Долгое время у меня лежал черновик документа по ИТ аудиту информационной системы. Последнее время я немного занимался этой темой, поэтому решил его опубликовать и обсудить с вами. Аудит писался как план действий и одновременно предложение для организаций. Думаю, он многим будет полезен, а я рассчитываю его дополнить и подредактировать с вашей помощью.

Содержание:

Введение

Информационная система является важной и неотъемлемой частью организации. Качество ее работы может прямо или косвенно влиять на доходы и расходы компании. Своевременное обслуживание и аудит ИТ системы позволяет снижать издержки и увеличивать уровень надежности и безопасности.

Простым примером роста издержек может служить распространенная в последнее время ситуация с договором на телекоммуникационные услуги в долларах или у.е. При росте курса растут расходы. В таких случаях нужно своевременно среагировать на ситуацию и изменить условия договора или поменять поставщика услуг.

Ненадлежащее качество хранения резервных копий коммерческой информации может привести к прямым финансовым потерям в случае выхода из строя оборудования. Регулярная проверка доступности системы архивирования поможет избежать потерь в будущем.

Уволенный нелояльный сотрудник с административными правами может серьезно нарушить работу информационной системы, если ему своевременно не отключить доступ.

Медленная работа базы данных может увеличивать нагрузку на менеджеров, работающих с клиентами, что косвенно увеличивает расходы организации на содержание штата сотрудников.

Эти и многие другие моменты требуют постоянной качественной работы по обслуживанию информационной системы. Для проверки текущего состояния, я предлагаю провести ИТ аудит организации. Данная работа проводится по следующей схеме.

Инвентаризация объектов аудита

На данном этапе выбирается цель аудита. В зависимости от цели обозначается круг исследуемых объектов в информационной системе. Примером объектов могут служить:

- серверное и пользовательское оборудование;
- программное обеспечение;
- телефония;

- системы передачи данных и д.р.

Определение внешних точек доступа в информационную систему и их защищенность

Производится анализ всех возможных подключений из интернета для доступа к ресурсам локальной сети организации. Примером таких ресурсов может быть доступ:

- к почтовым ящикам пользователей;
- rdp доступ для управления компьютером или сервером;
- доступ к файлам на сетевых ресурсах и др.

Проверка всех типов используемой информации и способы ее архивирования

Анализируется вся информация организации, которая представляет ценность. Составляется ее каталог и схемы резервного копирования. Примером такой информации могут служить:

- письма в почтовых ящиках пользователей;
- базы данных CRM систем;
- личные файлы пользователей;
- информация на общих сетевых дисках и др.

Составляется схема архивирования информации, на которой будет отражена глубина и полнота архивов, возможность восстановления информации и сроки этого процесса.

Анализ производительности серверов и каналов связи

На основе реальной загрузки серверной инфраструктуры проверяется соответствие используемых ресурсов для выполнения поставленных задач. Ресурсы могут быть как излишними, что ведет к повышению затрат на поддержку, так и недостаточными, что приводит к снижению быстродействия работы информационной системы и удорожанию ее обслуживания.

Оценка надежности оборудования и времени восстановления в случае сбоя

Оценивается качество оборудования и его функциональные возможности по предотвращению или восстановлению в случае сбоя в работе. К таким качествам, к примеру, относится

- наличие рейд-контроллера и настроенного рейда для хранения информации;
- возможность горячей замены жестких дисков или блоков питания на серверах;
- подключение оборудования к источникам бесперебойного питания и др.

На основе этой информации и полученных ранее данных о схеме бэкапа оценивается примерное время восстановление работоспособности информационной системы в случае выхода из строя различных узлов.

Аудит учетных записей

Проверка всех учетных записей с обычным и административным доступом к ресурсам информационной системы. Это могут быть данные для получения административных прав на контроллере домена, сервере баз данных, для доступа к серверу видео наблюдения, системы контроля доступа в помещения, обычный доступ к общим сетевым дискам и д.р.

Анализ способов хранения и передачи учетных данных.

Проверка лицензионного ПО

Аудит установленного программного обеспечения в информационной системе. Проверка соответствия установленного ПО количеству приобретенных лицензий. Выявление нарушений в установке и использовании ПО. Оценка стоимости для легализации всего использующегося ПО.

Аудит телефонной связи

Анализ направлений звонков и их сопоставление с текущими тарифными планами. Рассмотрение подключения дополнительных линий для снижения затрат на звонки по определенным направлениям. Проверка возможности перевода телефонии на IP протокол для автономности от локального оператора связи.

Анализ системы мониторинга

Проверка работы существующей системы мониторинга информационной системы. На основе собранных ранее данных, выполняется оценка качества мониторинга с учетом выявленных критических узлов в системе и регламентному времени реагирования на события.

Проверка работы ИТ отдела

Анализируется имеющая документация ИТ отдела, такая как:

- инструкции по работе с пользователями и ресурсами сети;
- план действий на случай нештатных ситуаций или аварий;
- должностные инструкции сотрудников;
- регламенты обслуживания;
- схемы информационных систем и т.д.

Проверяется структура отдела и распределение ролей сотрудников.

Заключение

> Не понравилась статья и хочешь научить меня администрировать? Пожалуйста, я люблю учиться. Комментарии в твоем распоряжении. Расскажи, как сделать правильно!

Буду рад комментариям, замечания дополнениям. Текст составлен полностью мной, нигде и ни у кого не копировал, не подсматривал. Основывался только на своем опыте, поэтому мог что-то упустить или забыть. Я работаю только с малым и среднем бизнесом, поэтому материал актуален только для них.

Если кого-то заинтересовал подобный аудит, и вы хотите провести его у себя в компании, обращайтесь ко мне.

Онлайн курс "DevOps практики и инструменты"

Если у вас есть желание научиться строить и поддерживать высокодоступные и надежные системы, научиться непрерывной поставке ПО, мониторингу и логированию web приложений, рекомендую познакомиться с онлайн-курсом «DevOps практики и инструменты» в OTUS. Курс не для новичков, для поступления нужны базовые знания по сетям и установке Linux на виртуалку. Обучение длится 5 месяцев, после чего успешные выпускники курса смогут пройти собеседования у партнеров. Проверьте себя на вступительном тесте и смотрите программу детальнее по ссылке.

Помогла статья? Есть возможность отблагодарить автора