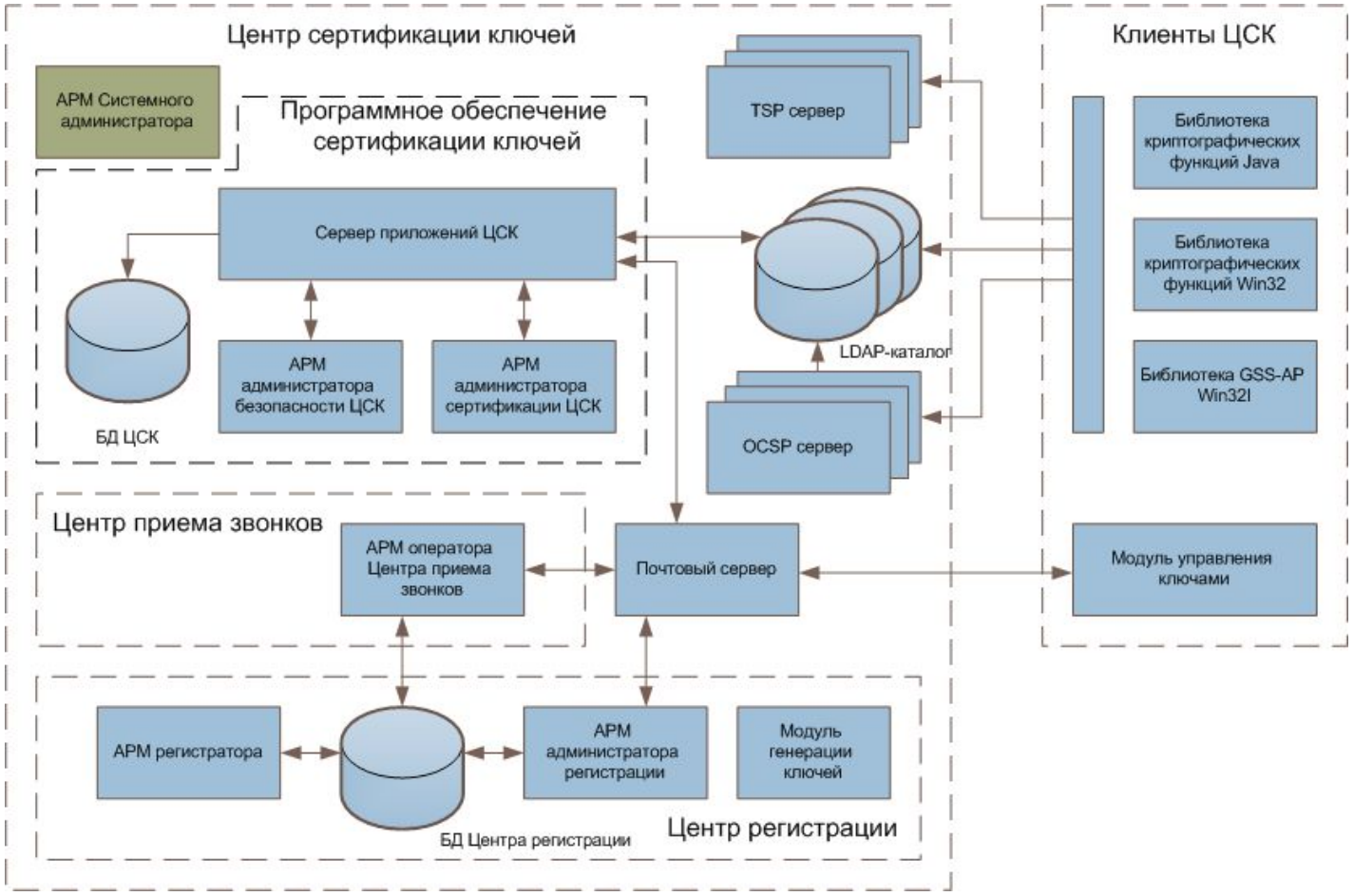
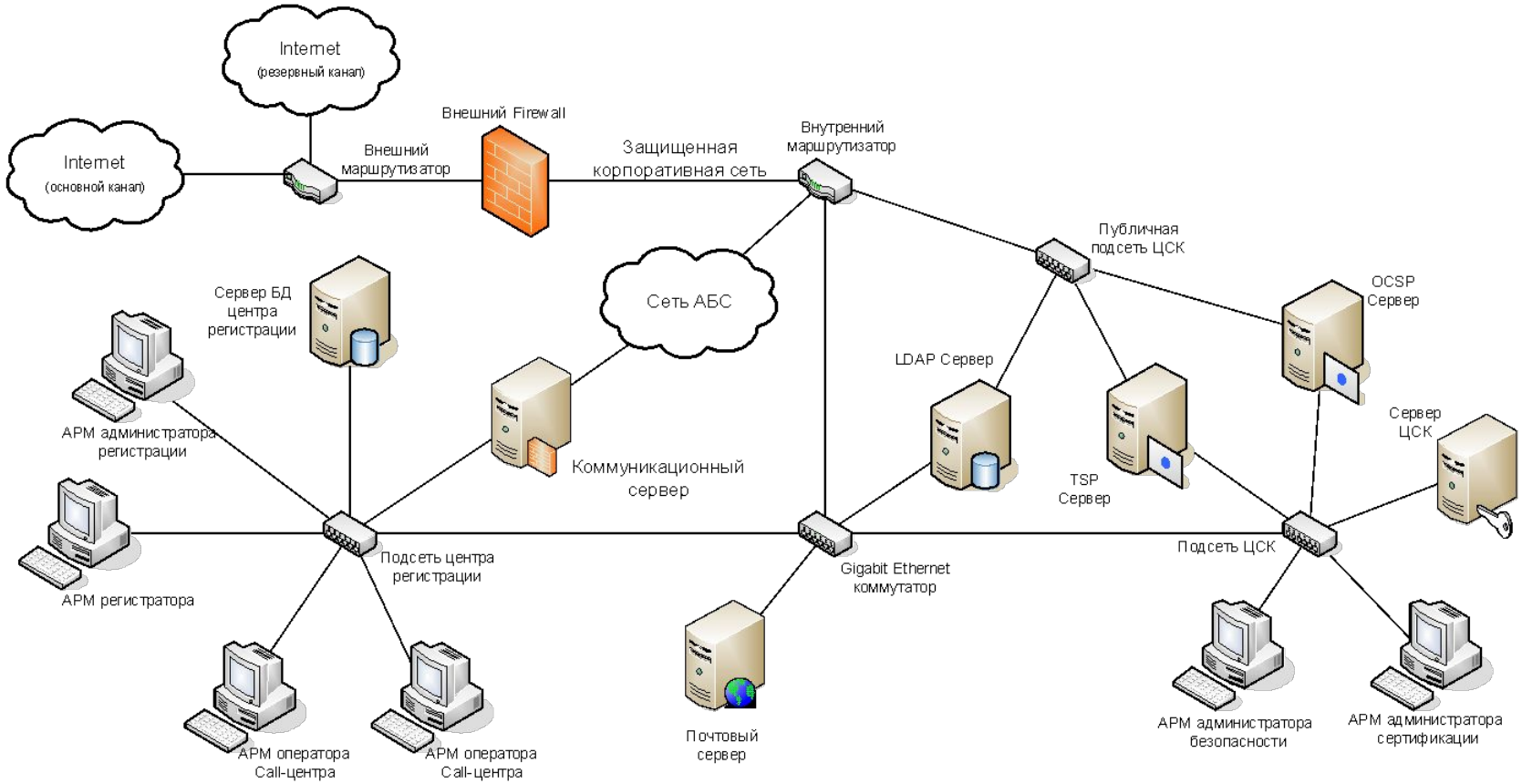


Схема развертывания

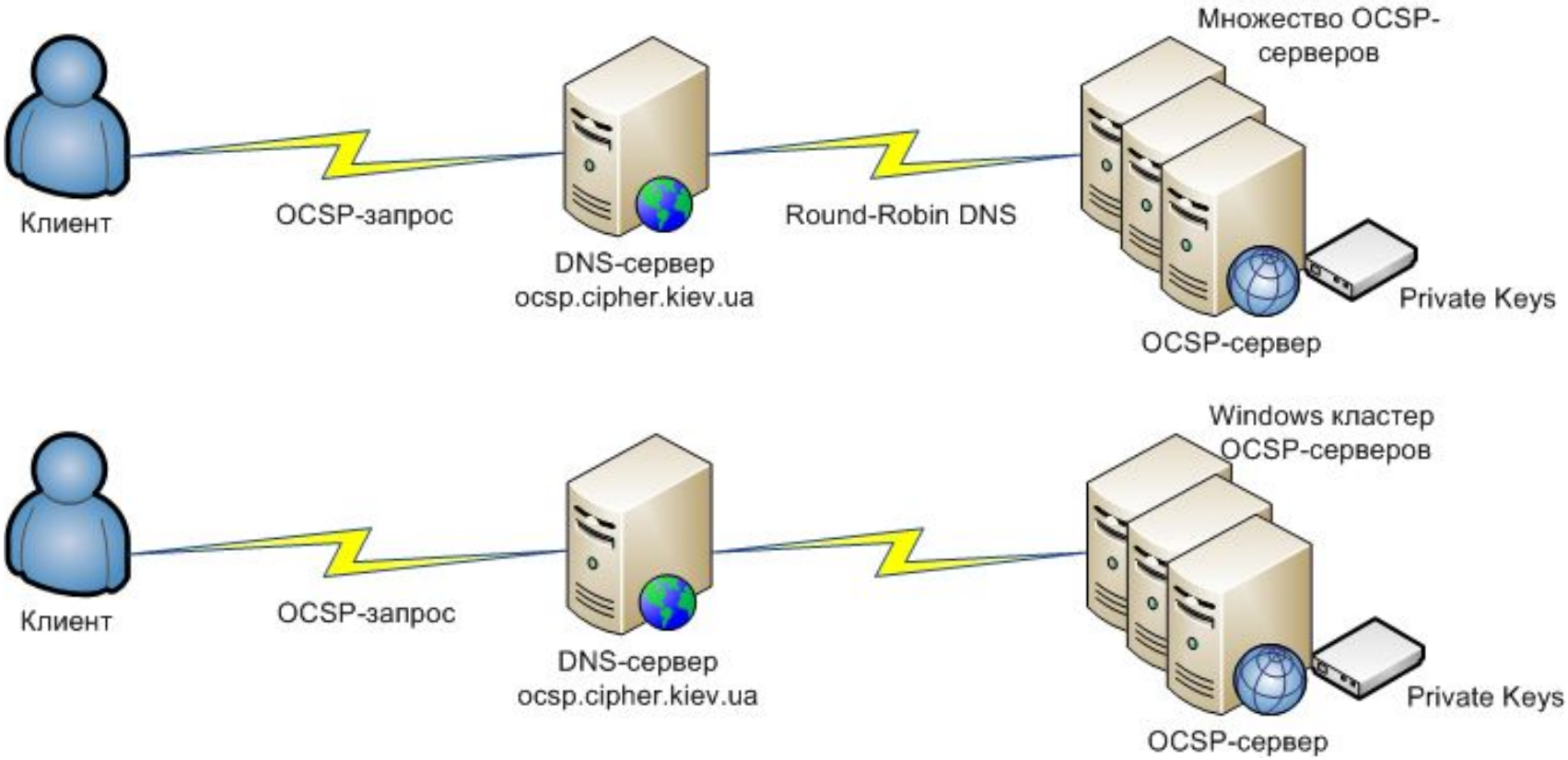


НАДЕЖНОСТЬ И ПРОИЗВОДИТЕЛЬНОСТЬ

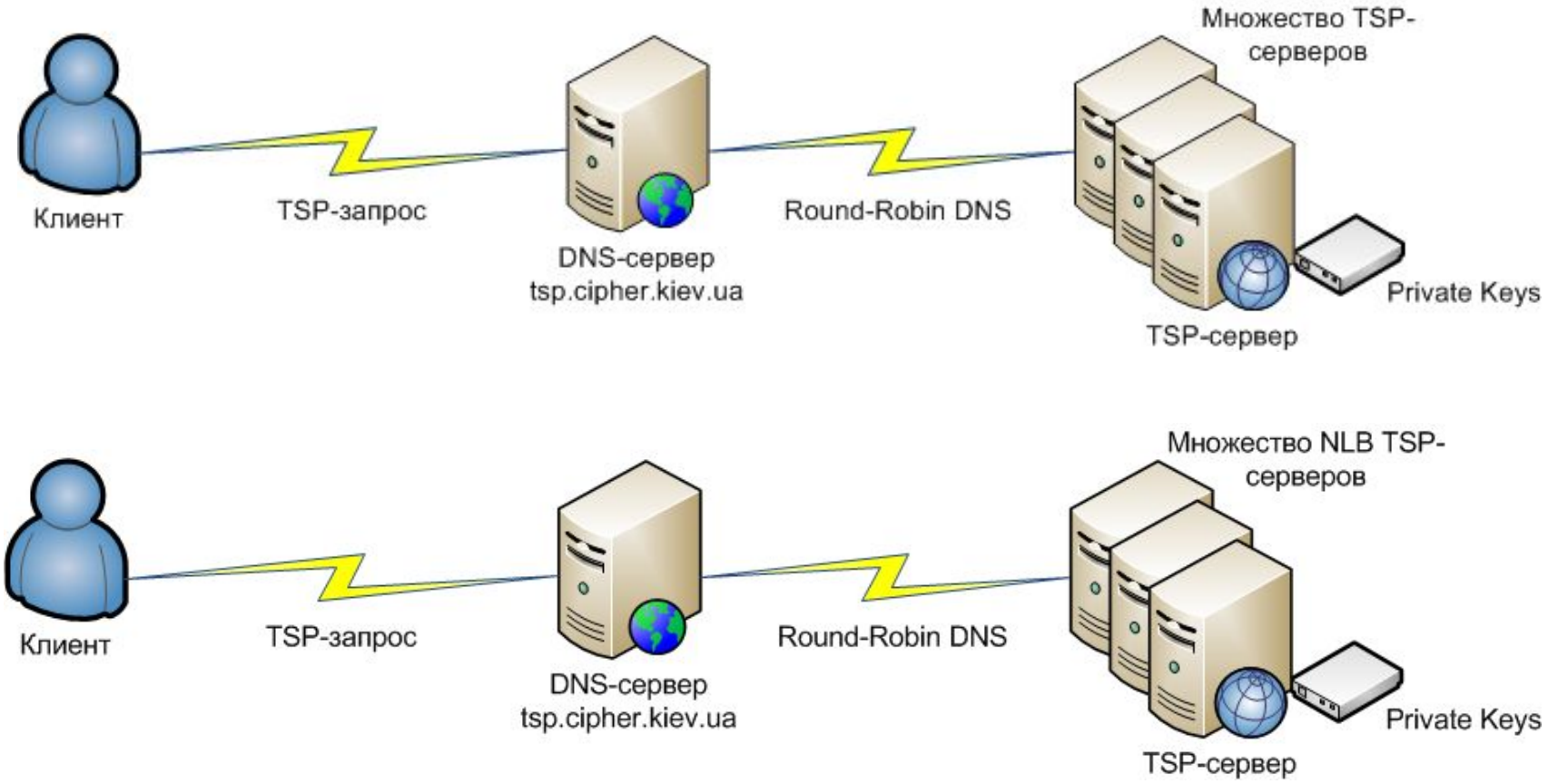
Возможности

- Масштабирование сервисов
- Резервирование сервисов
- Диагностика сервисов
- Резервное хранение данных

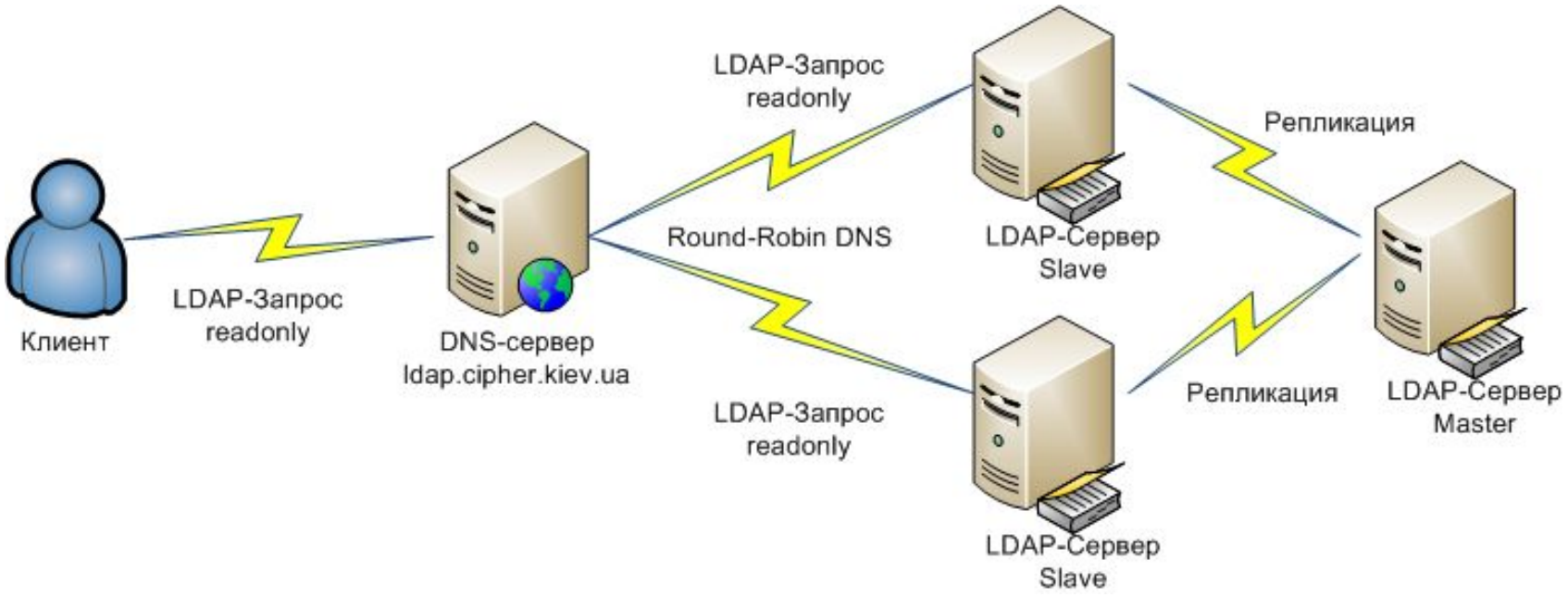
Масштабируемость OCSP



Масштабируемость TSP



Масштабируемость LDAP



Диагностика

Диагностика служб ЦСК реализуется средствами АРМ системного администратора:

- LDAP
- OCSP
- TSP
- Сервер приложений ЦСК
- Почтовый сервер

Диагностика

Диагностика серверных платформ ЦСК реализуется средствами АРМ системного администратора:

- для Windows Server
  - Performance Counters
- для Linux Server
  - Аналоги Performance Counters

Диагностика LDAP

- OpenLDAP Monitoring interface
  - Подключений (всего, сейчас)
  - Состояние Listener’ов
  - Статистка операций (Bind, Unbind, Add, Delete, Modify, …)
  - Статистика данных (Bytes, PDU, Entries, Referrals)
  - Потоков обработки (max, сейчас)
  - Время (запуска, текущее)

Диагностика LDAP

- Диагностические запросы - время отклика
  - Master (чтение, запись, поиск)
  - Slave (чтение, поиск)

Диагностика OCSP

- Диагностические запросы - время отклика
  - Подключение
  - Запрос на статус одного сертификата (один запрос)

Диагностика TSP

- Диагностические запросы - время отклика
  - Подключение
  - Запрос на метку

Диагностика сервера приложений ЦСК

- Диагностические запросы - время отклика
  - Подключение
  - Передача тестового запроса на сертификат (тестовый профиль)
  - Прием тестового сертификата* (тестовый профиль)

*Не сохраняются в БД ЦСК и LDAP

Диагностика сервера БД ЦСК

- Диагностические запросы - время отклика
  - Подключение
  - Тестовый поисковый запрос

Диагностика почтового сервера

- Диагностические запросы - время отклика
  - Отправка тестового почтового сообщения «сам на себя»

Резервируемость

- OCSP-сервер, решается в рамках масштабируемости
- TSP-сервер, решается в рамках масштабируемости
- LDAP-сервер, решается в рамках масштабируемости

Резервируемость

- Сервера приложений ЦСК достигается за счет полного клонирования*
- БД ЦСК достигается за счет репликации

*Личный ключ ЦСК в файловом контейнере в зашифрованном виде

Репликация БД

- Базы данных FireBird

Существуют различные утилиты для организации репликации:

- **FiBRE** - open source, cross-platform.
- FBReplicator - open source.
- **ReplicadorBR** - open source.
- Replicador Firebird – freeware.
- **DBRE** - open source.

Резервное хранение данных

- Базы данных FireBird

Существуют различные утилиты для организации резервирования и восстановления:

- Nbackup, входит в поставку FireBird для различных операционных систем.
- GBAK, бесплатная утилита поддерживаемая официально FireBird, которая, в отличие от nbackup, позволяет работать с многофайловыми БД под управлением FireBird.

Для эффективного резервирования используют различные подходы:

- Полное резервирование.
- Инкрементное резервирование.

Резервное хранение данных

- Базы данных FireBird

Инкрементная схема резервирования может выглядеть следующим образом:

- Каждый месяц создается резервная копия всей базы данных (уровня 0);
- Каждую неделю делается инкрементная резервная копия уровня 1;
- Каждые сутки создается инкрементная резервная копия уровня 2;
- Каждый час создается инкрементная резервная копия уровня 3.

Резервное хранение данных

- Базы данных OpenLDAP

Существуют встроенные утилиты для организации резервирования* и восстановления данных:

- slapcat, полностью копирует содержимое БД при работающем сервере;
- slapadd, восстанавливает содержимое БД при остановленном сервере.

*Каждые сутки создается резервная копия БД в LDIF файл.

Вопросы?

Спасибо за внимание!

ООО «САЙФЕР ЛТД»

Владислав Ковтун

email: vlad.kovtun@cipher.kiev.ua
www: http://www: http://www.www: http://www.cipher.kiev.ua

FireBird

- Максимальный размер таблицы:
  - 2.5 ТБ для страницы в 4 КБ;
- Максимальная длинна записи:
  - суммарно все поля: 64 кБ;
- Размер базы: 131 ТБ;
- Максимальное число одновременных подключений:
  - Windows SuperServer: 1024;
  - Linux: без перекомпиляции ядра - до 600.