Лекция 15. Основные задачи администрирования операционных систем. Системный администратор. Типовые задачи системного администрирования. Политика информационной безопасности организации.

Административные меры защиты

Организация эффективной и надежной защиты операционной системы невозможна с помощью одних только программно-аппаратных средств. Эти средства обязательно должны, дополняться административными мерами защиты. Без постоянной квалифицированной поддержки со стороны администратора даже самая надежная программно-аппаратная защита оборачивается фикцией.

Основные административные меры защиты.

1. *Постоянный контроль корректности функционирования операционной системы*, особенно ее подсистемы защиты. Такой контроль наиболее удобно организовать, если операционная система поддерживает регистрацию событий. В этом случае операционная система автоматически регистрирует в специальном журнале наиболее важные события, произошедшие в процессе функционирования системы.

2. *Организация и поддержание адекватной политики безопасности.*

Политика безопасности должна постоянно корректироваться, оперативно реагируя на изменения в конфигурации операционной системы, установку, удаление и изменение конфигурации прикладных программных продуктов и расширений операционной системы, попытки злоумышленников преодолеть защиту операционной системы и т.д.

3. *Инструктирование пользователей* операционной системы о необходимости соблюдения мер безопасности при работе с операционной системой и контроль за соблюдением этих мер.

4. *Регулярное создание и обновление резервных копий программ* и данных операционной системы. Постоянный контроль изменений в конфигурационных данных и политике безопасности операционной системы.

Основные принципы администрирования ОС.

- Непрерывность;
- Комплексность;
- Актуальность;
- Адекватность;
- Непротиворечивость. (разграничение доступа, настроек процессов);
- Формальный подход. Применение методик (инструкций, положений, приказов, РД и прочих рекомендательных документов) и четких концептуальных принципов при постановке задач администрирования и их реализации;
- Подконтрольность.

Задачи и принципы управления безопасностью.

Отдельные средства ИБ не обеспечивают эффективного функционирования и требуют объединения в единую и централизованно управляемую и постоянно действующую *систему информационной безопасности* Система ИБ обычно должна решать следующие задачи:

- ввод в систему списка имен пользователей и терминалов, допущенных к информации ИС;
- подготовку и ввод в систему, запись паролей пользователей на носители;
- ввод в систему назначенных полномочий пользователей и терминалов;
- раздачу пользователям носителей с паролями и значений паролей, запоминаемых и вводимых пользователями вручную с клавиатуры;
- сбор сигналов несовпадения паролей и нарушения полномочий пользователей;
- установление времени, места и причины НСД;
- анализ ситуации, принятие адекватных мер и восстановление нормального функционирования ИС
- контроль конфигурации системы;
- сбор сигналов вскрытия аппаратуры и контроль ввода (вывода) аппаратуры в (из) ремонт (а) и на (из) профилактику(и);
- контроль журнала регистрации доступа к информации ИС и периодический вызов справок из него;
- взаимодействие со службой функционального контроля ИС;
- контроль функционирования системы защиты;
- подготовку ключей, контроль и обеспечение функционирования средств шифрования информации;
- контроль стирания и уничтожения остатков секретной информации на машинных и бумажных носителях;
- регистрацию, учет и разграничение доступа к носителям информации и ПО;
- ведение статистики и прогнозирование НСД.

Системный администратор — сотрудник, должностные обязанности которого подразумевают обеспечение штатной работы парка компьютерной техники, сети, программного обеспечения. Зачастую системному администратору вменяется обеспечение информационной безопасности в организации. Разговорное название — **сисадмин**.

Системные администраторы — сотрудники, в обязанности которых входит создание оптимальной работоспособности компьютеров и программного обеспечения для пользователей, часто связанных между собой общей работой на определенный результат.

Нередко функции системного администратора перекладывают на компании, занимающиеся IT-аутсорсингом. Обычно такие компании предоставляют более низкую, чем содержание штатного сотрудника, стоимость обслуживания и осуществляют работу на основе абонементных договоров.
Ввиду быстрого роста Интернета и развития сетевых технологий, системному администратору становится всё сложнее противостоять всем проблемам, поэтому давно появились специализированные форумы и печатные издания, направленные на расширение кругозора начинающих системных администраторов и оказание помощи в решении различных IT-проблем. Косвенно это связано с наличием свободного времени у опытных системных администраторов ввиду их более высокого профессионального уровня.

Обязанности

В круг типовых задач системного администратора обычно входит:

- подготовка и сохранение резервных копий данных, их периодическая проверка и уничтожение;
- установка и конфигурирование необходимых обновлений для операционной системы и используемых программ;
- установка и конфигурирование нового аппаратного и программного обеспечения;
- создание и поддержание в актуальном состоянии пользовательских учётных записей;
- ответственность за информационную безопасность в компании;
- устранение неполадок в системе;
- планирование и проведение работ по расширению сетевой структуры предприятия;
- документирование всех произведенных действий.

В организациях с большим штатом сотрудников данные обязанности могут делиться между несколькими системными администраторами — например, между администраторами безопасности, учётных записей и резервного копирования. Также, в организациях с небольшим штатом сотрудников эти обязанности могут исполняться одним специалистом, занимающимся как консультированием пользователей, так и ремонтом аппаратной части персональных компьютеров и периферийных устройств.

Специализация

Системных администраторов можно разделить на несколько категорий:

- *Администратор веб-сервера* — занимается установкой, настройкой и обслуживанием программного обеспечения веб-серверов. Как правило, работает в хостинговой компании. Необходимы знания Unix-систем, умение конфигурировать веб-сервер Apache и почтовые сервера, которые установлены на более чем 90 % web-серверов во всем мире; дополнительно веб-сервер IIS и ОС семейства Windows Server. Обязательно глубокое понимание модели OSI, стека протоколов TCP/IP.
- *Администратор баз данных* — специализируется на обслуживании баз данных. Нужны глубокие знания СУБД , операционной системы, на которой работает база данных, знание особенностей реализации баз данных, а также знание информационно-логического языка SQL.
- *Администратор сети* — занимается разработкой и обслуживанием сетей. Необходимы глубокие познания в области сетевых протоколов и их реализации, маршрутизации, реализации VPN, системах биллинга, активного сетевого оборудования, физическом построении сетей.

•*Системный инженер* (или системный архитектор) — занимается построением корпоративной информационной инфраструктуры на уровне приложений.
Нужны знания распространённых ОС; службы каталогов; распространённые СУБД, , системы документооборота — связью которых в контексте бизнес-процессов и занимается.

•*Администратор безопасности сети* — занимается, соответственно, проблемами информационной безопасности, документированием политик безопасности, регламентов и положений об информационных ресурсах.
Требуются знания протоколов шифрования и аутентификации и их практическом применении.

•*Системный администратор малой компании* (от 5 до 50 рабочих мест) — занимается поддержанием работоспособности небольшого парка компьютерной техники и обслуживанием сети. Не имеет помощников и выполняет все обязанности, связанные с компьютерами и коммуникациями, в том числе техническую поддержку пользователей. В компаниях, занимающихся разработкой программного обеспечения, обслуживает Web-сервера, программы, используемые разработчиками. Также может тестировать разрабатываемое компанией программное обеспечение.
Требуется знание ОС от Microsoft, офисных и бухгалтерских программ , умение прокладывать локальную сеть, начальные знания баз данных и языков программирования.

•*Администратор почтовых серверов* — занимается настройкой и поддержкой электронной почты.
Требуется знание Windows Server или же Linux в зависимости от требования программы почтового сервера, дополнительные модули для проверки на вирусы, спам, или для интеграции с базами данных.
Требуется знание протоколов и технологий , стека протоколов TCP/IP и основных программ-клиентов электронной почты .

О политике информационной безопасности

Политика информационной безопасности – это высокоуровневый документ, который включает в себя принципы и правила, определяющие и ограничивающие определенные виды деятельности объектов и участников системы информационной безопасности, направленные на защиту информационных ресурсов организации.

Как известно, стратегическое планирование позволяет определить основные направления деятельности организации, связав воедино маркетинг, производство и финансы. Долгосрочный стратегический план позволяет компании выстроить все свои бизнес-процессы с учетом микро и макросреды для достижения наилучших финансовых показателей и темпов экономического роста. Важной составляющей в стратегическом планировании является учет требований политики информационной безопасности, которые должны быть краеугольным камнем при определении среднесрочных и долгосрочных целей и задач организации. С ростом компании и пересмотром планов политика также должна пересматриваться. Низкоуровневые документы информационной безопасности необходимо пересматривать в соответствии с реализацией краткосрочных планов.

Политика информационной безопасности неразрывно связана с развитием компании, ее стратегическим планированием, она определяет общие принципы и порядок обеспечения информационной безопасности на предприятии. Политика информационной безопасности тесно интегрируется в работу предприятия на всем этапе его существования. Все решения, предпринимаемые на предприятии, должны учитывать её требования.

Эффективное обеспечение требуемого уровня информационной безопасности организации возможно только при наличии формализованного и системного подхода к выполнению мер по защите информации. Целью разработки политики информационной безопасности организации является создание единой системы взглядов и понимания целей, задач и принципов обеспечения информационной безопасности.

Основные этапы разработки политики информационной безопасности следующие:

- Исследование текущего состояния информационной среды и информационной безопасности организации;
- Анализ полученных сведений по результатам исследования;
- Формирование плана работ по разработке политики информационной безопасности;
- Разработка политика информационной безопасности организации.

Пакет организационно-распорядительных документов по вопросам обеспечения информационной безопасности включает следующие типы документов:

- Политика информационной безопасности организации - высокоуровневый документ, описывающий основные принципы и правила, направленные на защиту информационных ресурсов организации;
- Регламенты информационной безопасности, раскрывающие более подробно процедуры и методы обеспечения информационной безопасности в соответствии с основными принципами и правилами, описанными в политике;
- Инструкции по обеспечению информационной безопасности для должностных лиц организации с учетом требований политики и регламентов;
- Прочие документы, представляющие собой отчеты, регистрационные журналы и прочие низкоуровневые руководящие документы.

Конкретные проекты необходимых документов каждого типа определяются в ходе обследования существующего уровня информационной безопасности Заказчика, её организационной структуры и основных бизнес процессов.