# Описание сети.

В данном документе рассматривается состояние компьютерной сети компании _____ на момент 1.02 — 2.03.2010.

Анализируемая сеть состоит из:

1. Сервера — 7 шт.
2. Компьютеры — 135 шт. (данные получены из базы данных Active Directory)
3. Управляемые коммутаторы (свичи) — 5 шт. (данные получены посредством сетевого сканирования)
4. Коммутационные линии (кабель категории UTP-5e различных версий, коннекторы RJ-45).

Сеть состоит их 2х доменов Windows Server 2003: …….

В сети представлен один AD сайт в каждом домене. Каждый контроллер домена является хозяином всех операций для своего домена (RID, PDC и др.).

Функциональные уровни доменов и лесов:……

В домене …….. представлено 6 серверов выполняющих следующие задачи: ……..

Локальная сеть компании состоит из одной подсети 192.168.3.0/24.

## 1. Инфраструктурные и общие проблемы компьютерной сети.

| п.№ | |
|---|---|
| 1 | **Проблема:**<br>В сети существует 1 контроллер домена для каждого домена (…… и ……)<br>**Существующие риски:**<br>Выход из строя контроллера домена приведёт к полной неработоспособности домена (пользователи не смогут зайти в свои компьютеры, перестанет работать интернет и почта и многое другое).<br>**Практические рекомендации:**<br>Либо установка дополнительного оборудования и размещение на нём контроллеров домена, либо поднятие роли контроллера домена на существующих серверах (к примеру на ……).<br>Действия в данном случае требуют оценки многих факторов, как технологических, так и финансовых.<br>**Плюсы и минусы предложенных практических рекомендаций:**<br>+<br>Отказоустойчивость процесса аутентификации пользователей в домене, DNS, WINS и др.<br>-<br>Большие затраты времени и, вероятно, значительные финансовые затраты. |
| 2 | **Проблема:**<br>На серверах и многих компьютерах не включены автоматические обновления Microsoft. Отсутствует политика установки обновлений.<br>**Существующие риски:**<br>Обновления Microsoft закрывают используемые взломщиками уязвимости в операционных системах Windows и других продуктах компании Microsoft. Отключенные автоматические обновления делают сервера и компьютеры уязвимыми для хакерских атак.<br>**Практические рекомендации:**<br>1. Включение на всех компьютерах и серверах в компьютерной сети автоматических обновлений. Для экономии интернет трафика в сети может быть установлен WSUS сервер, который централизованно скачивает выпущенные обновления с сайта update.microsoft.com и раздаёт их по локальной сети всем серверам и компьютерам.<br>2. Создание регламента установки обновлений на сервера и компьютеры. К примеру, критические обновления должны быть установлены в течении недели. Обычные обновления в течение месяца и др. Естественно, выполнение данного регламента должно контролироваться системным администратором как вручную, так и автоматическими средствами (например, средствами WSUS).<br>**Плюсы и минусы предложенных практических рекомендаций:**<br>+<br>Устранение существующих рисков<br>-<br>Значительные временные затраты. |
| 3 | **Проблема:**<br>Для администрирования серверов используется программное обеспечение DameWare. |

| | |
|---|---|
| | **Существующие риски:**<br>ПО DameWare может вызывать конфликты с существующими драйверами операционной системы (в частности видеокарты) и падение сервера.<br>Клиентская служба ПО потребляет системные ресурсы сервера (немного, но есть) и создаёт дополнительную нагрузку на систему.<br>**Практические рекомендации:**<br>Удаление со всех серверов ПО DameWare.<br>**Плюсы и минусы предложенных практических рекомендаций:**<br>+<br>Устранение существующих рисков.<br>-<br>Затраты времени. |
| 4 | **Проблема:**<br>На всех серверах в сети установлены Microsoft Firewall Client.<br>**Существующие риски:**<br>Проблемы в работе сетевого подключения сервера вызванного нестабильной работой фаервол клиента. Как следствие, недоступность сервера.<br>**Практические рекомендации:**<br>Удаление со всех серверов Microsoft Firewall Client.<br>**Плюсы и минусы предложенных практических рекомендаций:**<br>+<br>Устранение существующих рисков.<br>-<br>Затраты времени. |

## 2. Проблемы на серверах.

| п.№ | |
|---|---|
| **1.** | **Имя сервера: ……** |
| | **Роли сервера:**<br>1. Шлюз в интернет.<br>2. Пересылка почты (включая функцию антиспама) |
| | **Установленное программное обеспечение:**<br>1. ISA Server 2006 Standard Edition<br>2. ORF Enterprise Edition 4.3<br>3. Служба SMTP |
| | **Проблемы конфигурации:** |
| 1.1 | **Проблема:**<br>Политика ISA Server №6 разрешает весь трафик из любого источника в любое назначение для анонимных пользователей.<br>**Существующие риски:**<br>1. Несанкционированный доступ как внутри компании, так и извне.<br>2. Невозможность адекватной оценки работы ISA Server и устранения неполадок.<br>3. «Бесполезно» использованные средства на закупку мощного программного обеспечения.<br>**Практические рекомендации:**<br>Глубокий анализ политик доступа ISA Server исходя из принципа: «запретить всё, после чего разрешать только необходимое».<br>**Плюсы и минусы предложенных практических рекомендаций:**<br>+<br>1. Устранение возможностей для несанкционированного доступа.<br>2. Повышение стабильности работы сервера.<br>-<br>Затраты времени на анализ и настройку ISA Server. |
| 1.2 | **Проблема:**<br>На сервере работает SMTP служба, служащая для целей пересылки почты между интернетом и почтовым сервером. Также на сервере работает программное обеспечение ORF Enterprise Edition 4.3 служащая целям фильтрации спама<br>**Существующие риски:**<br>1. Дополнительная точка отказа в работе почтовой инфраструктуры. Отказ в работе данной службы приведёт к невозможности отправки почты на внешние почтовые сервера.<br>2. Возможность доступа к службе SMTP для несанкционированной рассылки почты (спама).<br>**Практические рекомендации:**<br>1. Удаление службы SMTP с сервера и настройка пересылки почты с сети Интернет напрямую с почтовым сервером используя встроенные возможности ISA Server.<br>2. Установка ORF Enterprise Edition 4.3 на почтовом сервере.<br>**Плюсы и минусы предложенных практических рекомендаций:**<br>+<br>1. Повышение отказоустойчивости за счёт устранения дополнительной точки отказа.<br>2. Устранение возможности для несанкционированной рассылки почты (спама).<br>-<br>Затраты времени на конфигурирование почтовой инфраструктуры, перенос настроек |

| | |
|---|---|
| | ПО ORF на почтовый сервер и тестирование. |
| 1.3 | **Проблема:**<br>Недостаточно очевидная политика работы VPN клиентов. Присутствует удалённый VPN сайт, VPN клиенты могут пользоваться интернетом и др.<br>**Существующие риски:**<br>1. Невозможность адекватной оценки работы ISA Server и устранения неполадок.<br>2. Возможный риск несанкционированного доступа.<br>**Практические рекомендации:**<br>Глубокий анализ политик работы VPN исходя из принципа: «запретить всё, после чего разрешать только необходимое».<br>**Плюсы и минусы предложенных практических рекомендаций:**<br>+<br>1. Устранение возможностей для несанкционированного доступа.<br>2. Повышение стабильности работы сервера.<br>-<br>Затраты времени на анализ и настройку ISA Server. |
| | |