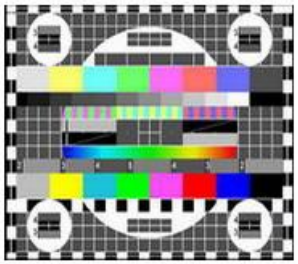
В,  ’  Ц Я

’’ 



”Х

+ Н + С ОЕ

”

СЖЛЦ

1 = В Е

Комплекс организационно-технических мероприятий

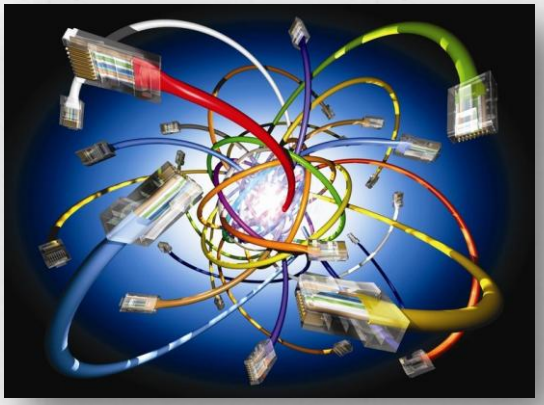
- **Техническое обслуживание (ТО)** - это комплекс организационно-технических мероприятий и работ, производимых на объекте и направленных на поддержание в рабочем или исправном состоянии оборудования (программного обеспечения (ПО)) технических систем в процессе их использования по назначению с целью повышения надежности и эффективности их работы.

Основные задачи технического обслуживания систем

- определение качественного состояния оборудования, кабельных сетей и проверка их работоспособности (в том числе ПО);
- своевременное выявление и устранение недостатков, снижающих эффективность работы систем и приводящих к возникновению отказов аппаратуры (ПО);
- предупреждение отказов оборудования (ПО), увеличение межремонтных сроков эксплуатации и сроков службы оборудования;

- проверка и доведение до установленных норм параметров оборудования систем, линейно-кабельных и распределительных устройств;
- подготовка оборудования к сезонной эксплуатации;
- анализ и обобщение сведений результатов выполненных работ, разработка мероприятий по совершенствованию форм и методов Технического обслуживания, эксплуатации систем;
- техническая консультативная поддержка эксплуатирующего персонала и руководителей по любым вопросам, связанным с эксплуатацией систем в целях эффективного использования.

Порядок планирования и проведения мониторинга компьютерных сетей и порядок организации работ по техническому сопровождению корпоративной компьютерной сети



Мониторинг аппаратного обеспечения

- Мониторинг работоспособности аппаратных компонентов КС осуществляется в процессе их обслуживания и при проведении работ по техническому обслуживанию оборудования.

Мониторинг парольной защиты

- Мониторинг парольной защиты и контроль надежности пользовательских паролей предусматривают:
  - установление сроков действия паролей;
  - периодическую (не реже 1 раза в месяц) проверку пользовательских паролей.

Мониторинг попыток несанкционированного доступа

Предупреждение и своевременное выявление попыток несанкционированного доступа осуществляется с использованием средств операционной системы, специальных программных средств и предусматривает:

- фиксацию неудачных попыток входа в систему в системном журнале;
- протоколирование работы сетевых сервисов;
- выявление фактов сканирования определенного диапазона сетевых портов в короткие промежутки времени с целью обнаружения сетевых анализаторов, изучающих систему и выявляющих ее уязвимости.

Мониторинг производительности

Мониторинг производительности КС производится по обращениям пользователей в ходе обслуживания систем и при проведении профилактических работ.

Системный аудит

- Системный аудит производится администратором информационной безопасности ежеквартально и в особых ситуациях. Он включает проведение обзоров безопасности с занесением записей в Журнал обзоров безопасности, тестирование системы, контроль внесения изменений в системное программное обеспечение.

Антивирусный контроль

Для защиты объектов вычислительной техники необходимо использовать антивирусные программы:

- резидентные антивирусные мониторы, контролирующие подозрительные действия программ;
- утилиты для обнаружения и анализа новых вирусов.
- Запуск антивирусных программ должен осуществляться автоматически по заданию, централизованно созданному с использованием планировщика задач (входящим в поставку операционной системы либо поставляемым вместе с антивирусными программами).

Анализ попыток взлома инцидентов

Если администратор информационной безопасности подозревает или получил сообщение о том, что система подвергается атаке или уже была скомпрометирована, то он должен установить:

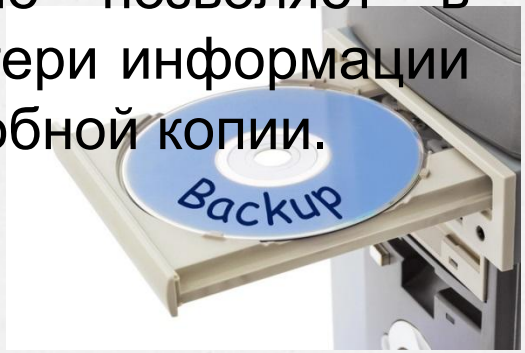
- факт попытки несанкционированного доступа (далее - НСД);
- продолжается ли НСД в настоящий момент;
- кто является источником НСД;
- что является объектом НСД;
- когда происходила попытка НСД;

- как и при каких обстоятельствах была предпринята попытка НСД;
- точка входа нарушителя в систему;
- была ли попытка НСД успешной;
- определить системные ресурсы, безопасность которых была нарушена;
- какова мотивация попытки НСД.

Порядок проведения резервного копирования

Для предотвращения потери данных из-за сбоев оборудования, уничтожения оборудования, программных ошибок, неправильных действий персонала и других возможных причин утери информации предусмотрена система регулярного резервного копирования данных.

Такое резервное копирование позволяет в случае возникновения ошибки и потери информации вернуться к ближайшей работоспособной копии.



Указания по проведению профилактических работ

- Профилактические работы проводятся строго в соответствии с установленным графиком. График проведения профилактических работ на серверах на следующий месяц составляется администратором.
- Администратор ЛС обязан включить в график все периодические профилактические работы, независимо от необходимости их проведения.
- Профилактика целостности операционной системы, сетевого взаимодействия, проверка работы сервисов и служб проводятся в рабочем порядке, поскольку в подавляющем большинстве случаев не требуют перезагрузки серверов.

- Профилактика баз данных, проверки на наличие вирусов, обновлений системы и серверных приложений, проверка отказоустойчивости системы, профилактика работоспособности дисковой и файловой подсистем, остановки сервера для чистки и вентиляции проводятся в рабочее время с учетом времени минимальной загрузки серверов.
- Профилактические работы на серверах, требующие длительного (более 1 часа) отключения и способные повлиять на рабочие процессы в организации, проводятся в выходные дни.

Процедуры, необходимые для проведения профилактических работ

- анализ журналов событий серверов: проводится ежедневно для выявления ошибок, связанных с функционированием базовых компонентов серверного аппаратно-программного комплекса;
- анализ отчетов системы безопасности: проводится ежедневно с целью выявления соответствия политик доступа к ресурсам локальной сети путем просмотра журналов системы безопасности серверов и программ, отвечающих за безопасность информационных потоков с оценкой соответствия доступа пользователей к ресурсам организации;

- проверка работоспособности почтовых служб и служб Интернет: проводится ежедневно с целью поддержания возможности получения пользователями оперативной информации из внешних источников;
- анализ возможностей доступа пользователей к сетевым ресурсам: проводится ежедневно с целью определения возможности совместного доступа к различным сетевым ресурсам и выполнения пользователями их должностных обязанностей;

- просмотр отчетов служебных программ: проводится с целью проверки работоспособности пользовательских приложений, установленных на сервере;
- проверка сетевого взаимодействия: производится еженедельно в начале рабочей недели и включает в себя краткий анализ журналов событий и графиков загрузки сети;
- анализ Интернет-трафика: проводится ежедневно с целью предотвращения нецелевого использования Интернет-ресурсов;

- проверка работы служб: проводится еженедельно на каждом из работающих серверов, находящихся в ЛС;

- проверка наличия обновлений операционной системы и серверных приложений: проводится еженедельно с целью поддержания работоспособности аппаратно-программного комплекса на должном уровне и сохранения безопасности использования внешних источников информации;

Перечень профилактических работ

- анализ журналов событий серверов (ежедневно);
- анализ отчетов системы безопасности (ежедневно);
- анализ изменения состава групп безопасности в AD (Active Directory);
- выявление попыток несанкционированного доступа к ресурсам;
- выявление попыток несанкционированного изменения уровня доступа к ресурсам;

- проверку работоспособности почтовых служб и служб Интернет (ежедневно);
- анализ Интернет-трафика (ежедневно);
- анализ возможностей доступа пользователей к сетевым ресурсам (ежедневно);
- просмотр отчетов служебных программ (ежедневно);
- проверку сетевого взаимодействия (1 раз в неделю);
- проверку работы сервисов и служб (1 раз в неделю);
- проверку наличия обновлений операционной системы и серверных приложений (1 раз в неделю);

- профилактику баз данных (1 раз в неделю);
- антивирусную профилактику сервера (1 раз в неделю);
- проверку целостности операционной системы (1 раз в 2 недели);
- принудительную проверку отказоустойчивости системы (1 раз в 2 недели);
- профилактику дисковой и файловой подсистем на сервере (1 раз в 2 недели);

- профилактическую остановку сервера (1 раз в 2 недели);
- составление отчета доступа к Интернет-ресурсам (1 раз в месяц);
- профилактические работы на объектах вычислительной техники (выполняются пользователем, по необходимости при помощи сотрудников ООВТ ЦСИТ).

Профилактические работы на объектах вычислительной техники

- проверка обновления клиентских приложений (по необходимости);
- проверка времени последнего обновления антивирусных баз (1 раз в неделю);
- выявление попыток несанкционированной установки приложений пользователем (ежедневно);

- удаление временных и устаревших копий файлов (по необходимости);
- выполнение прочих работ, непосредственно связанных с работоспособностью объектов вычислительной техники (по необходимости).