УТВЕРЖДЕН
приказом директора

от "____"_____2014г. №____

Отчет по аудиту ИТ-инфраструктуры

Содержание

1 Назначение документа

1.1 Цели аудита

Проанализировать целесообразность использования текущего количества серверов и выдать рекомендации по оптимизации. Проанализировать текущую модель безопасности.

1.2 Объекты аудита

Серверная инфраструктура, Active Directory, Exchange, доступ в Интернет, подключение филиалов, сервера 1С, прием факсов, корпоративный портал на базе SharePoint 2007, серверное помещение, сетевая инфраструктура.

1.3 Проведенные интервью

Системный администратор Иванов Иван.

2 Описание объекта аудита

2.1 Общее описание ИТ инфраструктуры

Инфраструктура состоит из головного офиса и четырех филиалов.

Филиалы связаны с головным офисом VPN каналами.

12 серверов в головном офисе.

34 рабочих станций в головном офисе.

В филиалах количество рабочих станций не превышает 5.

2.2 Инфраструктура бизнес-приложений

2.2.1 Почтовый сервер MS Exchange (бизнес critical)

Почтовый сервер компании реализован на базе MS Exchange 2003.Клиенты на рабочих станциях сотрудников, MS Outlook 2007, настроены на использование протоколов POP3, SMTP. Доступ к почтовым ящиком “снаружи” через Outlook Web Access (OWA) или ActiveSync не реализован. Вся почта компании храниться на локальных рабочих станциях сотрудников. Backup почтовых сообщений (почтовых ящиков) на регулярной основе не реализован.

2.2.2 Внутренний портал MS SharePoint

Внутренний портал реализован на базе MS Office SharePoint Server 2007. В основе “движка” портала лежит веб сайт на PHP, расположенный на рабочей станции системного администратора. Сотрудниками компании портал используется крайне редко.

2.2.3 1С (бизнес critical)

1С представлена на трех серверах. Один экземпляр 1с (предназначенный для производства), версия 7.7, установлен на сервере выделенным под домен контроллер. Второй экземпляр 1с (предназначенный для бухгалтерии), версия 7.7, установлен на выделенный сервер. Третий экземпляр 1с (предназначенный для бухгалтерии), версия 8.0, установлен на выделенный сервер. Сопровождением 1с занимается специалист, привлекаемый со стороны. Он же выполняет backup всех баз 1с. BackUp баз храниться за пределами компании у специалиста 1С. Текущие системные администраторы в процедурах backup и отработки процедур восстановления участия не принимают.

2.2.4 Доступ в интернет (бизнес critical)

Доступ в интернет предоставляется без антивирусной защиты на уровне прокси сервера.

2.2.5 Прием факсов (бизнес critical)

Прием факсов реализован на базе ПО VentaFax установленном на сервере FAXSPL, в который подключено 4 телефонных линии (установлены 4 модема). На компьютерах сотрудников компании установлено клиентское ПО VentaFax с помощью которого сотрудники компании отыскивают "свой" факс среди всех входящих факсов.

2.3 Операционная инфраструктура

2.3.1 ActiveDirectory

ActiveDirectory реализована на базе Windows Server 2003. В головном офисе размещены 2 контроллера. В каждом филиале, до недавнего времени, размещалось по одному домен контроллеру, на котором по совместительству располагался VPN сервер (на базе MS ISA 2004). На момент аудита филиальные домен контроллеры были остановлены. Периодически домен контроллеры выводятся из эксплуатации из-за возникновения большого количества ошибок и как следствие отказа в обслуживание, вместо выводимого домен контроллера вводиться новый. Служба ActiveDirectory реализована в русской локализации.

2.3.2 ISA сервер

ISA 2004 сервер в головном офисе выступает как VPN сервер, Firewall и прокси-сервер для доступа в интернет сотрудников компании.

2.3.3 Антивирусная защита

На рабочих станция сотрудников компании установлено антивирусное ПО NOD 32. Входящие и исходящие почтовые сообщения на почтовом сервере централизованную проверку на антивирус не проходят .Интернет трафик при доступе в Интернет сотрудниками компании не походит антивирусную проверку.

2.3.4 Backup

Нет регулярных процедур BackUp, как данных, так и конфигураций серверов, BackUp выполняется произвольно. Нет процедур проверки достаточности и целостности BackUp, и как следствие навыков по восстановлению тех или иных данных или приложений.

2.3.5 Серверное помещение

Вход в серверное помещение свободный. Охлаждение недостаточное, на момент аудита в помещении было жарко.

3 Результаты аудита

3.1 Выявленные проблемы

3.1.1 Неоптимальность архитектурных решений

Архитектура ИТ среды выстроена без четкой концепции и понимания, как это должно быть. Важные компоненты ИТ среды (например, домен контроллеры) подвергаются частым и необоснованным изменениям которые несут в себе большие риски. Модель подключения филиалов и сотрудников филиалов к головному офису часто претерпевает изменения и также не имеет четкой концепции.

3.1.2 Неэффективность использования серверных ресурсов

Серверные ресурсы используются недостаточно оптимально. При текущих потребностях компании в используемых приложениях количество серверов можно сократить до 6-7.

3.1.3 Организационные и процедурные проблемы

Процедуры резервного копирования, как важных данных компании, так и компонентов ИТ инфраструктуры не производятся на регулярной основе (последний раз частичное резервное копирование делалось в апреле). Как следствие отсутствуют процедуры восстановления того или иного компонента ИТ среды или данных. Отсутствуют сформулированные и понятные политики безопасности, а также правила пользования приложениями для сотрудников компании (потребителей ИТ услуг).

3.2 Риски сопровождения ИТ инфраструктуры

3.2.1 Краткосрочные риски

Краткосрочные риски включают в себя выход из строя любого компонента ИТ среды, как на аппаратном, так и на уровне приложений, что влечет за собой перерыв в оказании важных для бизнеса услуг для сотрудников компании, т.е простой. Также нельзя исключать потерю важных для компании данных и невозможность их восстановления в принципе (восстанавливать просто неоткуда).

3.3 Предложения по результатам аудита

3.3.1 Проект по оптимизации ИТ инфраструктуры

Как вариант наша компания может разработать архитектуру ИТ среды компании с учетом текущих потребностей бизнеса и передать проект на реализацию силами специалистов ИТ отдела компании. В данном варианте успешность в реализации проекта в большей степени зависит от компетенции специалистов ИТ отдела компании.

3.3.2 Разовое мероприятие по нормализации серверной инфраструктуры

Возможно разовое мероприятие по нормализации и оптимизации ИТ среды компании, включая настройку приложений, исправления текущего состояния методом выявления ошибок приложений и их устранение, а также разработка правил и процедур для управления ИТ средой. И как конечный этап передача управления ИТ средой специалистам ИТ отдела компании. При этом варианте успешность мероприятия будет зависеть от компетенции специалистов ИТ отдела при сопровождении “выстроенной” ИТ среды и отсутствия необдуманных инициатив по изменению ИТ среды.

3.3.3 Передача на аутсорсинг критичных бизнес-приложений

Наиболее безопасный и "правильный" вариант, с учетом сложившейся ситуации, видится передача на аутсорсинг бизнес критичных приложений (корпоративная почта, 1С, ActiveDirectory, доступ в интернет). В данном варианте бизнес компании будет потреблять услуги на функциональном уровне, не вдумываясь, что за этим стоит и как это сделано, и может иметь возможность полностью сосредоточиться на самом бизнесе

