

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

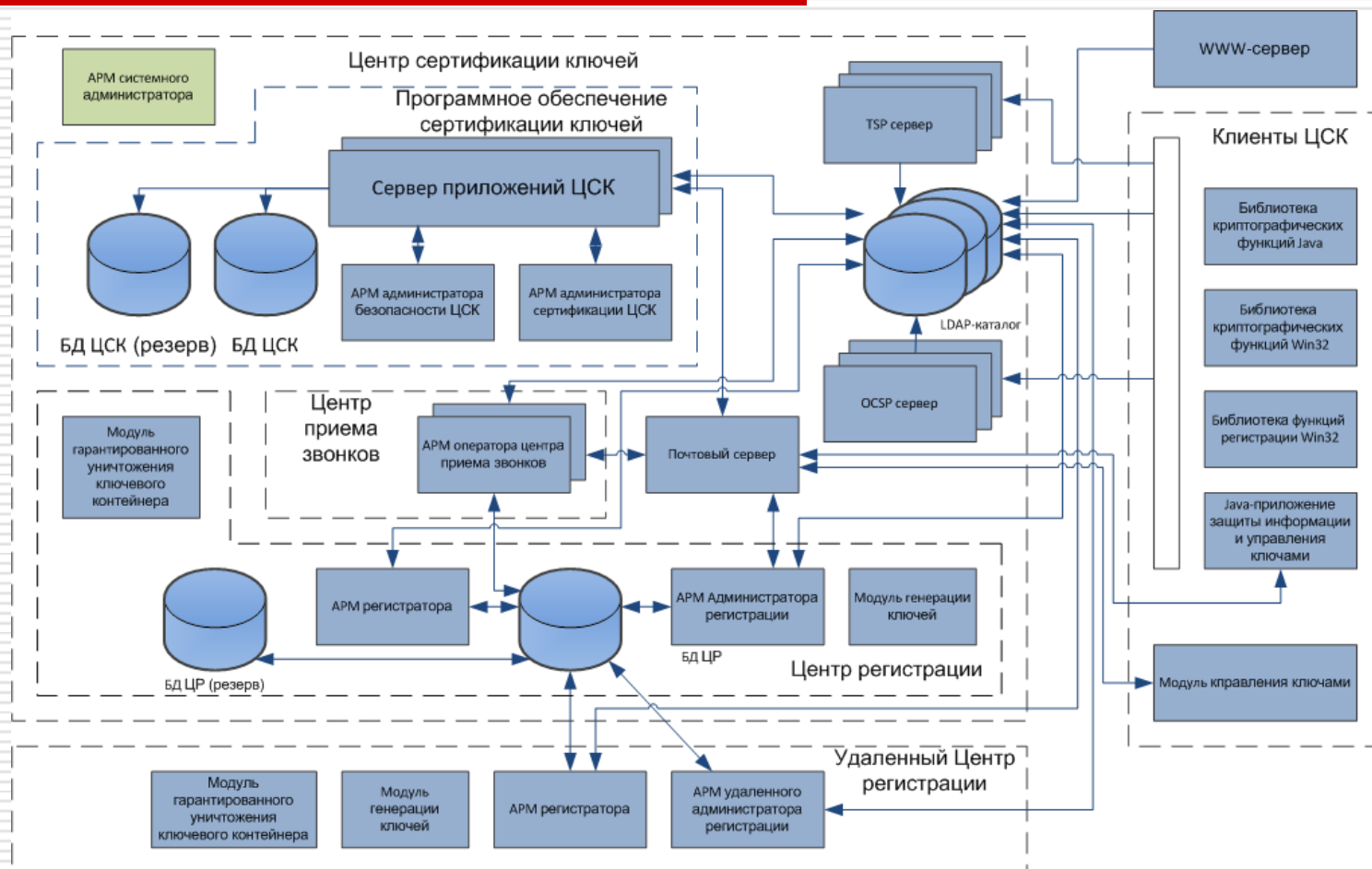


Схема развертывания (1)

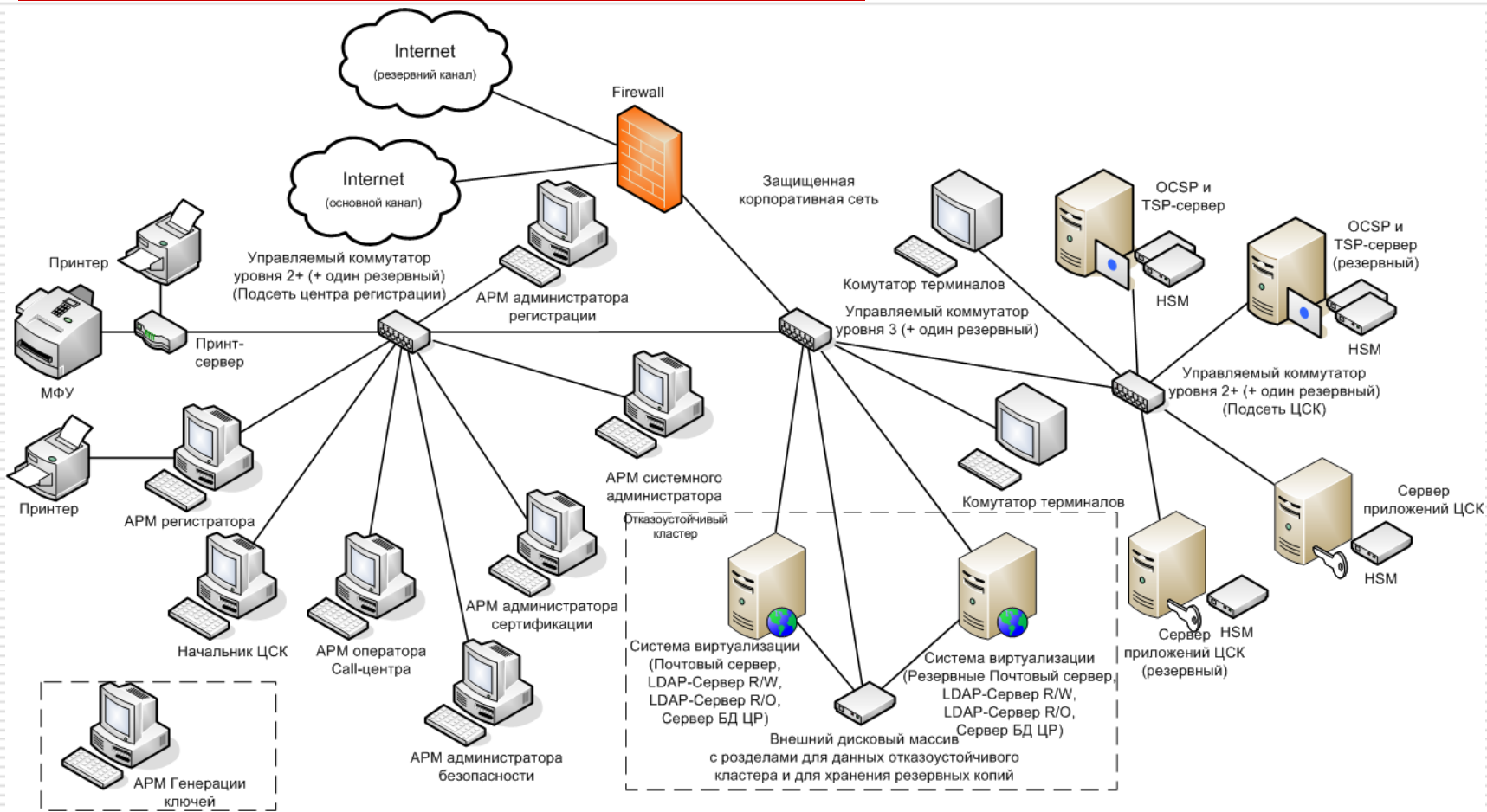
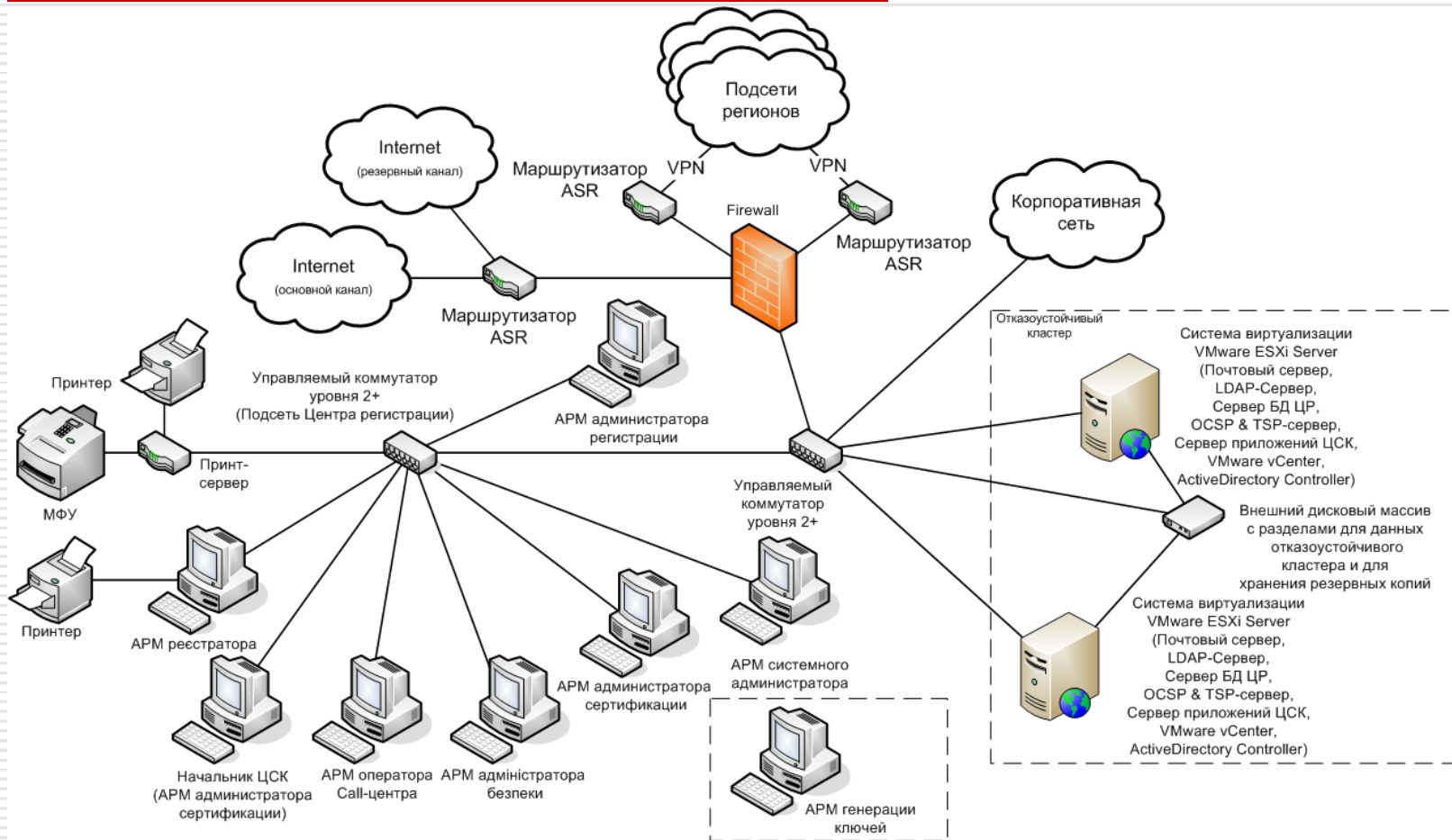


Схема развертывания (2)



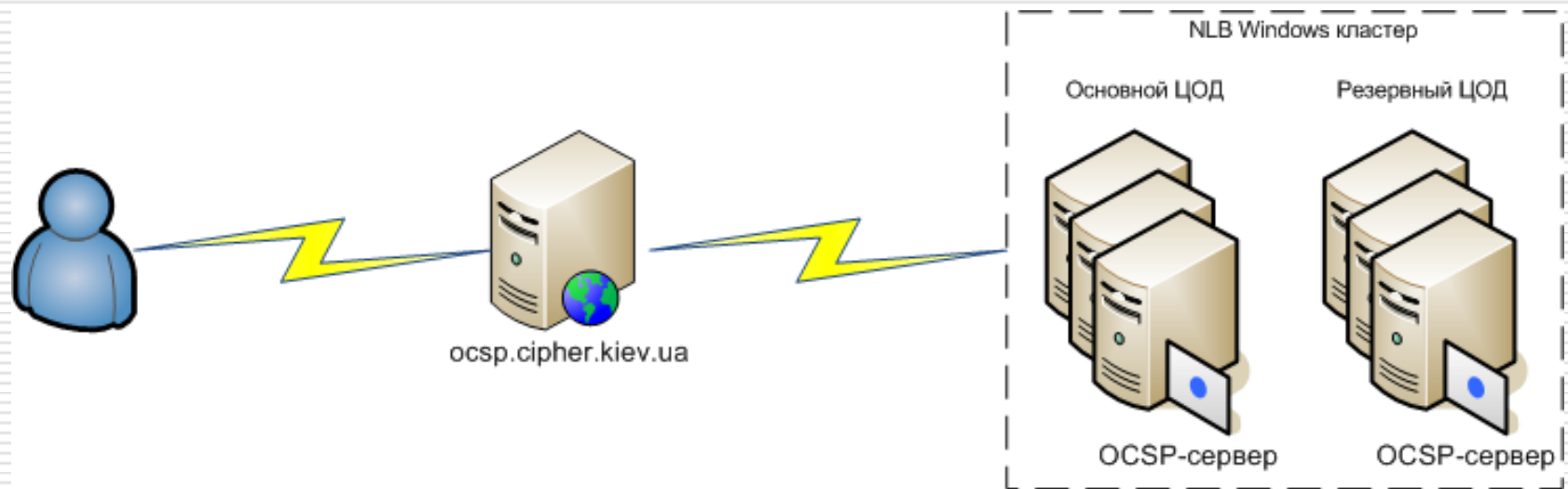
СКЗИ «Шифр-Х.509»

НАДЕЖНОСТЬ И ПРОИЗВОДИТЕЛЬНОСТЬ

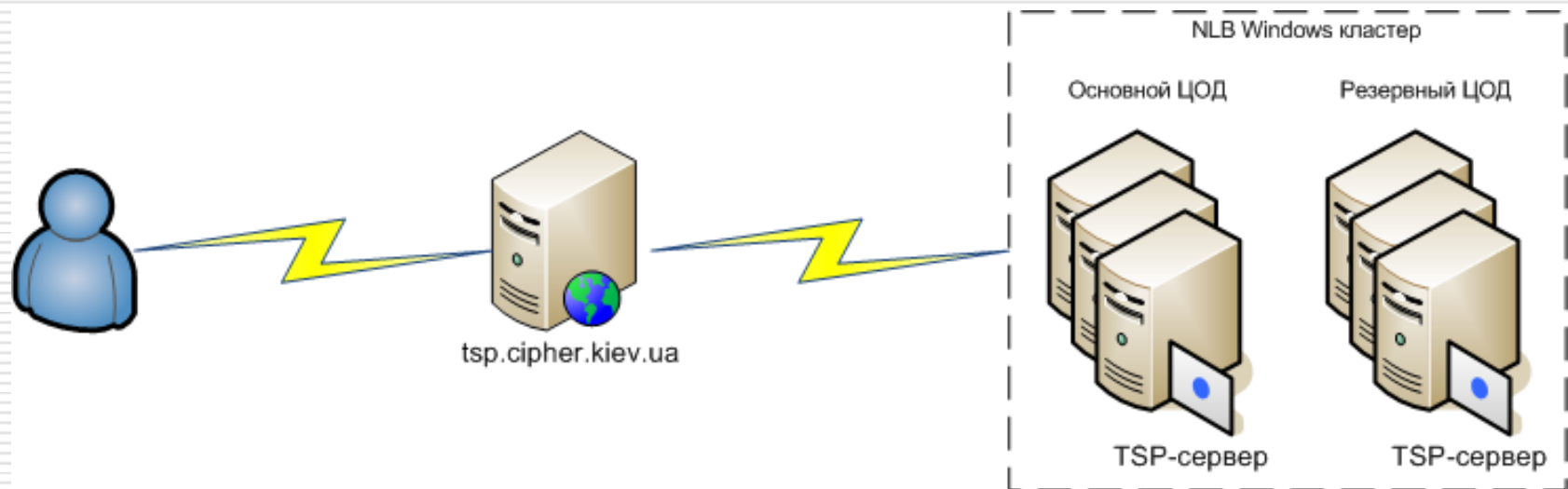
Возможности ЦСК

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

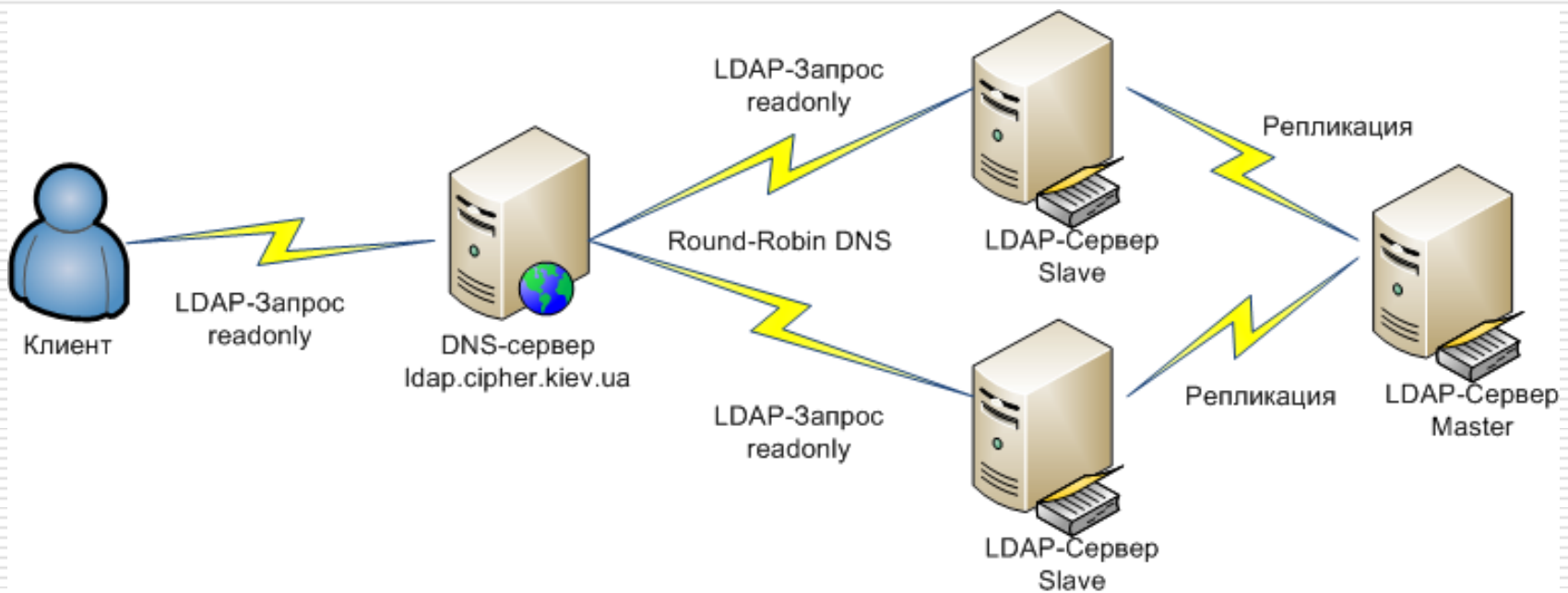
Масштабируемость OCSP



Масштабируемость TSP



Масштабируемость LDAP



Масштабируемость Сервера приложений ЦСК

Схема 1

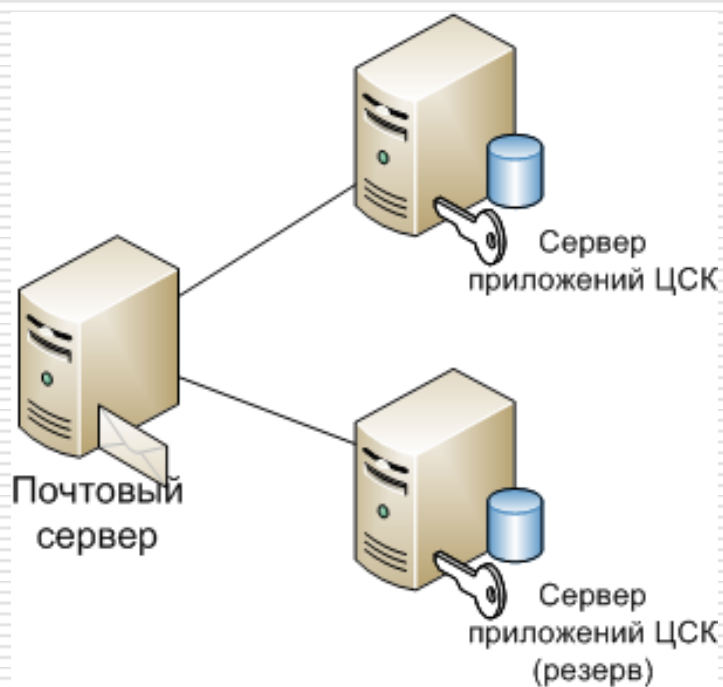
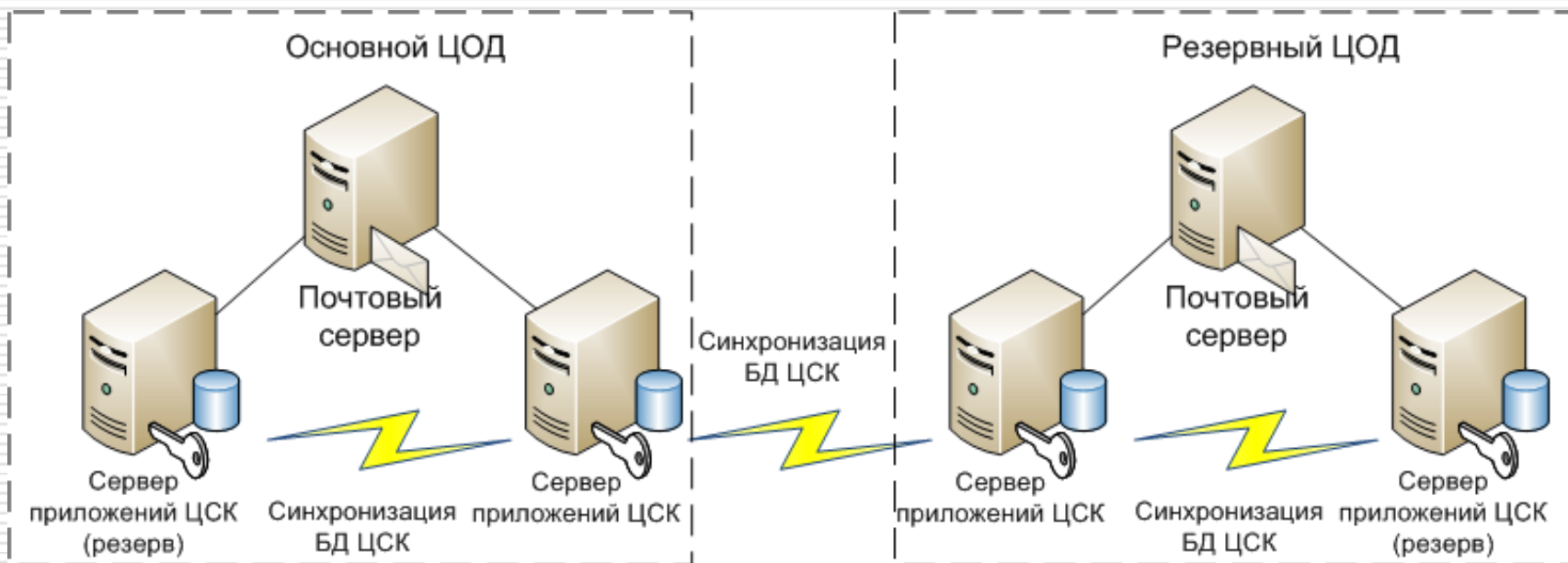


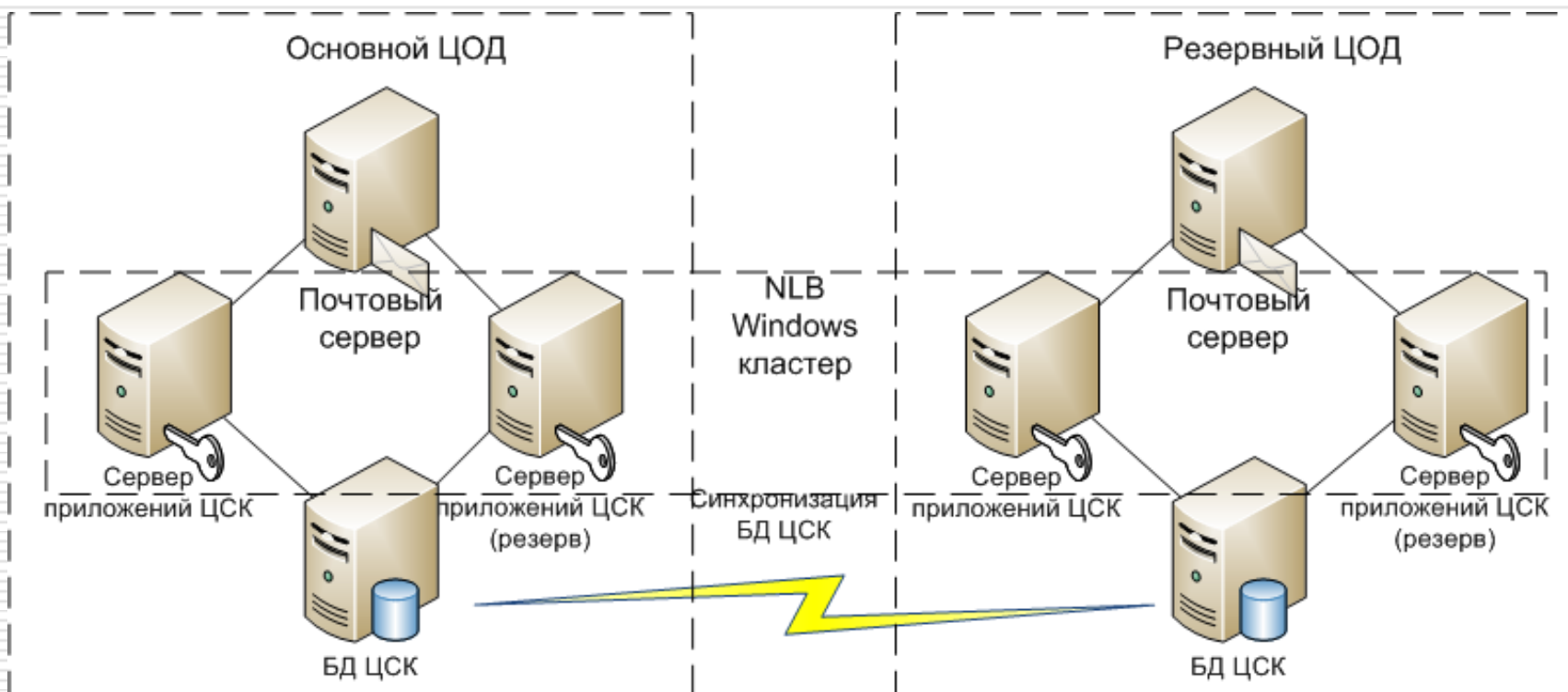
Схема 2



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)
 - Поток 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	y
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

The screenshot displays the APM System Administrator interface. The left sidebar shows a tree view of active nodes under the 'ЦСК' folder, including 'Общие', 'OCSIP', 'TSP', 'LDAP', 'Mail', 'Firebird DB', and 'Сервер приложений'. The main area is divided into several panels:

- Общие (General):**
 - IP адрес: 46.182.83.77
 - Описание: Основной OCSIP-сервер. Microsoft Windows 2008 R2 x64.
 - Загрузка процессора: 11 %
 - Свободно памяти: 1139.59 МБ
 - Состояние: подключен
 - Мониторинг: работает
 - Время работы без выключения (перезагрузки): 16 дн. 9 час. 42 мин. 39 сек.
 - Начало мониторинга: 11.04.2013 20:34:36
 - Последний успешный запрос: 11.04.2013 20:53:56
- OCSIP:**
 - Диагностика: включена
 - Состояние сервиса: работает
 - Текущее время отклика: 20 мс
 - Среднее время отклика: 18 мс
 - Готовность: 1.0000
 - Начало диагностирования: 11.04.2013 20:52:51
 - Последний успешный запрос: 11.04.2013 20:53:31
 - Выключить диагностику
- Процессор (Processor):**
 - Общее количество ядер: 8
 - Загрузка процессора: 11 %
 - Пользовательские процессы: 6 %
 - Системные процессы: 5 %
 - Обработка прерываний: 2 %
- Память (Memory):**
 - Свободно памяти: 1139.59 МБ
 - Зарезервировано на жестком диске (файл подкачки): 1768.68 МБ
 - Записано страниц на диск: 0 стр.
 - Считано страниц с диска: 226 стр.
 - Всего операций со страницами: 226
 - Ошибка обработки страниц: 4746
- Команды (Commands):**
 - Выключить мониторинг
 - Редактировать свойства узла
- Последние события (Recent Events):**

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 итерации: 3031 мс; Тайм-аут: 2000 мс;
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 итерации: 2194 мс; Тайм-аут: 2000 мс;
11-04-2013 20:53:03 418	Диагностика	Сервис LDAP находится в работоспособном состоянии	IP адрес: 46.182.83.77; Группа: LDAP;

Мониторинг



Мониторинг

APM Системного администратора

Файл Узлы Сервис Справка

Активные узлы

- ЦСК
 - Общие
 - OCSIP
 - Primary OCSIP [46.182.83]
 - TSP
 - Primary TSP [46.182.83]
 - LDAP
 - Primary LDAP [46.182.83]
 - Mail
 - Primary Mail [46.182.83]
 - Firebird DB
 - CA DB [46.182.83]
 - Сервер приложений
 - Primary Сервер пр... [46.182.83]

Сводные данные Производительность События

Общие

IP адрес: 46.182.83.77
 Описание: Основной OCSIP-сервер. Microsoft Windows 2008 R2 x64.
 Загрузка процессора: 18 %
 Свободно памяти: 1211.29 МБ
 Состояние: подключен
 Мониторинг: работает
 Вреня работы без выключения (перезагрузки): 16 дн. 9 час. 45 мин. 27 сек.
 Начало мониторинга: 11.04.2013 20:55:03
 Последний успешный запрос: 11.04.2013 20:56:43

Команды

Выключить мониторинг
 Редактировать свойства узла

OCSIP

Диагностика: включена
 Состояние сервиса: работает
 Текущее время отклика: 20 мс
 Среднее время отклика: 19 мс
 Готовность: 1.0000
 Начало диагностирования: 11.04.2013 20:52:51
 Последний успешный запрос: 11.04.2013 20:56:11

Выключить диагностику

Процессор

Общее количество ядер: 8
 Загрузка процессора: 18 %
 Пользовательские процессы: 14 %
 Системные процессы: 4 %
 Обработка прерываний: 1 %

Память

Свободно памяти: 1211.29 МБ
 Зарезервировано на жестком диске (файл подкачки): 1679.95 МБ
 Записано страниц на диск: 0 стр.
 Считано страниц с диска: 83 стр.
 Всего операций со страницами: 83
 Ошибок обработки страниц: 8517

Диски и разделы

Раздел (диск): "D:\\"
 Размер: 0 МБ
 Свободно: 0 МБ
 Занято: 0 МБ

Раздел (диск): "Virtual Memory"
 Размер: 4452 МБ
 Свободно: 2773 МБ
 Занято: 1679 МБ

Раздел (диск): "Physical Memory"
 Размер: 3071 МБ
 Свободно: 1216 МБ
 Занято: 1855 МБ

Раздел (диск): "A:\\"
 Размер: 0 МБ
 Свободно: 0 МБ

Последние события

Очистить все

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: OCSIP;
11-04-2013 20:55:03 033	Мониторинг	Состояние подключения к узлу	IP адрес: 46.182.83.77; Группа: OCSIP;

Мониторинг

APM Системного администратора

Файл Узлы Сервис Справка

Активные узлы

Сводные данные Производительность События

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]

Журнал мониторинга

ID	Дата возникновения	Время возникновения	Описание события
5453	11.04.13	20:55:43	Восстановлено подключение к узлу
5458	11.04.13	20:55:3	Отсутствует подключение к узлу
5457	11.04.13	20:55:3	Мониторинг узла включен
5456	11.04.13	20:55:3	Мониторинг узла выключен
5455	11.04.13	20:38:34	Восстановлено подключение к узлу
5454	11.04.13	20:38:11	Восстановлено подключение к узлу
5453	11.04.13	20:37:54	Отсутствует подключение к узлу
5452	11.04.13	20:37:54	Мониторинг узла включен
5451	11.04.13	20:37:54	Мониторинг узла выключен
5450	11.04.13	20:37:31	Отсутствует подключение к узлу
5449	11.04.13	20:37:31	Мониторинг узла включен
5448	11.04.13	20:37:31	Мониторинг узла выключен
5447	11.04.13	20:36:56	Восстановлено подключение к узлу
5446	11.04.13	20:36:16	Отсутствует подключение к узлу
5445	11.04.13	20:36:16	Мониторинг узла включен
5444	11.04.13	20:36:16	Мониторинг узла выключен
5443	11.04.13	20:35:29	Восстановлено подключение к узлу
5442	11.04.13	20:35:28	Восстановлено подключение к узлу
5441	11.04.13	20:35:26	Восстановлено подключение к узлу
5440	11.04.13	20:35:23	Восстановлено подключение к узлу
5439	11.04.13	20:35:20	Восстановлено подключение к узлу
5438	11.04.13	20:35:16	Восстановлено подключение к узлу
5437	11.04.13	20:34:49	Отсутствует подключение к узлу
5436	11.04.13	20:34:40	Мониторинг узла включен

Последние события

Очистить все

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: OCSP;
11-04-2013 20:55:43 933	Мониторинг	Отсутствует подключение к узлу	IP адрес: 46.182.83.77; Группа: OCSP;

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. A central dialog box titled "Настройки узла" (Node Settings) is open, showing the "Общие" (General) tab for the OCSP node. The "Диагностирование" (Diagnosis) section is expanded, showing the following settings:

- Порт TCP(UDP): 5001
- 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 interface shows a tree view of active nodes (ЦСК, OCSP, TSP, LDAP, Mail, Firebird DB, CA DB, Server applications) and a "Диски и разделы" (Disks and partitions) section with pie charts for D:\, Virtual Memory, Physical Memory, and A:\. A "Последние события" (Recent events) table is visible at the bottom.

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 20:55:43.968	Мониторинг	Включение мониторинга

Диагностика TSP

The screenshot displays the APM System Administrator interface. The main window shows a tree view of active nodes under 'ЦСК'. The 'Primary TSP' node is selected. A 'Node Settings' dialog box is open, showing the 'TSP' configuration page. The 'Port TCP(UDP)' is set to 318. The 'Diagnostic' section includes the following settings:

- Interval between requests: 40 c
- Number of iterations of test request execution: 3
- Interval between iterations: 100 ms
- Iteration timeout: 2000 ms
- Minimal percentage of successful iterations in request: 100 %
- Save diagnostic results to the log

The background interface shows a summary of system metrics for the selected node, including CPU load (11%), free memory (1214.42 MB), and monitoring status (active). The bottom of the window shows a log of recent events, including a 'Service LDAP. Exceeded iteration timeout' error.

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 box is open. The 'Общие' (General) tab is active, showing the following configuration:

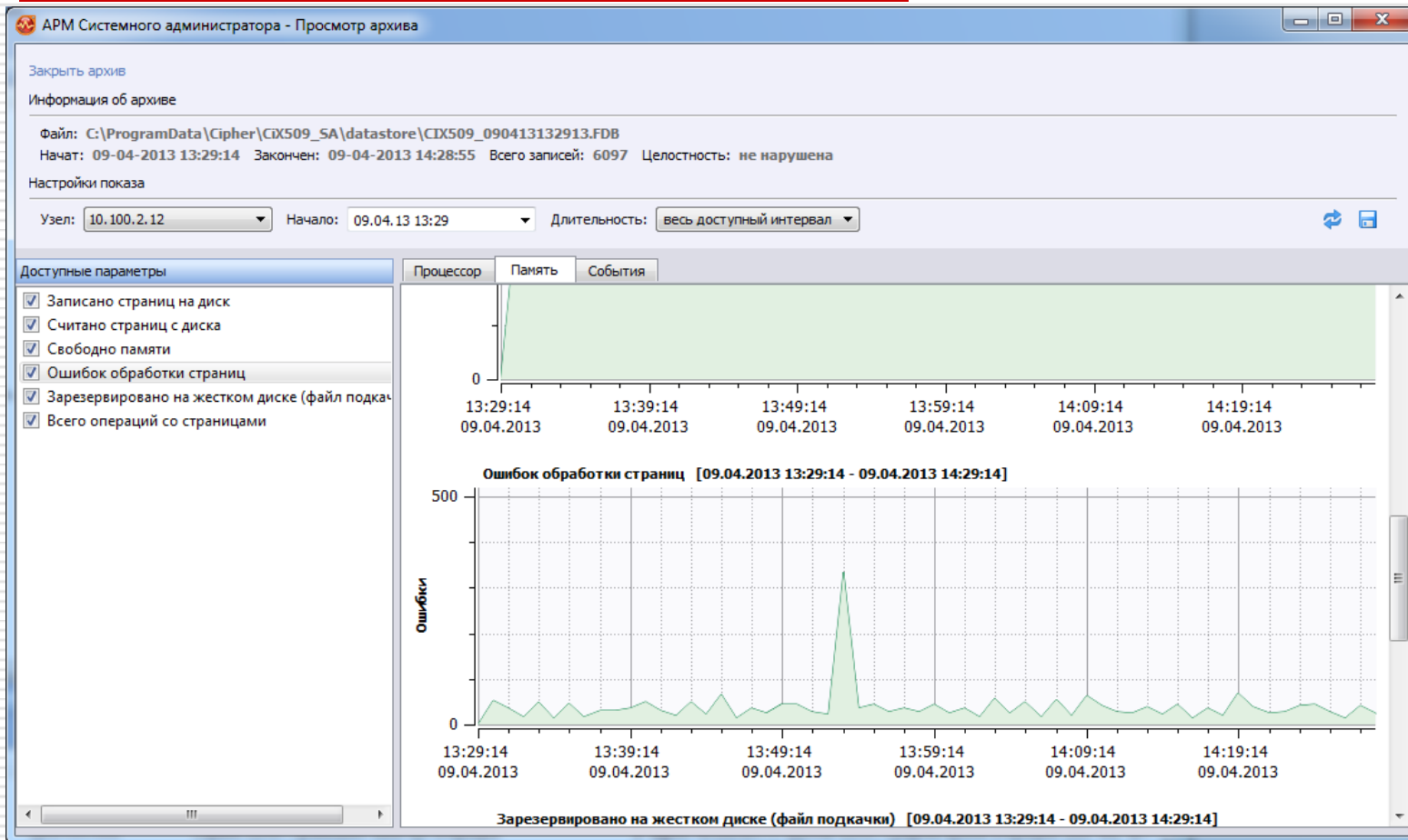
- Порт TCP(UDP): 389
- Базовое DN: dc=cipher,dc=com
- DN пользователя: cn=admin,dc=cipher,dc=com
- Пароль: (masked)
- Показать пароль

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

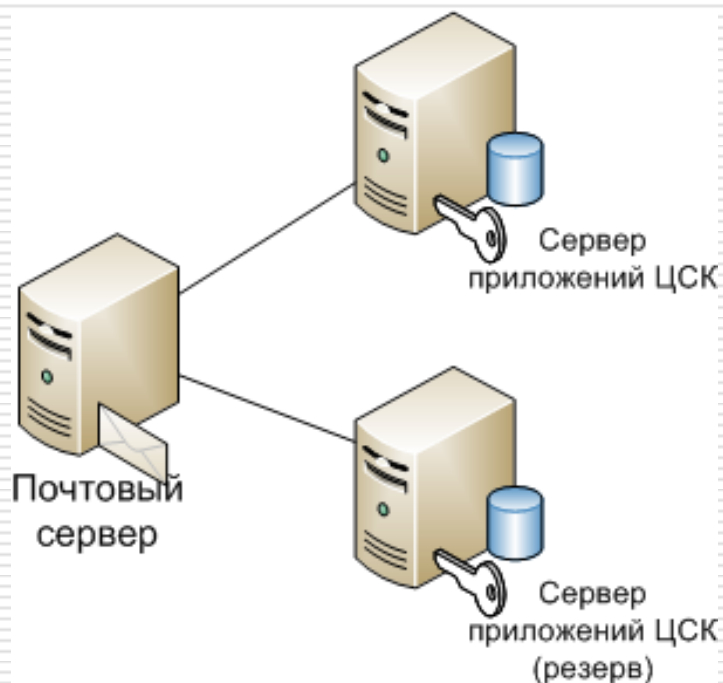


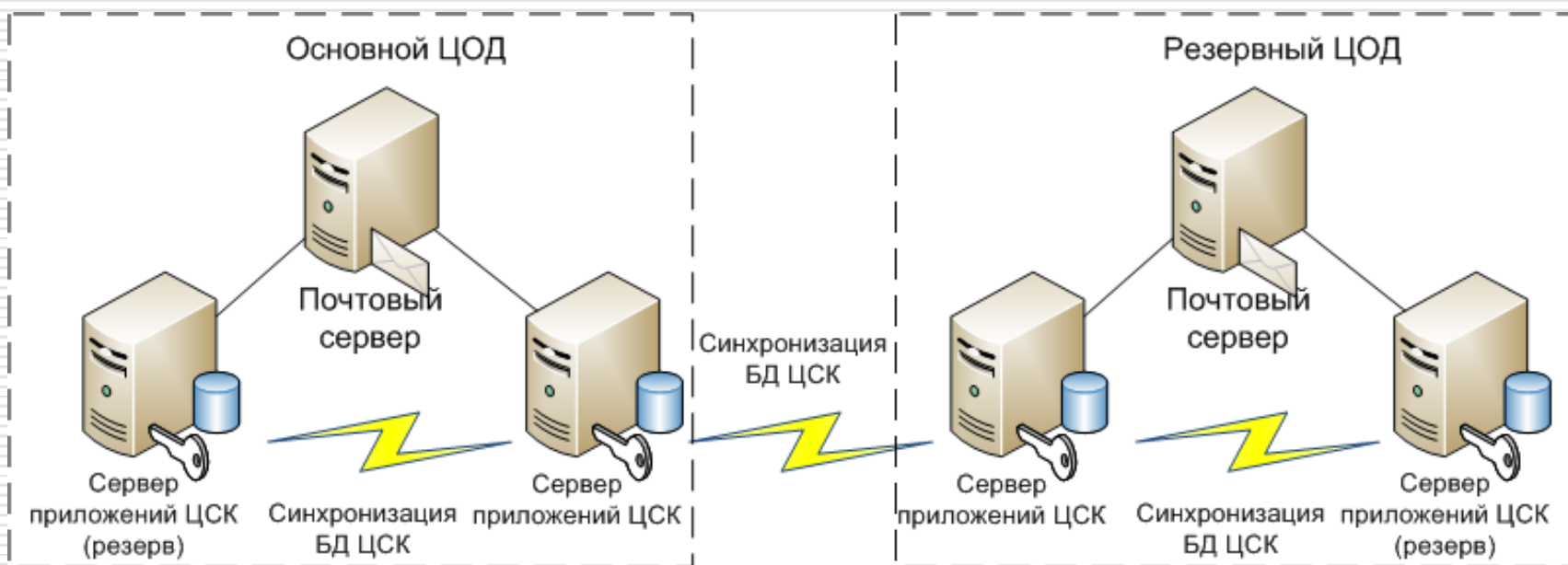
Схема 2



Резервируемость сервера приложений ЦСК (1)

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

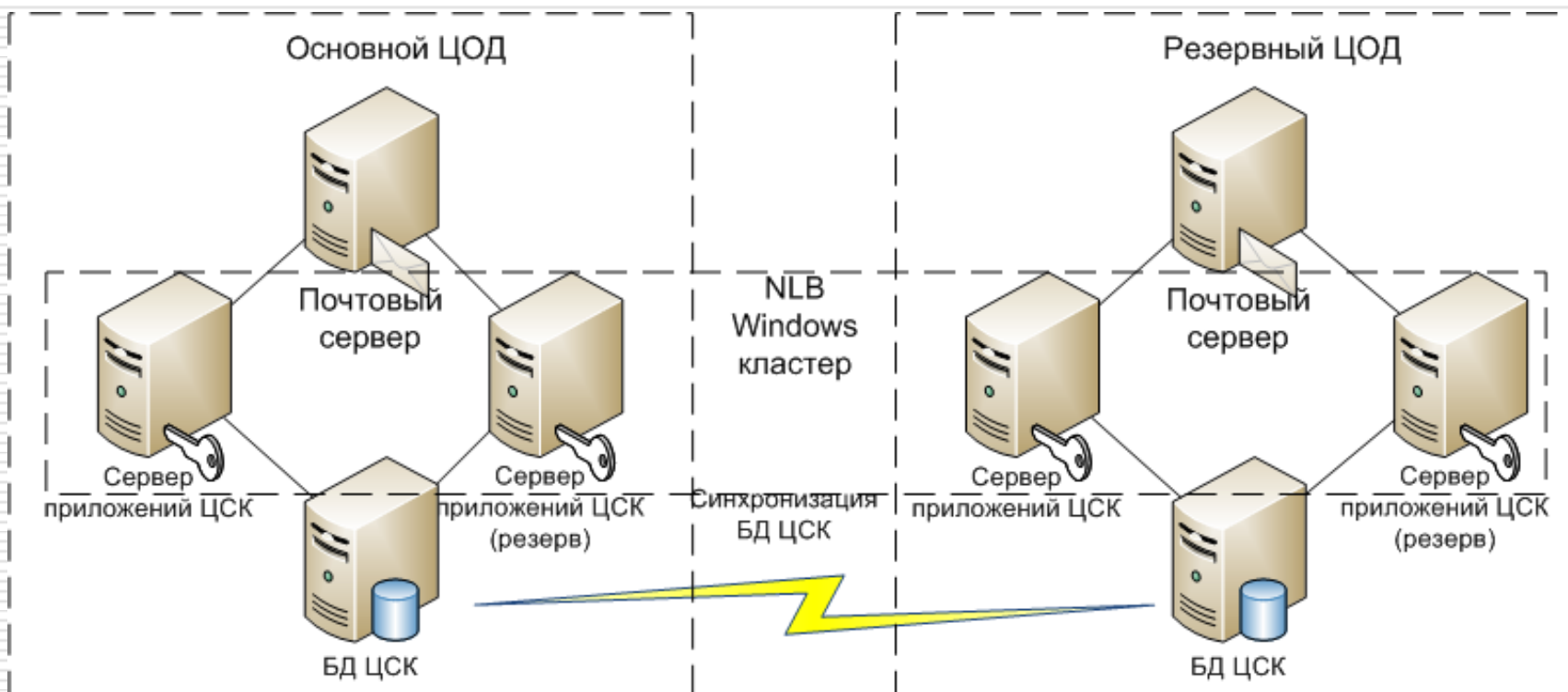
Резервируемость сервера приложений ЦСК (1)



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