

СКЗИ «Шифр-Х.509»

Масштабирование,
резервируемость,
диагностика, репликация и
резервное хранение данных
ЦСК банков

ООО «Сайфер ЛТД», к.т.н. Влад Ковтун

Назначение системы

Система криптографической защиты информации «Шифр-Х.509» предназначена для построения ЦСК: управления персональными ключами и сертификатами для ЭЦП и шифрования информации, согласно стандарту Х.509

Содержание

- Требования НБУ к ИТС ЦСК
- Краткая характеристика и архитектура ЦСК
- Масштабирование ЦСК
- Резервирование ЦСК
- Диагностика ЦСК
- Резервное хранение данных ЦСК

Предпосылки

- Постановление НБ Украины от 17.16.2004 г. №265 с изменениями согласно постановления НБ Украины от 05.04.2012 г. № 174 «**Об утверждении Положения об обеспечении непрерывного функционирования информационных систем НБ Украины и банков Украины**»
- Активная интеграция технологий X.509 в системы автоматизации банков и системы дистанционного обслуживания банков

Требования к ЦСК

- Усі вимоги цього Положення стосовно САБ поширюються також на ВМПС у разі її наявності, а також на інші комплекси програмно-апаратних засобів, призначені для розв'язання банками власних завдань у сфері автоматизації, технічної й технологічної підтримки діяльності **ЗЦ НБУ, АЦСК НБУ, ЦСК банку та завдань взаємодії з інформаційною мережею НБУ**

Требования к ЦСК

□ Надежность

- Мониторинг и диагностика
- Резервируемость сервисов (резервные сервисы, резервный ЦОД)
- Резервируемость и репликация данных
- Восстановление после сбоев (резервные сервисы, резервные копии данных, резервный ЦОД)

□ Производительность

- Масштабируемость сервисов
- Репликация данных

СКЗИ «Шифр-Х.509»

ОСОБЕННОСТИ ПОСТРОЕНИЯ

Архитектура

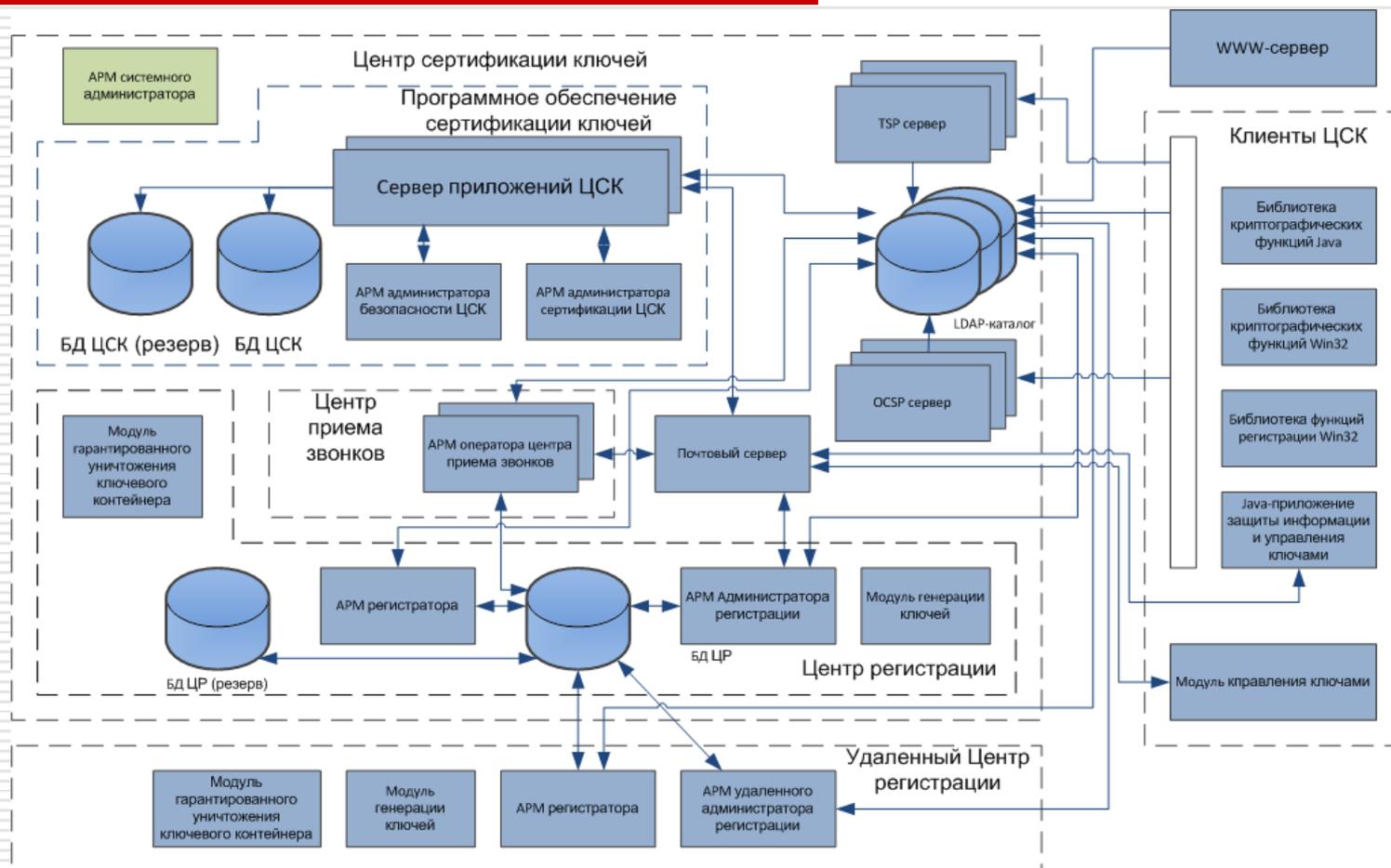


Схема развертывания (1)

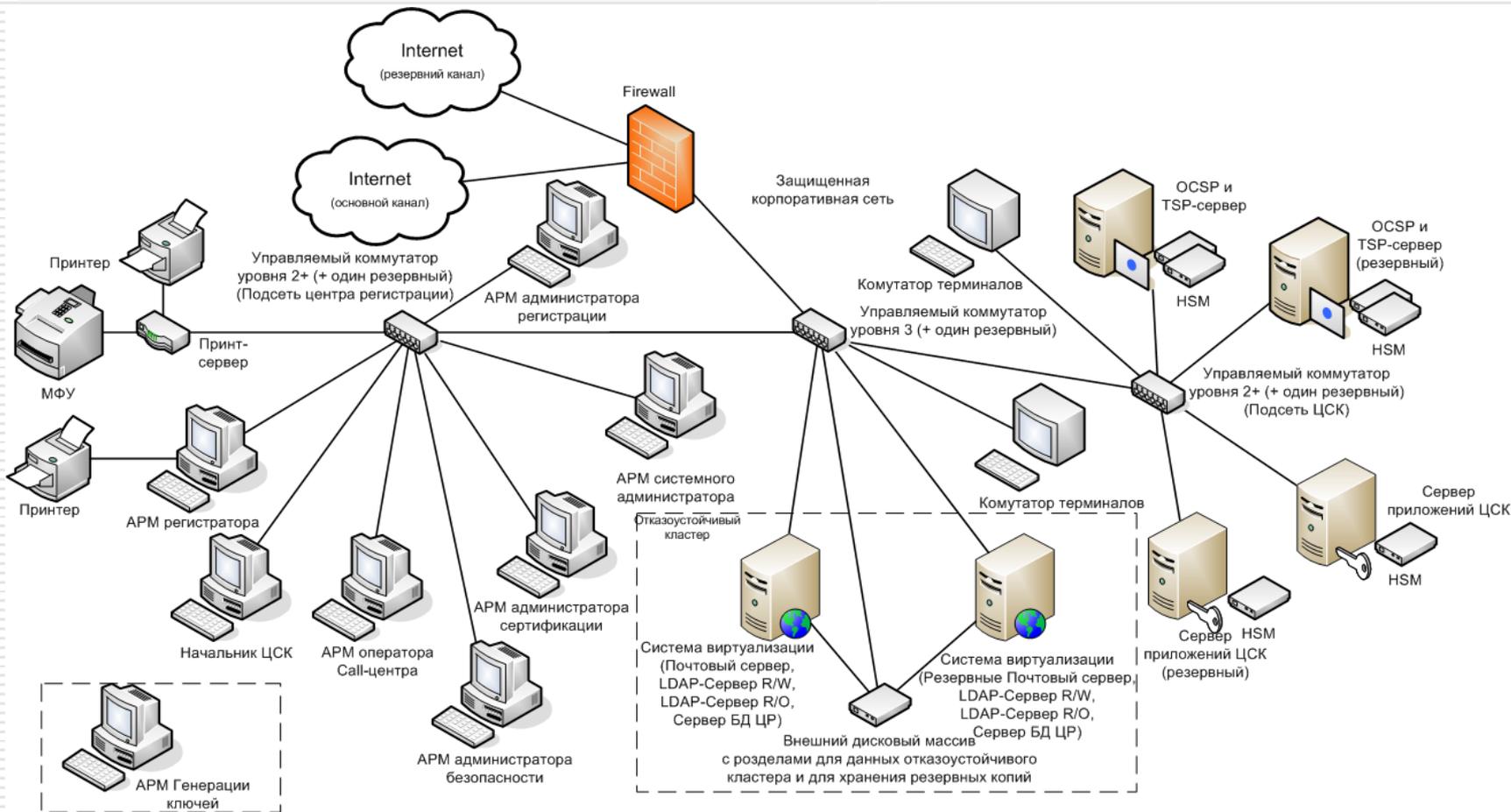
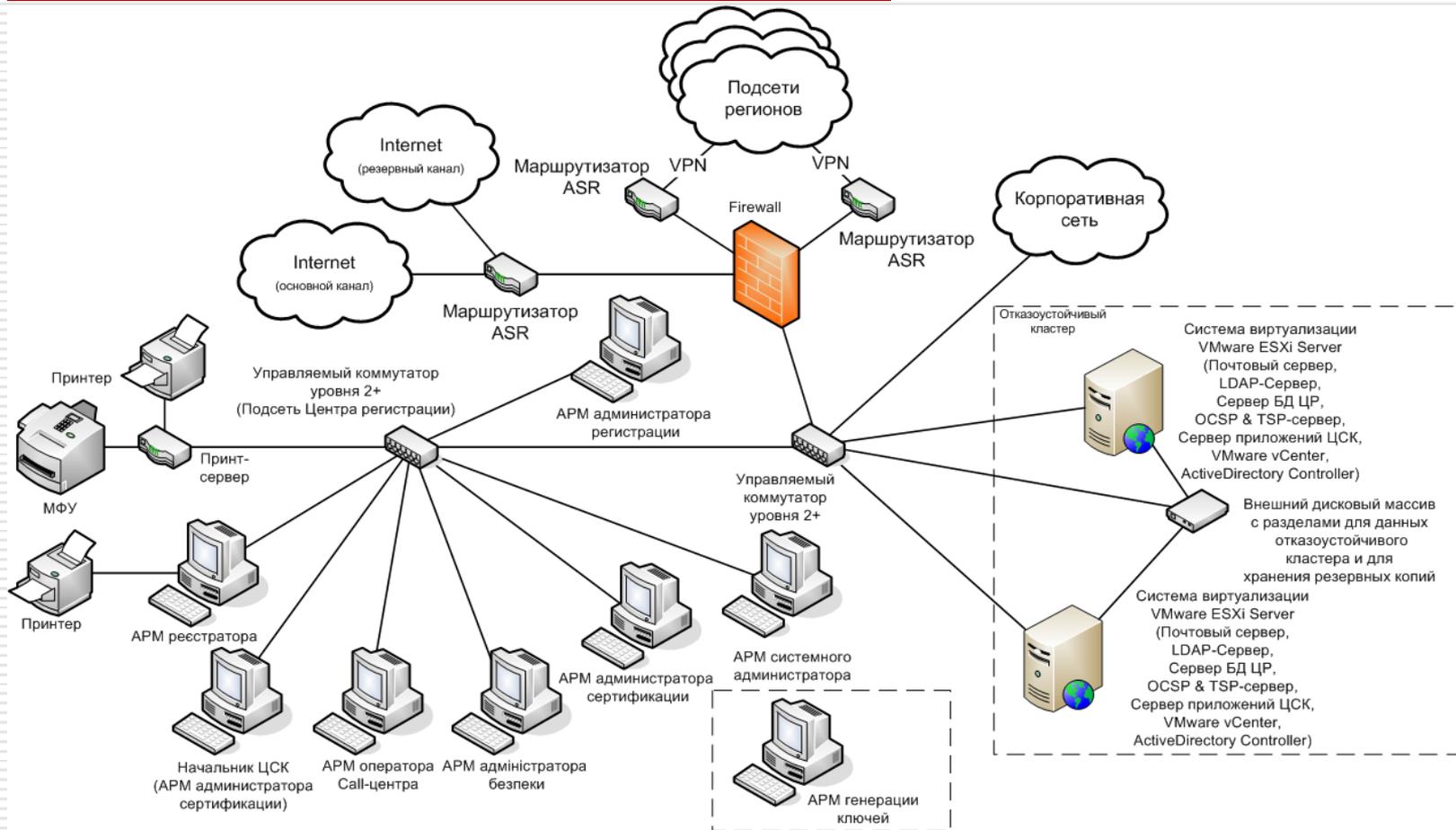


Схема развертывания (2)



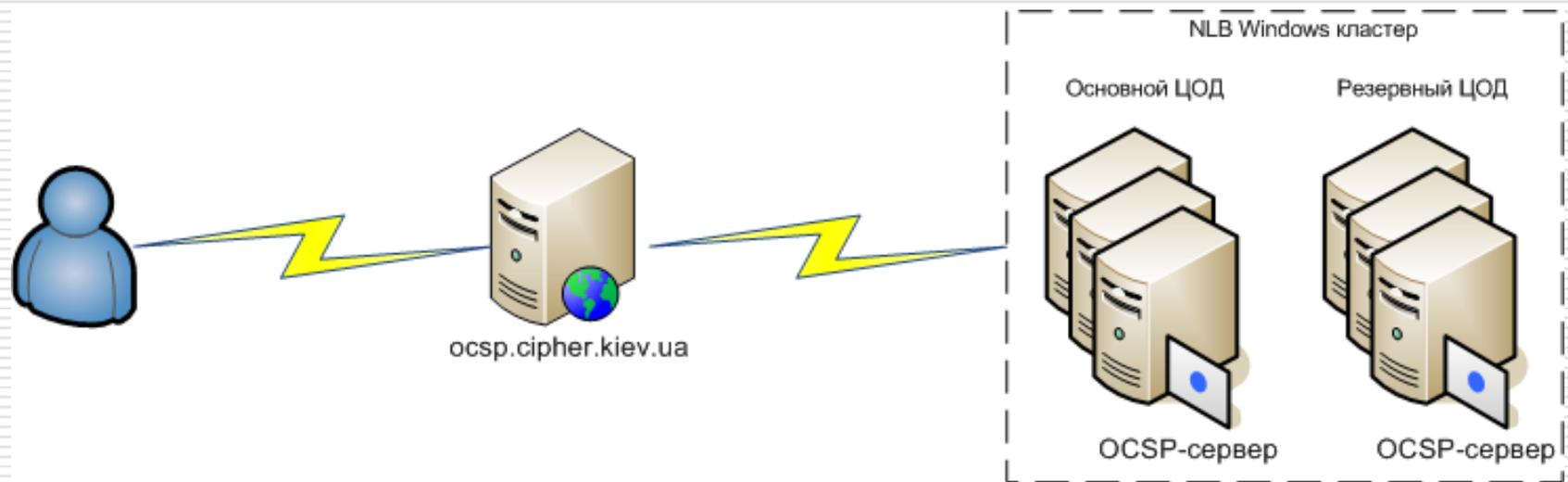
СКЗИ «Шифр-Х.509»

НАДЕЖНОСТЬ И ПРОИЗВОДИТЕЛЬНОСТЬ

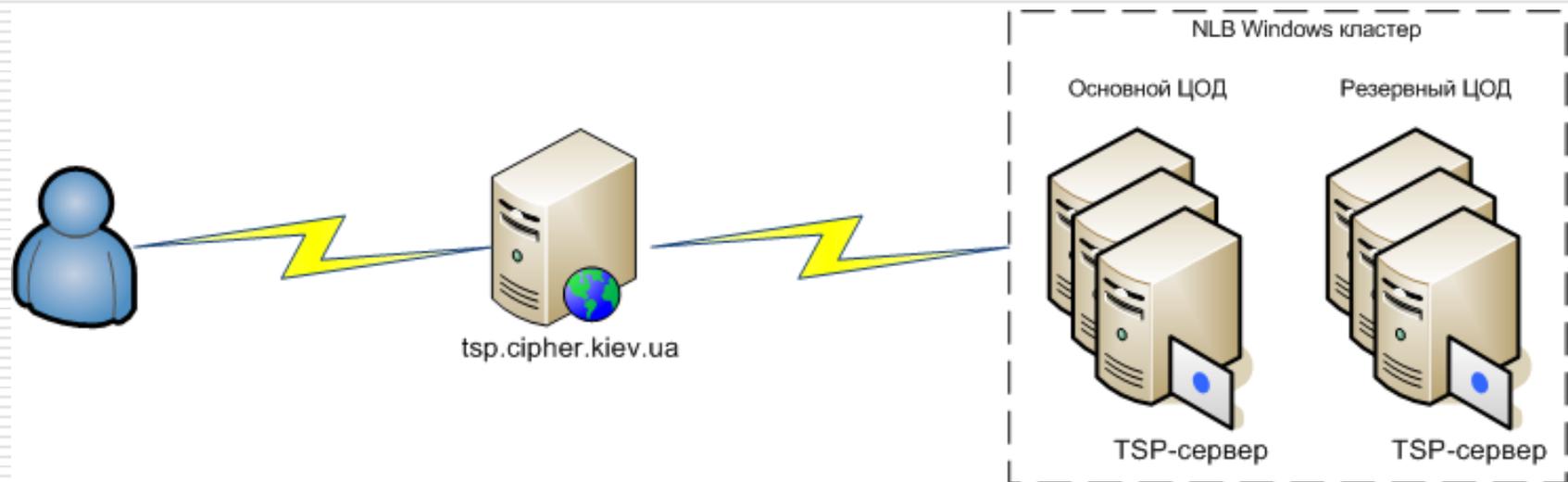
Возможности ЦСК

- ❑ Масштабирование сервисов
- ❑ Резервирование сервисов
- ❑ Мониторинг и диагностика сервисов
- ❑ Резервирование данных

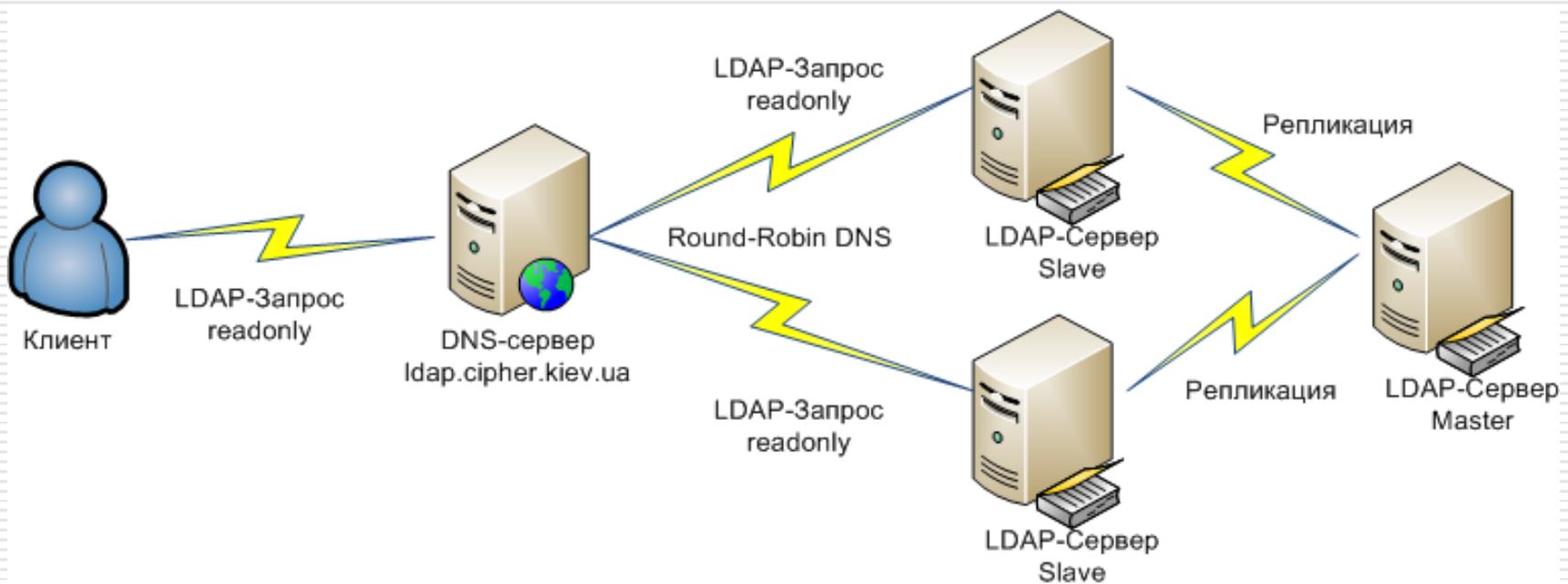
Масштабируемость OCSP



Масштабируемость TSP



Масштабируемость LDAP



Масштабируемость Сервера приложений ЦСК

Схема 1

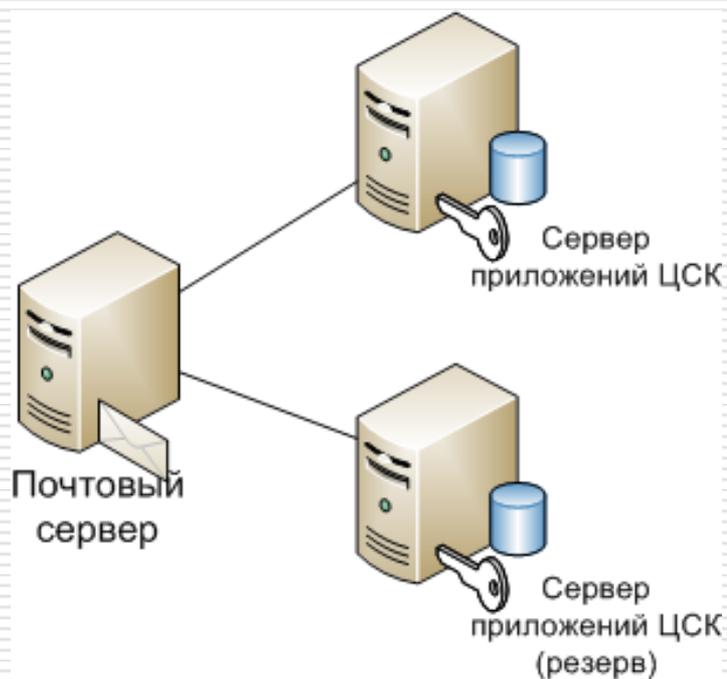
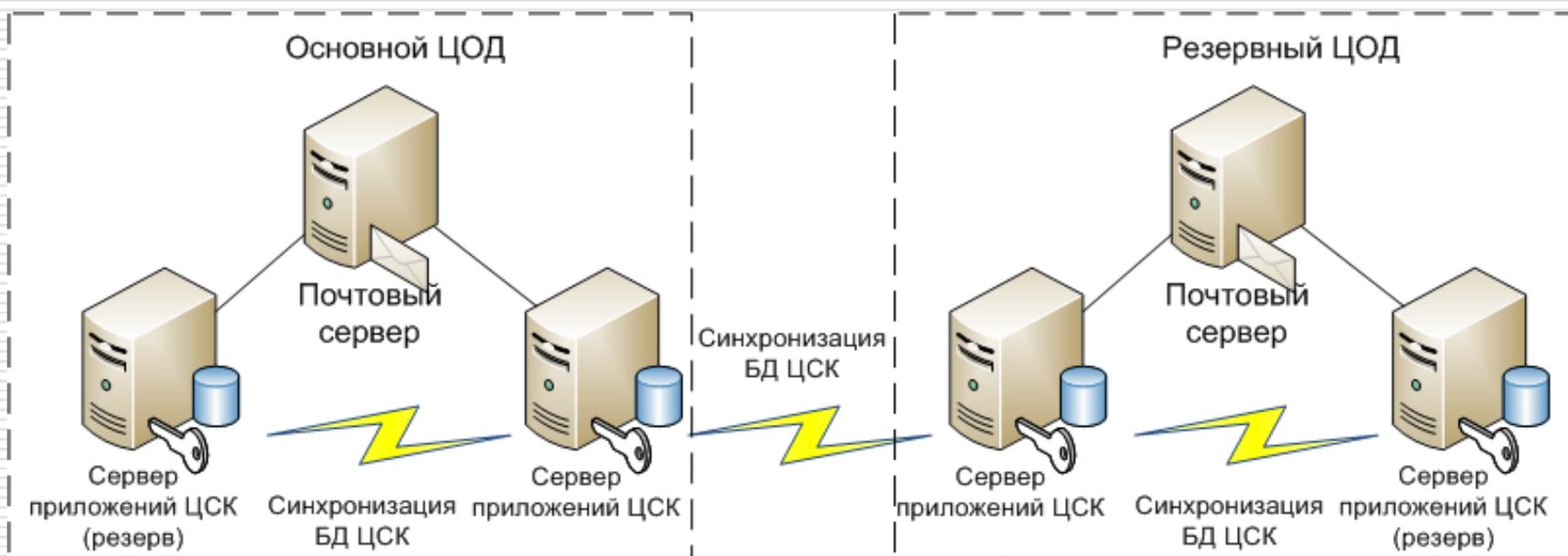


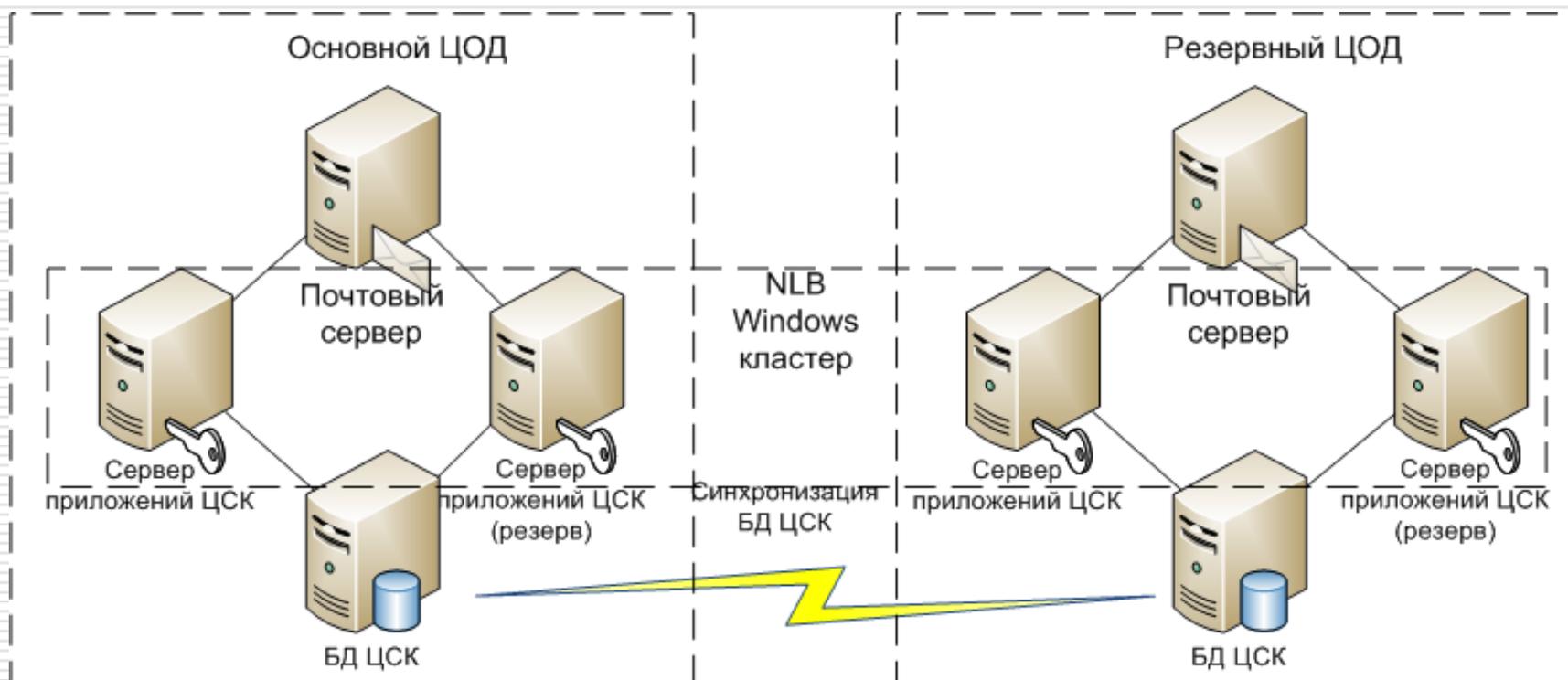
Схема 2



Масштабируемость Сервера приложений ЦСК (схема 1)



Масштабируемость Сервера приложений ЦСК (схема 2)



Мониторинг

Существующие решения:

- Nagios
- Zabbix
- Cacti
- и др.

Требуется существенная переработка:

- Целостность
- Доступность/Разграничение доступа
- Авторство
- Неотказуемость
- Диагностика/Мониторинг специфических сервисов

Мониторинг

Диагностика компонентов ЦСК (АРМ системного администратора):

- для Windows Server
 - SNMP (Informant SNMP Agent, NET-SNMP)
- для Linux Server
 - SNMP (NET-SNMP)
- Сетевое оборудование
 - SNMP

Мониторинг OCSP

- Собственные параметры SNMP
 - Подключений (всего, сейчас)
 - Состояние Listener'ов
 - Статистка успешных запросов
 - Статистика данных
 - Поток обработки (max, сейчас)
 - Время (запуска, текущее)

Мониторинг TSP

- Собственные параметры SNMP
 - Подключений (всего, сейчас)
 - Состояние Listener'ов
 - Статистка успешных запросов
 - Статистика данных
 - Поточков обработки (max, сейчас)
 - Время (запуска, текущее)

Мониторинг сервера БД TSP

Firebird Audit & Trace Service

- Не зависит от платформы

- Трассировка событий в хронологическом порядке

- Database-specific

- Connect, Disconnect

- Start/Commit/Rollback of transactions

- Prepare/Start/Finish/Free of SQL statements

- Start/Finish of stored procedures and triggers

- и др.

Мониторинг LDAP

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

Мониторинг сервера БД ЦСК

Firebird Audit & Trace Service

- Не зависит от платформы

- Трассировка событий в хронологическом порядке

- Database-specific

- Connect, Disconnect

- Start/Commit/Rollback of transactions

- Prepare/Start/Finish/Free of SQL statements

- Start/Finish of stored procedures and triggers

- и др.

Мониторинг сервера БД ЦР

Firebird Audit & Trace Service

- Не зависит от платформы

- Трассировка событий в хронологическом порядке

- Database-specific

- Connect, Disconnect

- Start/Commit/Rollback of transactions

- Prepare/Start/Finish/Free of SQL statements

- Start/Finish of stored procedures and triggers

- и др.

Мониторинг

APM Системного администратора

Файл Узлы Сервис Справка

Активные узлы

- ЦСК
 - Общие
 - OCSP
 - Primary OCSP [46.182.83.77]
 - TSP
 - Primary TSP [46.182.83.77]
 - LDAP
 - Primary LDAP [46.182.83.77]
 - Mail
 - Primary Mail [46.182.83.77]
 - Firebird DB
 - CA DB [46.182.83.77]
 - Сервер приложений
 - Primary Сервер пр... [46.182.83.77]

Сводные данные События

Описание	IP адрес	Состояние	Мониторинг	Загрузка процессора	Доступная память	Начало мониторинг	У
Основной OCSP-сервер. Micro...	46.182.83.77	Подключен	Работает	0 %	1201.81 Мб	11.04.2013 20:34:36	1:
Основной TSP-сервер. Micro...	46.182.83.77	Подключен	Работает	0 %	1201.62 Мб	11.04.2013 20:34:40	1:
Основной LDAP-каталог. RHE...	46.182.83.77	Подключен	Работает	0 %	1202.04 Мб	11.04.2013 20:34:43	1:
Основной почтовый сервер. ...	46.182.83.77	Подключен	Работает	0 %	1201.34 Мб	11.04.2013 20:34:46	1:
Основная БД ЦСК. RHEL 6.3 х...	46.182.83.77	Подключен	Работает	7 %	1202.45 Мб	11.04.2013 20:37:31	1:
Основной сервер приложен...	46.182.83.77	Подключен	Работает	7 %	1202.42 Мб	11.04.2013 20:37:54	1:

Последние события

Очистить все

Время регистрации	Тип события	Описание	Дополнительная информация
11-04-2013 20:53:45 928	Диагностика	Сервис LDAP. Превышен тайм-аут итерации	IP адрес: 46.182.83.77; Группа: LDAP; Среднее время ...
11-04-2013 20:53:03 418	Диагностика	Сервис LDAP находится в работоспособном состоянии	IP адрес: 46.182.83.77; Группа: LDAP;
11-04-2013 20:53:03 418	Диагностика	Сервис LDAP. Превышен тайм-аут итерации	IP адрес: 46.182.83.77; Группа: LDAP; Среднее время ...
11-04-2013 20:53:50 534	Диагностика	Сервис TSP находится в работоспособном состоянии	IP адрес: 46.182.83.77; Группа: TSP;

Мониторинг



Мониторинг

The screenshot displays the APM System Administrator interface. The main window is titled "APM Системного администратора" and contains several panels:

- Left Panel (Active Nodes):** A tree view showing a hierarchy of nodes under "ЦСК". The selected node is "Primary OCSPP [46.182.83]".
- Summary Panel (Общие):** Displays general information for the selected node, including IP address (46.182.83.77), description (Microsoft Windows 2008 R2 x64), CPU load (18%), free memory (1211.29 MB), and status (connected and monitoring).
- OCSP Panel:** Shows the status of the OCSP service, which is "включена" (enabled) and "работает" (working). It also displays response times and diagnostic logs.
- Processor Panel (Процессор):** Displays CPU usage statistics, including the number of cores (8), overall load (18%), user processes (14%), and system processes (4%).
- Memory Panel (Память):** Shows memory usage, including free memory (1211.29 MB), reserved memory (1679.95 MB), and disk usage for memory pages.
- Disks and Partitions Panel (Диски и разделы):** Displays disk usage for various partitions, including "D:\", "Virtual Memory", "Physical Memory", and "A:\", with pie charts showing free and used space.
- Bottom Panel (Last Events):** A table of recent events, including diagnostics and monitoring logs.

Время регистрации	Тип события	Описание	Дополнительная информация
11-04-2013 20:56:22 859	Диагностика	Сервис LDAP. Превышен тайм-аут итерации	IP адрес: 46.182.83.77; Группа: LDAP; Среднее время итерации: 2007 мс; Тайм-аут: 2000 мс;
11-04-2013 20:55:44 623	Диагностика	Сервис LDAP. Превышен тайм-аут итерации	IP адрес: 46.182.83.77; Группа: LDAP; Среднее время итерации: 2595 мс; Тайм-аут: 2000 мс;
11-04-2013 20:55:43 968	Мониторинг	Восстановлено подключение к узлу	IP адрес: 46.182.83.77; Группа: OCSPP;
11-04-2013 20:55:02 033	Мониторинг	Состояние узла	IP адрес: 46.182.83.77; Группа: OCSPP;

Мониторинг

The screenshot displays the 'APM Системного администратора' (APM System Administrator) window. The main area shows a tree view of services under 'ЦСК' (Central Control) and a corresponding log table. The log table has columns for ID, IP address, description, date, and time. A context menu is open over the log, showing options like 'Журнал мониторинга' (Monitoring Log) and 'Журнал диагностирования' (Diagnostic Log).

ID	IP	Описание события	Дата возникновения	Время возникновения
5453	46.182.83.77	Восстановлено подключение к узлу	11.04.13	20:55:43
5458	46.182.83.77	Отсутствует подключение к узлу	11.04.13	20:55:3
5457	46.182.83.77	Мониторинг узла включен	11.04.13	20:55:3
5456	46.182.83.77	Мониторинг узла выключен	11.04.13	20:55:3
5455	46.182.83.77	Восстановлено подключение к узлу	11.04.13	20:38:34
5454	46.182.83.77	Восстановлено подключение к узлу	11.04.13	20:38:11
5453	46.182.83.77	Отсутствует подключение к узлу	11.04.13	20:37:54
5452	46.182.83.77	Мониторинг узла включен	11.04.13	20:37:54
5451	46.182.83.77	Мониторинг узла выключен	11.04.13	20:37:54
5450	46.182.83.77	Отсутствует подключение к узлу	11.04.13	20:37:31
5449	46.182.83.77	Мониторинг узла включен	11.04.13	20:37:31
5448	46.182.83.77	Мониторинг узла выключен	11.04.13	20:37:31
5447	46.182.83.77	Восстановлено подключение к узлу	11.04.13	20:36:56
5446	46.182.83.77	Отсутствует подключение к узлу	11.04.13	20:36:16
5445	46.182.83.77	Мониторинг узла включен	11.04.13	20:36:16
5444	46.182.83.77	Мониторинг узла выключен	11.04.13	20:36:16
5443	46.182.83.77	Восстановлено подключение к узлу	11.04.13	20:35:29
5442	46.182.83.77	Восстановлено подключение к узлу	11.04.13	20:35:28
5441	46.182.83.77	Восстановлено подключение к узлу	11.04.13	20:35:26
5440	46.182.83.77	Восстановлено подключение к узлу	11.04.13	20:35:23
5439	46.182.83.77	Восстановлено подключение к узлу	11.04.13	20:35:20
5438	46.182.83.77	Восстановлено подключение к узлу	11.04.13	20:35:16
5437	46.182.83.77	Отсутствует подключение к узлу	11.04.13	20:34:49
5436	46.182.83.77	Мониторинг узла включен	11.04.13	20:34:10

Below the log, there is a 'Последние события' (Last Events) section with a table:

Время регистрации	Тип события	Описание	Дополнительная информация
11-04-2013 20:56:22 859	Диагностика	Сервис LDAP. Превышен тайм-аут итерации	IP адрес: 46.182.83.77; Группа: LDAP; Среднее время итерации: 2007 мс; Тайм-аут: 2000 мс;
11-04-2013 20:55:44 623	Диагностика	Сервис LDAP. Превышен тайм-аут итерации	IP адрес: 46.182.83.77; Группа: LDAP; Среднее время итерации: 2595 мс; Тайм-аут: 2000 мс;
11-04-2013 20:55:43 968	Мониторинг	Восстановлено подключение к узлу	IP адрес: 46.182.83.77; Группа: OSCP;
11-04-2013 20:55:03 033	Мониторинг	Отсутствует подключение к узлу	IP адрес: 46.182.83.77; Группа: OSCP;

Диагностика

Диагностика служб ЦСК (АРМ системного администратора):

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

Диагностика OCSP

- Диагностические запросы - время отклика
 - Подключение
 - Запрос на статус одного сертификата
 - Запрос на статус пакета сертификатов

Диагностика TSP

- Диагностические запросы - время отклика
 - Подключение
 - Запрос на метку времени
 - Запрос на пакет меток времени

Диагностика LDAP

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

Диагностика сервера приложений ЦСК

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

Диагностика сервера БД ЦСК

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

Диагностика сервера БД ЦР

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

Диагностика почтового сервера

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

Диагностика OCSP

The screenshot displays the APM System Administrator interface. The main window is titled "APM Системного администратора" and shows a tree view of active nodes on the left. The "Активные узлы" pane lists nodes such as ЦСК, OCSP, TSP, LDAP, Mail, Firebird DB, CA DB, and Server applications. The "Сводные данные" pane for the selected OCSP node shows details like IP address (46.182.83...), description (Основной Microsoft R2 x64...), and monitoring status (поднят). A "Настройки узла" dialog box is open, showing the "Общие" tab for OCSP. The "Диагностирование" section includes settings for the interval between requests (40 c), number of test requests (3), interval between iterations (100 мс), iteration timeout (2000 мс), and minimum success percentage (100 %). A checkbox "Заносить результаты диагностирования в журнал" is checked. The "Диски и разделы" pane on the right shows disk usage for D:\, Virtual Memory, Physical Memory, and A:\. The "Последние события" pane at the bottom shows a log of events, including LDAP service timeouts and OCSP diagnostics.

Настройки узла

Общие

OCSP

Порт TCP(UDP): 5001

Диагностирование

Интервал между запросами: 40 с

Число итераций выполнения тестового запроса: 3

Интервал между итерациями: 100 мс

Таймаут итерации: 2000 мс

Минимальный процент успешных итераций в запросе: 100 %

Заносить результаты диагностирования в журнал

Ok Отмена

Диски и разделы

Раздел (диск): "D:\\"

Размер: 0 M6

Свободно: 0 M6

Занято: 0 M6

Раздел (диск): "Virtual Memory"

Размер: 4452 M6

Свободно: 2772 M6

Занято: 1680 M6

Раздел (диск): "Physical Memory"

Размер: 3071 M6

Свободно: 1215 M6

Занято: 1856 M6

Раздел (диск): "A:\\"

Размер: 0 M6

Свободно: 0 M6

Занято: 0 M6

Последние события

Время регистрации	Тип события	Описание
11-04-2013 20:57:50 6	Приложение	Ротация файлов базы данных
11-04-2013 20:56:22 859	Диагностика	Сервис LDAP. Превышен тайм-аут итерации
11-04-2013 20:55:44 623	Диагностика	Сервис LDAP. Превышен тайм-аут итерации
11-04-2013 20:55:43 068	Мониторинг	Сервис OCSP. IP адрес: 46.182.83.77; Группа: LDAP; Среднее время итерации: 2595 мс; Тайм-аут: 2000 мс;

Диагностика TSP

The screenshot displays the APM System Administrator interface. The main window shows a tree view of active nodes under 'ЦСК', including 'Общие', 'OCSP', 'Primary OCSP', 'TSP', 'Primary TSP', 'LDAP', 'Primary LDAP', 'Mail', 'Primary Mail', 'Firebird DB', 'CA DB', and 'Сервер приложений'. The 'Primary TSP' node is selected, and its 'Настройки узла' (Node Settings) dialog is open.

The 'Настройки узла' dialog has two tabs: 'Общие' (General) and 'TSP'. The 'TSP' tab is active, showing the following settings:

- Порт TCP(UDP): 318
- Диагностирование (Diagnostic):
 - Интервал между запросами: 40 с
 - Число итераций выполнения тестового запроса: 3
 - Интервал между итерациями: 100 мс
 - Таймаут итерации: 2000 мс
 - Минимальный процент успешных итераций в запросе: 100 %
 - Заносить результаты диагностирования в журнал

The background window shows the 'Сводные данные' (Summary) tab for the selected node, displaying various system metrics such as CPU load (11%), free memory (1214.42 MB), and monitoring status (active).

At the bottom, the 'Последние события' (Recent Events) table shows the following entries:

Время регистрации	Тип события	Описание
11-04-2013 20:57:50.6	Приложение	Ротация файлов базы данных
11-04-2013 20:56:22.859	Диагностика	Сервис LDAP. Превышен тайм-аут итерации
11-04-2013 20:55:44.623	Диагностика	Сервис LDAP. Превышен тайм-аут итерации
11-04-2013 20:55:13.068	Мониторинг	Время работы без выключения (перезагрузки): 16 дн. 9 ч. 16 мин. 16 сек.

Диагностика LDAP

The screenshot displays the APM System Administrator interface. The main window shows a tree view of active nodes under 'ЦСК', including 'Общие', 'OCSP', 'TSP', 'LDAP', 'Mail', and 'Сервер приложений'. The 'LDAP' node is selected, and its 'Настройки узла' (Node Settings) dialog is open. The 'Общие' (General) tab is active, showing the following configuration:

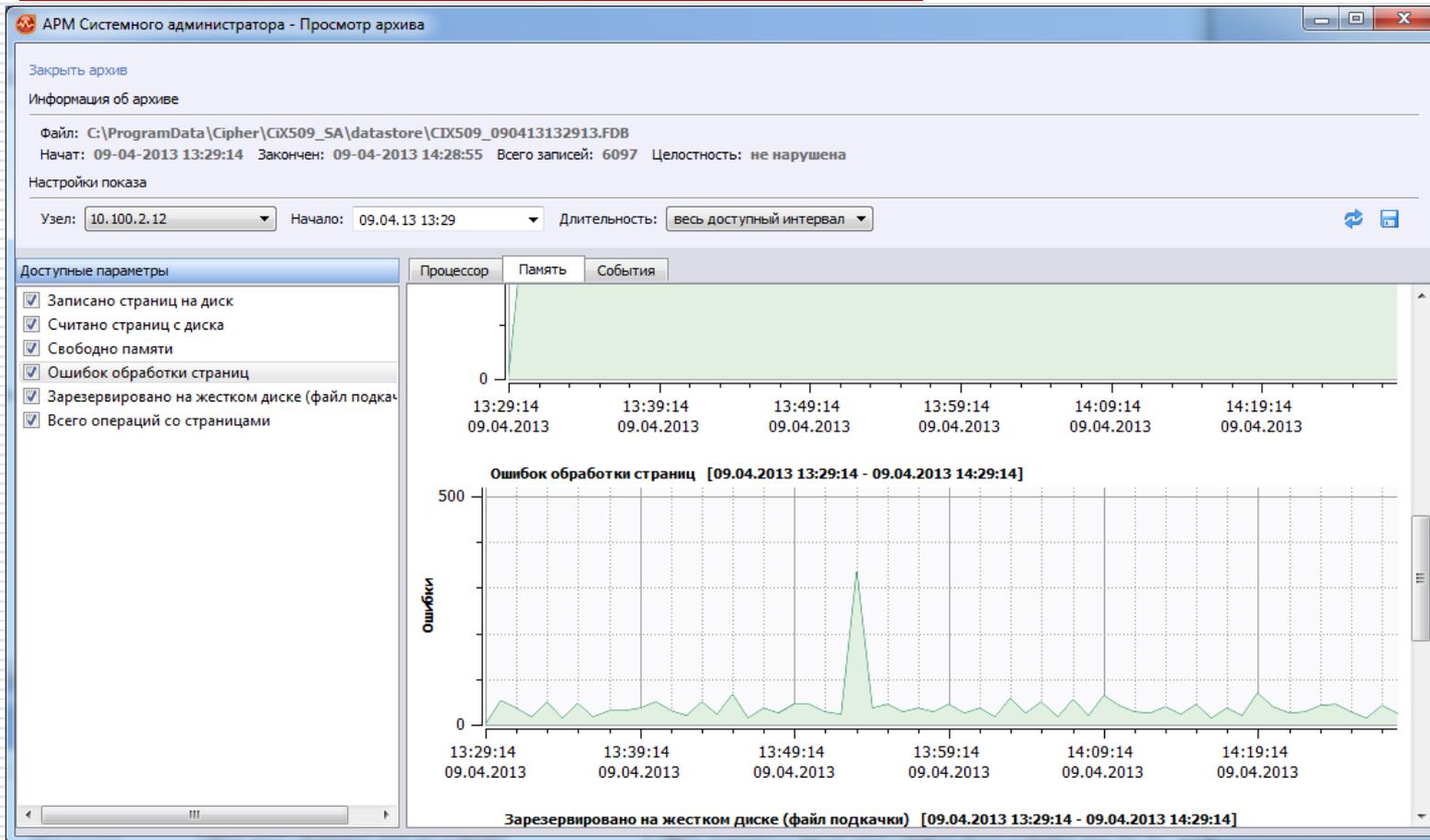
- Порт TCP(UDP): 389
- Базовое DN: dc=cipher,dc=com
- DN пользователя: cn=admin,dc=cipher,dc=com
- Пароль: (masked)
- Показать пароль

The 'Диагностирование' (Diagnosis) section includes the following settings:

- Интервал между запросами: 40 с
- Число итераций выполнения тестового запроса: 3
- Интервал между итерациями: 100 мс
- Таймаут итерации: 2000 мс
- Минимальный процент успешных итераций в запросе: 100 %
- Заносить результаты диагностирования в журнал

At the bottom of the dialog, 'Ok' and 'Отмена' (Cancel) buttons are visible. The background window shows a 'Сводные данные' (Summary) pane with various system metrics and a 'Последние события' (Recent Events) log at the bottom.

Работа с архивом



Резервируемость сервисов

- ❑ OSCP-сервер, решается в рамках масштабируемости
- ❑ TSP-сервер, решается в рамках масштабируемости
- ❑ LDAP-сервер, решается в рамках масштабируемости
- ❑ Сервер приложений ЦСК, решается в рамках масштабируемости

Резервируемость сервера приложений ЦСК

Схема 1

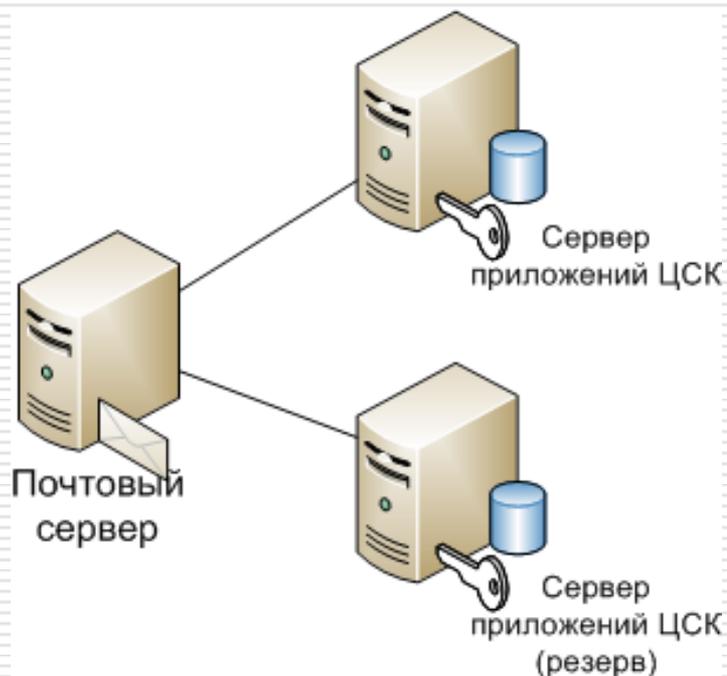


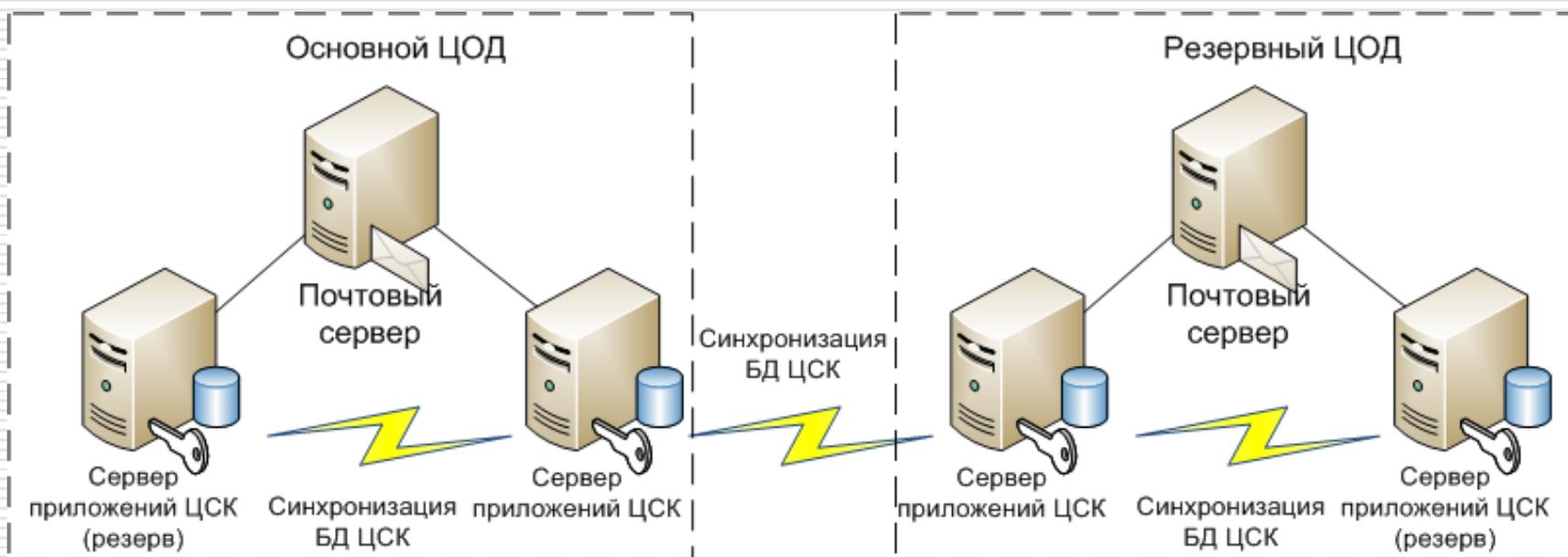
Схема 2



Резервируемость сервера приложений ЦСК (1)

- ❑ Сервера приложений ЦСК организуются в NLB Windows кластер
- ❑ БД ЦСК выносятся на отдельный сервер с общим доступом узлов кластера

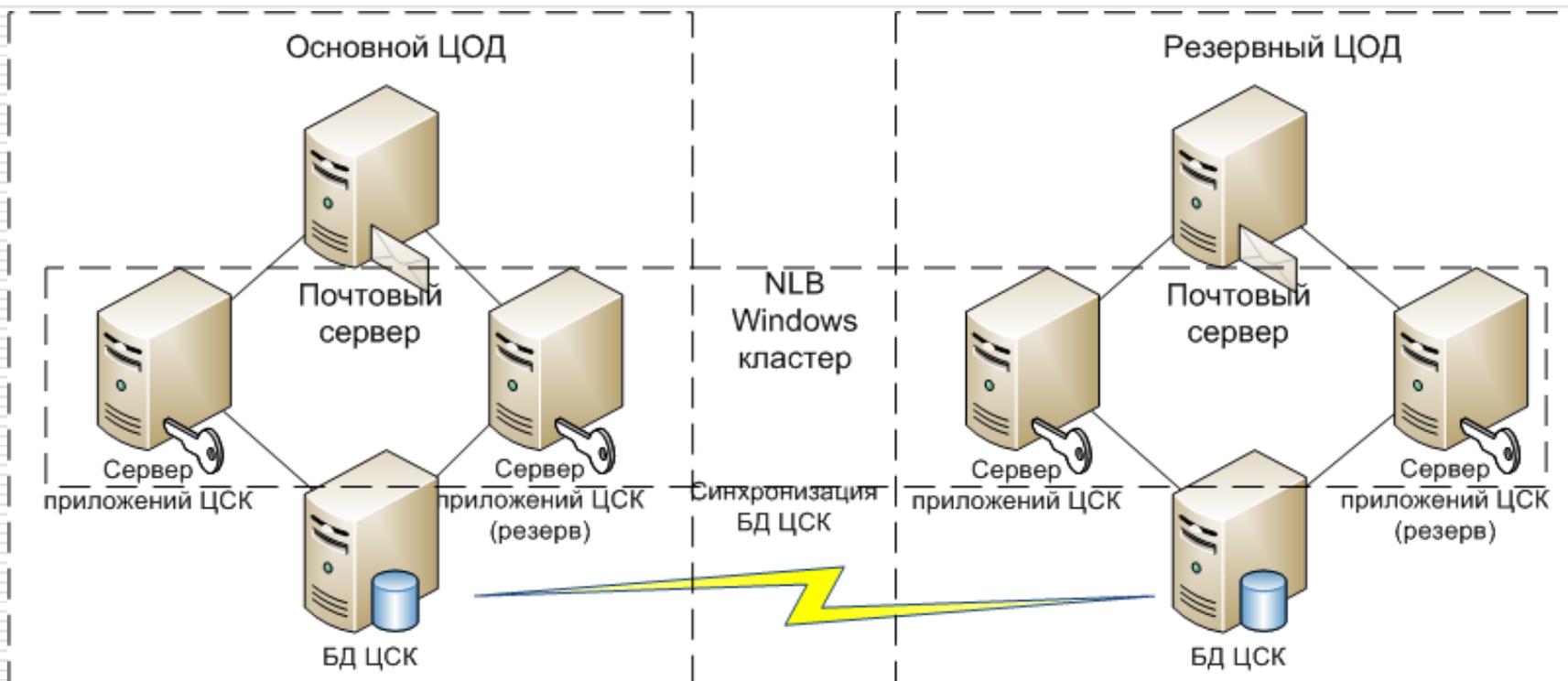
Резервируемость сервера приложений ЦСК (1)



Резервируемость сервера приложений ЦСК (2)

- ❑ Сервера приложений ЦСК достигается за счет полного клонирования
- ❑ Основной ведет запись в свою БД и в БД резервного Сервера приложений ЦСК
- ❑ Периодическая синхронизации БД ЦСК

Резервируемость сервера приложений ЦСК (2)



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.
- и т.д.

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 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.cipher.kiev.ua>

СУБД FireBird

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