С. А. КЛЕЙМЕНОВ, В. П. МЕЛЬНИКОВ, А. М. ПЕТРАКОВ

АДМИНИСТРИРОВАНИЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Под редакцией В. П. МЕЛЬНИКОВА

Допущено
Учебно-методическим объединением
по университетскому политехническому образованию
в качестве учебного пособия для студентов высших учебных заведений,
обучающихся по специальности «Информационные системы и технологии»

ACADEMIA

Москва
Издательский центр «Академия»
2008

УДК 681.518(075.8)
ББК 32.965я73
К48

Рецензенты:
д-р техн. наук, проф. кафедры «Транспортные установки»,
академик Российской Академии космонавтики им. К. Э. Циолковского
В. И. Великоиваненко;
проф. кафедры информационных систем и компьютерных технологий,
декан ФПКП Балтийского государственного технического университета
«Военмех» им. Д. Ф. Устинова, ученый секретарь Объединенного
учебно-методического совета по направлению
230201 «Информационные системы» *В. В. Касаткин*

Клейменов С. А.

К48 Администрирование в информационных системах : учеб. пособие для студ. высш. учеб. заведений / С. А. Клейменов, В. П. Мельников, А. М. Петраков ; под ред. В. П. Мельникова. — М. : Издательский центр «Академия», 2008. — 272 с.
ISBN 978-5-7695-4708-9

Рассмотрены основные положения и особенности информационных систем; задачи, функции, службы, процедуры и методология администрирования систем; управление конфигурацией и архитектурой, техническим информационным и программным обеспечением операционных систем Windows, Unix, Linux с позиций администрирования информационных потоков; инсталляции сетевого обеспечения на базе сетевых служб и сетевых команд; технологии управления ими, а также пользователями и дисками при администрировании. Большое внимание уделено обеспечению информационной безопасности в системах и их сетях: методологии обеспечения безопасности процессов переработки информации в информационной системе, технологиям безопасной работы администратора сети.

Для студентов высших учебных заведений.

УДК 681.518(075.8)
ББК 32.965я73

ISBN 978-5-7695-4708-9

ВВЕДЕНИЕ

В рамках федеральной целевой программы «Электронная Россия» внедрения концепции электронного правительства большое внимание должно быть уделено подготовке сертифицированных специалистов в области администрирования управления на базе информационных систем (ИС). Наиболее распространенными ИС в настоящее время являются сетевые системы MS DOS, Windows и Unix, причем администраторами сетей в наибольшей мере становятся экономисты, менеджеры, использующие эти сети в интересах работы в конкретной предметной области.

Существующие в настоящее время учебники и учебные пособия содержат в основном материалы программного сетевого обеспечения: обеспечение бесперебойной работы узлов, управление пользователями, серверами, сетевыми службами управления общего пользования, конфигурацией, регистрации, сбора и обработки информации, печати, планирования и развития, оперативное управление и регламентные работы в ИС и ряд других программно-технических функций. Как правило, в каждой из них представлен ограниченный набор инструкций пользователю-администратору без методологической формализации построения и структурирования по функциональному и объектовому применению. В этих изданиях мало внимания уделено методологии информационного обеспечения службы администрирования по функциональным и объектовым признакам, классификациям и примерам ИС администрирования, аппаратно-программных платформ эксплуатации и сопровождения функционирования ИС.

В ряде учебных изданий по ИС управления государственного, муниципального, предприятиями и организациями рассматриваются общеметодологические вопросы построения, функционирования и информационно-программного обеспечения управления на базе системного подхода при обработке информации. В некоторых изданиях отражены процессы администрирования при применении ИС управления, большей частью в локальных сетях.

Данное учебное пособие значительно отличается от изданных ранее. В нем изложено методологически обоснованное построение материала по информационному, организационному и программному обеспечению служб администрирования, эксплуатации, сопровождения и инсталляции ИС различного назначения

по управлению. В нем также рассмотрены информационные технологии администрирования; дана оценка различных сетевых операционных систем по областям применения, возможностям и эффективности; описаны классификационные признаки ИС администрирования и приведены примеры систем; рассмотрены методология организации баз данных администрирования, аппаратно-программных платформ, оперативного управления, обслуживания и регламентных работ программно-технических средств. Значительное внимание уделено формированию и функционированию служб управления конфигурацией, ошибочными ситуациями, общего пользования, регистрацией, сбором и обработкой информации, планирования и развития, эксплуатации и сопровождения ИС, контролем их характеристик. Рассмотрены также вопросы обеспечения информационной безопасности (ИБ) функционирования ИС администрирования. Здесь особо выделяются права, функции, обязанности и технологии принятия управленческих решений администратора сети в вопросах предотвращения, парирования и нейтрализации угроз функционирования ИС.

Учебное пособие состоит из семи глав. В каждой главе рассмотрен определенный круг вопросов по изучению приемов и методов администрирования ИС как в локальных представлениях сетей, так и в распределенных корпоративных конфигурациях. Все темы размещены в логической последовательности ознакомления учащихся как с проблемами административного управления ИС, так и с их современными решениями на базе информационных технологий.

В гл. 1 рассмотрены информационное обеспечение управления в ИС, особенности протекания информационных процессов и технологий принятия управленческих решений для эффективного функционирования ИС управления; сформулированы цели, задачи и функции администрирования для различных объектов; представлены требования к программному обеспечению различных уровней административного управления.

В гл. 2 представлены материалы по построению службы общего администрирования и описанию ее функционального назначения. Основное внимание уделено построению и архитектуре различных операционных систем (Windows NT, 2000, NET Server и Unix). Описаны их особенности и возможности в системном управлении при реализации процесса администрирования ИС и ее сети.

В гл. 3 рассмотрены структуры и особенности внемашинного и внутримашинного информационного и программного обеспечения управленческих функций, приведены системы показателей, классификации и кодирования, организации документооборота на базе унификации документации, варианты организации внутримашинного информационного обеспечения, банки данных, их состав, модели баз данных и знаний, информационное обеспечение технологий деятельности администратора и менеджера.

В гл. 4 описана методология обеспечения ИБ переработки управленческой и иной информации в защищенных и не защищенных ИС различного вида. Раскрывается основной набор методов и программно-аппаратных средств предотвращения, парирования и нейтрализации угроз функционированию ИС при администрировании.

В гл. 5 представлено техническое, программное и функциональное конфигурирование ИС и сетей; описана методология управления сетевыми ресурсами организационно-технического и программного характера на основе административных сетевых команд и технического расширения компьютерной сети.

В гл. 6 приведено описание различных сетевых служб (DNS, DHCP, WINS, RRAS и др.), технологий пользования ими, управления IP-адресами, маршрутизацией и удаленным доступом, а также мониторинга сети по производительности и диспетчеризации задач в различных технологических операциях ее работы: с утилитой Performance Monitor, Network Monitor, при просмотре журналов событий и др.

В гл. 7 описаны технологии управления различными службами на примере использования операционной системы Windows по процедурам управления пользовательскими учетными записями, пользователей и групп доменов по различным модификациям Windows, управление технологиями защиты Windows и ее ревизии и т.д. Рассмотрены также технологии управления сетевыми службами в сетях, например Windows NT, службами и приложениями в сетях Windows 2000, администрирования и управления дисками в них.

СПИСОК СОКРАЩЕНИЙ

АИС — автоматизированная информационная система
АИТ — автоматизированная информационная технология
АРМ — автоматизированное рабочее место
АУ — аппарат управления
БД — база данных
ВИН — ведомственные информационные накопители
ГА — Генеральная Ассамблея (ООН)
ГВС — государственная вычислительная система
ГИП — государственная информационная политика
ДДС — движение денежных средств
ЕС — Европейский Союз
ИБ — информационная безопасность
ИБП — источник бесперебойного питания
ИИ — информационное изделие
ИП — информационный продукт
ИР — информационные ресурсы
ИС — информационная система
ИСУ — интегрированная система управления
ИТ — информационные технологии
ИУС — информационная управляющая система
КБ — конструкторское бюро
КИС — корпоративная информационная система
КИСиТ — корпоративная информационная система и технологии
ЛВС — локальная вычислительная сеть
МСЭ — Международный совет электросвязи
НИН — независимый информационный накопитель
НСД — несанкционированный доступ
ОБСЕ — Организация по безопасности и сотрудничеству в Европе
ОД — обработка данных
ОЗУ — оперативное запоминающее устройство
ООН — Организация Объединенных Наций
ОС — операционная система
ОУ — объект управления
ПК — персональный компьютер
ПО — программное обеспечение
ПЭВМ — персональная электронно-вычислительная машина
СМИ — средства массовой информации
СУ — система управления
СУБД — система управления базами данных

СЭИСУ — социально-экономическая информационная система управления
СЭО — социально-экономический объект
ТИИ — точечные источники информации
УОТ — управление основной тематикой
ЦП — центральный процессор
ЭВМ — электронно-вычислительная машина

Глава 1

ИНФОРМАЦИОННЫЕ ПРОЦЕССЫ В СИСТЕМАХ УПРАВЛЕНИЯ. ЦЕЛИ, ЗАДАЧИ И ФУНКЦИИ АДМИНИСТРИРОВАНИЯ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

1.1. Информационные системы управления

1.1.1. Классификационные признаки и особенности построения и функционирования информационных СУ

Так как имеются различные интересы, особенности и уровни управления организациями, то существуют и различные виды информационных систем управления (СУ). Никакая единственная система не может полностью обеспечивать потребности организации во всей информации. Информационные СУ можно подразделить по уровням управления (стратегический, управленческий, «знания» и эксплуатационный), а также на функциональные области типа продажи и маркетинга, производства, финансов, бухгалтерского учета и человеческих ресурсов. Системы создаются, чтобы обслужить различные организационные интересы. Различные организационные уровни управления обслуживают четыре главных типа информационных СУ: системы уровня знания, системы с эксплуатационным уровнем, системы уровня управления и системы со стратегическим уровнем. Основными пользователями этих систем являются группы служащих, определяющих управленческие функции.

Типы информационных СУ и группы служащих — пользователей ими приведены в табл. 1.1. Можно считать, что все они создают свои особенности в администрировании этих информационных СУ и группы служащих — пользователей ими.

Системы стратегического уровня — это инструмент помощи руководителям высшего уровня, которые подготавливают стратегические исследования и длительные тренды в фирме и деловом окружении. Их основное назначение — приводить в соответствие изменения в условиях эксплуатации с существующей организационной возможностью.

Системы управленческого уровня разработаны для обслуживания контроля, управления, принятия решений и административных действий средних менеджеров. Они определяют, хорошо ли работают объекты, и периодически извещают об этом. Например,

Таблица 1.1

Типы информационных СУ и группы служащих — пользователей ими

№ п/п	Типы информационных СУ	Группы служащих — пользователей ими
1	Стратегический уровень	Высшее руководство
2	Управленческий уровень	Средние менеджеры
3	Уровень «знания»	Работники знания и данных
4	Эксплуатационный уровень	Управляющие операциями

система управления перемещениями сообщает о перемещении общего количества товара, равномерности работы торгового отдела и отдела, финансирующего затраты для служащих во всех разделах компании, отмечая, где фактические издержки превышают бюджеты.

Некоторые системы уровня управления поддерживают необычное принятие решений. Они имеют тенденцию сосредотачиваться на менее структурных решениях, для которых информационные требования не всегда ясны.

Системы уровня «знания» поддерживают работников знания и обработчиков данных в организации. Цель системы уровня «знания» заключается в том, чтобы помочь интегрировать новое знание в бизнес и помогать организации управлять потоком документов. Системы уровня «знания», особенно в форме рабочих станций и офисных систем, в настоящее время являются наиболее быстрорастущими приложениями в бизнесе.

Системы эксплуатационного уровня поддерживают управляющих операциями, следят за элементарными действиями организации типа продажи, платежей, обналичивают депозиты, платежную ведомость. Основная цель системы эксплуатационного уровня заключается в том, чтобы отвечать на обычные вопросы и проводить потоки транзакций через организацию. Чтобы отвечать на эти вопросы, информация вообще должна быть легко доступна, оперативна и точна.

Информационные системы управления также классифицируются по функциональным признакам. Главные организационные функции типа продажи и маркетинга, производства, финансов, бухгалтерского учета и человеческих ресурсов обслуживаются собственными СУ, а в больших организациях подфункции каждой из этих главных функций также имеют собственные системы. Например, функция производства могла бы иметь системы для управления запасами, управления процессом, обслуживания завода, автоматизированной разработки и материального планирования требований.

Таблица 1.2

Основные типы ИС, разделенные по уровням управления

Типы систем	Назначение				
Системы стратегического уровня					
Исполнительные системы (ESS)	Пятилетний прогноз продаж	Пятилетнее оперативное планирование	Пятилетний прогноз бюджета	Планирование прибыли	Планирование личного состава
Системы управленческого уровня					
Управляющие информационные системы (MIS)	Управление сбытом	Контроль инвентаря	Ежегодный бюджет	Анализ капиталовложения	Анализ перемещений
Системы поддержки принятия решений (DSS)	Коммерческий анализ региона	Планирование производства	Анализ затрат	Анализ рентабельности	Анализ стоимостей контрактов
Системы уровня «знания»					
Системы работы (KWS)	АРМ проектирования	Графические рабочие станции	Управленческие рабочие станции		
Системы автоматизации делопроизводства (OAS)	Текстовые редакторы	Создание изображений	Электронные календари		

Системы эксплуатационного уровня					
Системы диалоговой обработки запросов (TPS)	—	Машинная обработка	Торговля ценными бумагами	Платежные ведомости	Вознаграждения
	Отслеживание приказов	Планирование деятельности предприятий	—	Платежи	Обучение и развитие
	Отслеживание процессов	Перемещение материалов	Регулирование денежных операций	Дебиторская задолженность	Хранение отчетов служащих
	Продажа и маркетинг	Производство	Финансы	Бухгалтерия	Людские ресурсы

Примечание: ESS — Executive Support Systems; MIS — Management Information Systems; DSS — Decision Support Systems; KWS — Knowledge Work Systems; OAS — Office Automation Systems; TPS — Transaction Processing Systems.

Таблица 1.3

Характеристики информационных процессов систем управления

Типы систем	Информационные вводы	Обработка	Информационные выводы	Пользователи
ESS	Совокупные данные: внешние, внутренние	Графика; моделирование; интерактивность	Проекции; реакции на запросы	Старшие менеджеры; администраторы сетей
MIS	Итоговые операционные данные; данные большого объема; простые модели	Обычные доклады; простые модели; простейший анализ	Резюме и возражения	Средние менеджеры; администраторы сетей
DSS	Слабоформализованные данные; аналитические данные	Моделирование; анализ; интерактивность	Специальные доклады; анализ решений; реакция на запросы	Профессионалы; управляющие персоналом
KWS	Технические данные проекта; база знаний	Моделирование; проигрывание	Модели; графика	Профессионалы; технический персонал
OAS	Документы; расписания	Документы управления; планирование; связь	Документы; графики; почта	Служащие; администраторы сетей
TPS	Транзакции; результаты	Сортировка; список; слияние; модифицирование	Детальные доклады; списки; резюме	Оперативный персонал; управляющие

Типичная организация имеет системы различных уровней: эксплуатационную, управленческую, «знания» и стратегическую для каждой функциональной области. Например, коммерческая функция имеет коммерческую систему на эксплуатационном уровне, чтобы делать запись ежедневных коммерческих данных и обрабатывать заказы. Система уровня «знания» создает соответствующую информацию для демонстрации изделий фирмы. Системы уровня управления отслеживают ежемесячные коммерческие данные всех коммерческих операций и докладывают об операциях, где продажа превышает ожидаемый уровень или опускается ниже ожидаемого уровня. Система прогноза предсказывает коммерческие тренды в течение пятилетнего периода — обслуживает стратегический уровень.

Рассмотрим определенные категории систем, обслуживающих каждый организационный уровень. В табл. 1.2 представлены типы ИС, соответствующие каждому организационному уровню.

Характеристики процессов ИС из табл. 1.2 приведены в табл. 1.3.

Каждая система может иметь компоненты, которые используются разными организационными уровнями или одновременно несколькими. При этом секретарь директора может находить информацию об MIS, средний менеджер может нуждаться в данных анализа из TPS.

Уровни принятия решений можно подразделить на неструктурированные и структурированные. *Неструктурированные* — решения, в которых принимающий решение должен обеспечить суждение, оценку и проникновение в прикладную область. Каждое из этих решений оригинально, важно, не имеет аналогов или разработанной методики для их принятия. *Структурированные* решения, наоборот, являются повторяемыми и обычными и имеют определенную процедуру для их принятия, чтобы они не рассматривались каждый раз как новые. Некоторые решения слабоструктурированы — в таких случаях только часть проблемы имеет четкий ответ, обеспеченный в соответствии с принятой процедурой.

1.1.2. Модели функционирования систем управления

Для эффективного администрирования в информационных СУ целесообразно рассмотрение моделей ее функционирования.

Старшие менеджеры используют класс информационных СУ, названных исполнительными системами поддержки принятия решений (ESS), которые обслуживают стратегический уровень организации. Они ориентированы на неструктурированные решения и проводят системный анализ окружающей среды лучше, чем любые прикладные и специфические системы. ESS разработаны,

чтобы включить данные относительно внешних результатов типа новых налоговых законов или конкурентов, но они также выбирают суммарные данные из внутренних MIS и DSS. Они фильтруют, сжимают и выявляют критические данные, сокращая время и усилия, требуемые для получения информации, полезной для руководителей. ESS используют наиболее продвинутое графическое ПО и могут поставлять графики и данные из многих источников немедленно в офис старшего менеджера или в зал заседаний.

В отличие от других типов информационных систем ESS не предназначены для решения определенных проблем. Вместо этого ESS обеспечивают обобщенные вычисления и передачу данных, которые могут применяться к изменяющемуся набору проблем. ESS имеют тенденцию использовать меньшее количество аналитических моделей, чем DSS.

ESS помогают найти ответы на следующие вопросы:

- в каком бизнесе мы должны быть;
- что делают конкуренты;
- какие новые приобретения защитили бы нас от циклических деловых колебаний;
- какие подразделения мы должны продать, чтобы увеличить наличность?

ESS состоит из рабочих станций с меню, интерактивной графикой и возможностями связи, которым могут быть доступны исторические и конкурентоспособные данные из внутренних систем и внешних баз данных (БД). Так как ESS разработаны для использования старшими менеджерами, которые часто имеют немного прямых контактов с машинными ИС, ESS имеют легкий в использовании интерфейс.

Системы поддержки принятия решений (DSS) помогают принятию решений управления, объединяя данные, сложные аналитические модели и удобное для пользователя программное обеспечение (ПО) в единую мощную систему, которая может поддерживать слабоструктурированное и неструктурированное принятие решений. DSS находятся под управлением пользователя от начала до реализации и используются ежедневно.

Основная концепция DSS — дать пользователям инструментальные средства, необходимые для анализа важных блоков данных, используя легкоуправляемые сложные модели гибким способом. DSS разработаны для того, чтобы предоставить возможности, а не просто для того, чтобы ответить на информационные потребности.

Принятие решений включает в себя четыре этапа: распознавание, проект, выбор и реализация. DSS предназначены для того, чтобы помогать проектировать, оценивать альтернативы и контролировать процесс реализации.

Система поддержки принятия решений имеет три основных компонента: БД, модели и систему программного обеспечения DSS (рис. 1.1). База данных DSS — собрание текущих или исторических данных из ряда приложений или групп, организованных для легкого доступа к областям применения. Система управления БД DSS защищает целостность данных при управлении, которое хранит поток данных, а также сохраняет исторические данные. DSS используют организационные данные (из таких систем, как производство и продажа) так, чтобы личности и группы были способны принять решения, основанные на фактических данных. Данные обычно извлекаются из соответствующих БД и запасены специально для использования DSS. Модель БД — это комплекс математических и аналитических моделей, которые могут быть сделаны легкодоступными для пользователя DSS. В то же время

Рис. 1.1. Функциональная схема взаимодействия DSS с другими информационными СУ

БД — это абстрактное представление, которое поясняет компоненты или связи явления.

Анализ моделей часто используется для того, чтобы предсказать продажу. Пользователь этого типа модели мог быть снабжен набором предыдущих данных, чтобы оценить будущие условия и продажу, которые могли бы следовать из этих условий. Изготовитель решения может затем изменить эти будущие условия (например, повышение затрат сырья или появление новых конкурентов на рынке), чтобы определить, как эти новые условия могли бы влиять на продажу. Компании часто используют это ПО для того, чтобы попытаться предсказать действия конкурентов.

Программное обеспечение DSS обеспечивает простое взаимодействие между пользователями системы, БД DSS и эталонным вариантом. Подсистема ПО DSS управляет созданием, хранением и восстановлением моделей в образцовой основе и интегрирует их с данными в базе данных DSS. Система программного обеспечения DSS также обеспечивает графический, легкий в использовании, гибкий интерфейс пользователя, который поддерживает диалог между пользователем и DSS. Пользователи DSS — это обычно исполнители или менеджеры. Часто они имеют малый опыт работы с компьютером или вообще не имеют его, поэтому интерфейс должен быть дружественным.

DSS также обслуживают уровень управления организацией. Они помогают менеджерам принимать решения, которые являются слабоструктурированными, уникальными или быстро изменяющимися и которые не могут быть легко указаны заранее. Эти системы должны быть достаточно гибкими, чтобы использоваться несколько раз в день, соответствуя изменяющимся условиям. DSS в основном используют внутреннюю информацию из TPS и MIS, но часто вводят информацию из внешних источников типа текущих цен на бирже или цен изделия конкурентов.

DSS имеют большую аналитическую мощность, чем другие системы: они построены с рядом моделей, чтобы анализировать данные. Они построены так, чтобы пользователи могли работать с ними непосредственно; эти системы имеют удобное для пользователя ПО. Системы DSS интерактивны; пользователь может изменять предположения и включать новые данные.

DSS помогают находить ответы не только на прямой вопрос: «что, если?», но и на подобные вопросы. Типичные примеры технологий поддержки решений:

1) анализ примеров — оценка значений выходных величин для заданного набора значений входных переменных;

2) параметрический («что, если?») анализ — оценка поведения выходных величин при изменении значений входных переменных;

3) анализ чувствительности — исследование поведения результирующих переменных в зависимости от изменения значений одной или нескольких входных переменных;

4) анализ возможностей — нахождение значений входной переменной, которые обеспечивают желаемый результат (известен также под называниями «поиск целевых решений», «анализ значений целей», «управление по целям»);

5) анализ влияния — выявление для выбранной результирующей переменной всех входных переменных, влияющих на ее значение, и оценка величины изменения результирующей переменной при заданном изменении входной переменной, например на 1 %;

6) анализ данных — прямой ввод в модель ранее имевшихся данных и манипулирование ими при прогнозировании;

7) сравнение и агрегирование — сравнение результатов двух или более прогнозов, сделанных при различных входных предположениях, или сравнение предсказанных результатов с действительными, или объединение результатов, полученных при различных прогнозах или для разных моделей;

8) командные последовательности — возможность записывать, исполнять, сохранять для последующего использования регулярно выполняемые серии команд и сообщений;

9) анализ риска — оценка изменения выходных переменных при случайных изменениях входных величин;

10) оптимизация результатов — поиск значений управляемых входных переменных, обеспечивающих наилучшее значение одной или нескольких результирующих переменных.

Управляющие информационные системы MIS обслуживают управленческий уровень организации, обеспечивая менеджеров докладами, в некоторых случаях — с интерактивным доступом к текущей работе организации и историческим отчетам. Обычно они ориентируются только на внутренние результаты, не относящиеся к окружающей среде. MIS прежде всего обслуживают функции планирования, управления и принятия решений на управленческом уровне. MIS суммируют результаты и докладывают об основных действиях компании.

Характеристика управляющих информационных систем:

- поддерживают структурированные и слабоструктурированные решения на эксплуатационном и управленческом уровнях; могут быть полезны для планирования штата главных менеджеров;
- ориентированы для отчетов и контроля; разработаны для того, чтобы помогать обеспечивать текущий учет действий;
- полагаются на существующие общие данные и потоки данных;
- имеют немного аналитических возможностей;

• помогают в принятии решений, используя старые и новые данные;
• относительно негибки;
• имеют, скорее, внутреннюю, чем внешнюю ориентацию;
• часто требуют длинного анализа и проектирования процесса;
• информационные требования известны и устойчивы.

MIS обычно обслуживают менеджеров, заинтересованных в еженедельных, ежемесячных и ежегодных результатах. Эти системы вообще негибки и имеют немного аналитических возможностей. Большинство MIS используют простую установившуюся практику типа резюме и сравнения, в противоположность сложным математическим моделям и статистическим методам.

Системы работы «знания» (KWS) и системы автоматизации делопроизводства (OAS) обслуживают информационные потребности на уровне знаний организации. Системы работы «знания» помогают работникам знания, в то время как системы автоматизации делопроизводства прежде всего помогают обработчикам данных.

Работники знания — это люди, обладающие учеными степенями, которые часто имеют такие профессии, как инженер, врач, адвокат, а также ученые. Их работа заключается прежде всего в создании новой информации и знаний. Системы работы «знания» типа научных или инженерных рабочих станций (мест), а также автоматизированных рабочих мест (АРМ) способствуют созданию новых знаний и гарантируют, что новые знания и технический опыт должным образом интегрируются в бизнес.

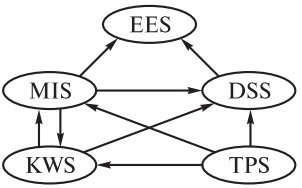
Обработчики данных обычно имеют образование, которое по уровню ближе к обработке, чем к созданию информации. Они состоят прежде всего из секретарей, бухгалтеров или менеджеров, чья работа заключается главным образом в использовании или распространении информации.

Системы автоматизации делопроизводства — информационные приложения технологии, разработанные для увеличения производительности труда обработчиков данных в офисе.

Системы диалоговой обработки запросов (TPS) — основные деловые системы, которые обслуживают эксплуатационный уровень организации. TPS — компьютеризированная система, которая выполняет и рассчитывает рутинные транзакции, необходимые для проведения бизнеса (например, коммерческие расчеты продаж, системы бронирования мест в гостинице, платежная ведомость, хранение отчетов служащих и отгрузка).

Описанные ранее системы интегрируют между собой. Их сочетание зависит от конкретной ситуационной модели (рис. 1.2). Общая схема взаимосвязей приведенных ИС показала, что связи между DSS с существующими TPS организации, KWS и MIS являются преднамеренно неопределенными. В некоторых случаях DSS тесно

Рис. 1.2. Взаимосвязи между информационными СУ



связаны с существующими общими информационными потоками. Однако часто DSS изолированы от главных организационных ИС.

DSS имеют тенденцию быть автономными системами, разработанными для конечных пользователей — отделов или групп не под центральным управлением, хотя целесообразнее, если они объединены в организационные системы, когда это функционально требуется.

1.2. Функции, процедуры, объекты и задачи административного управления в ИС

Описанные ранее основные конфигурации и модели функционирующих информационных СУ требуют организационной, программной и технической поддержки. Это реализуется через работу системного администратора.

Действия, выполняемые администратором, могут изменяться в зависимости от рабочей среды и приложений, с которыми приходится работать. Но независимо от среды необходимо иметь системную политику и строго следовать ей, а также ознакомить с данной политикой всех пользователей.

Это лишь одна из многих стратегий, которым нужно следовать в работе.

Иногда создается впечатление, что основная задача системного администратора заключается в выслушивании упреков в свой адрес, когда система работает не так, как того ожидают пользователи.

Действительно, когда дела идут нормально, работа над системой кажется чем-то, не заслуживающим особого внимания. И лишь тогда, когда система начинает давать сбои, вспоминают о существовании администратора. Самое лучшее, что можно сделать, — это заранее поработать над системой, чтобы не допустить подобной ситуации.

Администратор решает самые разные вопросы. Чаще всего его задача заключается в нахождении компромисса между различными противоречивыми интересами. Администратор — это пользователь со многими привилегиями. Он разрешает все проблемы, возникающие при работе системы, отвечает за ее загрузку и остановку.

Независимо от того, занимаете вы формально должность администратора или совмещаете администрирование с другими делами, вашей основной обязанностью будет поддержка системы и обеспечение бесперебойной работы сервисов.

Несомненно, основной задачей системного администратора является поддержка работы компьютеров. При работе с системой необходимо ее запускать и останавливать работу. При этом необходимо проверять, работает ли система, есть ли на дисках свободное место и корректно ли работают необходимые сервисы.

Очевидно, что как только поступит сообщение о том, что система перестала работать, руководство сразу же обратит на это внимание.

В таких случаях необходимо знать технологии упреждающего мониторинга системы. Если правильно применять описанные методы на практике, то можно, как правило, заранее знать о том, что система скоро может выйти из строя.

На примере мониторинга, применяемого в системах Unix, можно выделить упреждающие технологии.

Процедура сбора данных или сбор нужной информации по следующим частям информационных СУ:

- центральный процессор (ЦП) — здесь фиксируется использование ЦП, обычно по средней нагрузке, и определяется производительность системы;
- память — сбор данных для ее мониторинга осуществляется перемещением на жесткий диск блоков памяти (страниц памяти), в том числе и блоков с оперативной памятью, и, наоборот, восстановлением в оперативной памяти страниц, хранящихся на диске. При интенсивном обмене информацией между памятью и диском происходит «пробуксовывание» системы;
- файлы журналов — они служат документальным подтверждением ошибок и отказов сервисов, работающих в системе;
- диски — на них хранятся файлы операционных систем (ОС) и БД. Команды ОС прежде всего задействуются с дисков;
- пользователи — их мониторинг распространяется как на авторизованных регистрацией пользователей, так и на законных. Обе эти группы могут быть источниками проблем, возникающих при функционировании системы.

В сетевой среде для получения информации о других системах можно воспользоваться возможностями сети, например с помощью удаленного управления. Чтобы в каждой системе не регистрироваться и не запускать команды, целесообразно пользоваться локальными агентами. Тогда можно выполнять мониторинг какого-либо параметра системы и передавать на удаленную консоль отчеты о его состоянии.

При мониторинге сетевых сервисов можно написать сценарий для одной системы сети, имеющей доступ к сетевым сервисам

другой системы, и из центрального пункта осуществлять проверку и сбор данных.

Типовая технология мониторинга (сбор и анализ данных) состояния системы предусматривает четыре этапа:

1) определение цели сбора информации (например, по состоянию обработки сообщений электронной почты, обработки учетных записей зарегистрированных в системе пользователей, реализации соглашений по обслуживанию и т.д.). Здесь же вырабатываются критерии оценки для последующего анализа;

2) создание сценария сбора информации. Необходимо определить последовательность команд, их кратность использования, в том числе и в автоматизированных режимах;

3) систематизация и подготовительная обработка информации — наиболее важный этап, так как он определяет итоговые результаты выводов;

4) анализ и синтез полученных результатов; определение тенденций и закономерностей реакций системы на воздействие; выявление информации для дальнейшего планирования и принятия решений по системе.

Большое значение в мониторинге информационных СУ придается состоянию функционирования системы памяти.

Все команды выполняются программами, записанными на диск (или встроенными в оболочку). В системе Unix все устройства представляются как файлы. Данные, обрабатываемые на узле, также расположены на диске. На диске (в области подкачки) могут быть расположены даже некоторые фрагменты оперативной памяти.

Практически все, с чем работает система, записывается на диск, поэтому нужно вовремя подключать новые диски, создавать разделы файловой системы, проверять целостность файловых систем (в этом поможет команда fsck), создавать резервные копии и восстанавливать данные, а также при необходимости освобождать дисковое пространство.

Необходимо выработать политику резервного копирования. Эта задача часто осложняется тем, что размеры современных дисков очень велики. Производители накопителей на лентах быстро увеличивают объем своих устройств, что способствует решению данной проблемы.

Мониторинг периферийных устройств также необходим. Принтеры, устройства чтения компакт-дисков и другие устройства обычно хорошо работают в среде Unix, однако для этого надо выполнить соответствующие настройки. Unix представляет все устройства как файлы, поэтому приходится создавать новые записи об устройствах в каталоге /dev.

Unix предоставляет возможность совместного использования принтеров через сеть, однако для этого нужно настроить программу lp или lpr так, чтобы она отправляла по сети запросы к

соответствующей машине. Если принтер подключен к системе, то необходимо сконфигурировать средства, предназначенные для приема по сети запросов на печать. Также нужно проследить, чтобы в системе спулинга было достаточно дисковой памяти для хранения требуемого количества документов определенного размера. Нехватка свободного места на диске является основной проблемой при работе с принтерами через сеть.

Мониторинг сети — довольно сложная задача.

Большинство систем, работающих под управлением Unix, соединены с другими системами. Это значит, что нужно правильно сконфигурировать каждую систему в сети, чтобы обеспечить взаимодействие между ними. Способность к обмену информацией не должна снижаться при расширении сети и замене маршрутизаторов, концентраторов, коммутаторов и мостов. Необходимо гарантировать нормальную работу сетевых кабелей, а также обеспечивать нормальное время отклика при повышенной загруженности сети.

Устанавливая новые системы, надо подключить их к сети. В круг обязанностей администратора входит присвоение узлам имен и IP-адресов и настройка сетевых интерфейсов. После того как новая система будет настроена, необходимо, чтобы о ее существовании узнали все остальные системы в сети. Для этого требуется настроить NIS (Network Information Service — сервис сетевой информации «служба») или DNS (Domain Name Service — сервис доменных имен).

Пользователи в мониторинге системы занимают особое положение. Многие системные администраторы жалуются на своих пользователей, хотя именно ради них существуют системы, которыми управляют администраторы. Им часто приходится добавлять и удалять пользователей, следить, чтобы пользователи выполняли корректные действия. Многие задачи, касающиеся работы с пользователями, имеют непосредственное отношение к системе безопасности Unix (эти вопросы подробно рассмотрены в гл. 4). Возможно, придется изменять пароли пользователей, назначать исходные пароли и следить, чтобы при выборе пароля пользователи не выбирали очень простые последовательности символов. При этом может пригодиться программа COPS (Computer Oracle and Password System).

Возможно, администратору придется помогать пользователям решать повседневные задачи, связанные с вычислениями. Если это занимает слишком много времени, то можно придумать другой способ содействия пользователям, например создать Web-страницу, содержащую список часто встречающихся вопросов и ответы на них (список FAQ), и разместить ее во внутренней сети компании.

Большинство разработчиков очень требовательны. Им необходимо устанавливать новые версии ПО, часто создавать резервные

копии, поддерживать справочную систему для отладчиков и т.д. Чтобы облегчить эту работу, можно установить систему, с помощью которой пользователь будет сам создавать резервные копии. Также можно выделить для разработчика определенную область, где он будет иметь право сам устанавливать ПО.

Операционная система в мониторинге — предмет особого внимания администратора. Занимаясь администрированием, приходится часто устанавливать заплаты для компонентов операционной системы или ее более новые версии. Это особенно важно при взаимодействии с Интернетом или при работе над проектами, для которых требуются последние версии JVM (Java Virtual Machine — виртуальная машина Java). Иногда требуется установить заплату (patch), а иногда приходится полностью переустановить систему. Производители Unix постоянно добавляют новые компоненты к своим операционным системам и устраняют замеченные ошибки.

Обеспечение безопасности системы — еще одна задача, при решении которой часто приходится устанавливать заплаты в системе. Как правило, очередные пробелы в системе защиты обнаруживаются раз в месяц. В некоторых ОС, не принадлежащих к семейству Unix, такие недостатки выявляются каждую неделю. Доработка ОС может сводиться к замене исполняемого файла, но иногда предполагает достаточно сложные действия, например изменение двоичного кода ядра с помощью отладчика. Большинство производителей Unix поставляют специальные инструменты, с помощью которых можно быстро и надежно установить заплаты. Перед изменением ядра Unix всегда нужно создавать резервную копию системы. Также обязательно нужно прочитать файлы readme или инструкцию, поставляемую вместе с заплатами.

Системный администратор должен обновлять ПО и управлять его использованием. В некоторых случаях необходимо убедиться, что все нужные домены запущены и пользователи имеют доступ к требуемым приложениям. Не исключено, что именно в тот момент, когда все приложения заработают нормально, необходимо будет обновить их для того, чтобы они соответствовали новой версии ОС.

Несмотря на то, что вопросы безопасности, как правило, связаны с работой пользователей, необходимо учитывать, что среди них могут быть такие, которые хотят получить доступ к системе, не имея на это права.

Необходимо постоянно принимать меры против несанкционированного доступа; это особенно важно, если система подключена к Интернету. Даже если хакер, проникая в систему, не ставит целью разрушить ее, он все равно может случайно вывести систему из строя.

Необходимо также проверять защиту каждый день, чтобы узнать, не предпринималась ли попытка взлома. Помогут в этом системы обнаружения вторжений.

Основная задача большинства систем Unix заключается в предоставлении тех или иных сервисов. Система может выполнять функции сервера баз данных, Web-сервера, файлового сервера, почтового сервера и т.д. Главная задача администратора заключается в обеспечении такого уровня обслуживания, который позволит пользователям выполнять свою работу.

От системы постоянно ожидают определенных сервисов. Для того чтобы эффективно обеспечивать сервис, необходимо знать, в чем действительно нуждаются пользователи. Нужно работать, тесно сотрудничая с пользователями, чтобы понимать и удовлетворять их потребности.

Не обязательно дожидаться, когда пользователи обратятся с просьбами и вопросами. Необходимо выступать инициатором взаимодействия с пользователями.

Когда администрация отказывается выделять деньги на покупку оборудования, которое требуют пользователи, считается, что виноват в этом системный администратор. Пользователи часто не отдают себе отчет, что он работает в рамках бюджета и вынужден распределять его на решение различных задач. Необходимо объяснить пользователям реальное положение дел.

Соглашение о предоставляемых услугах — один из способов убедиться в том, что стороны «говорят на одном языке». Достигнув необходимого уровня обслуживания, необходимо контролировать его. Требуется проверить, имеют ли пользователи доступ к требующимся им данным, хватает ли им времени, выделенного для работы с сетью, чтобы успешно решать повседневные задачи.

Например, система Unix обеспечивает следующие сервисы:

- файлы. Файловый сервер часто использует NFS (Network File System — сетевая файловая система) и предоставляет дисковое пространство и данные компании для совместного использования. В сочетании с резервным копированием это помогает сохранить целостность данных компании и обеспечивает доступ из различных систем. Другой способ работы с файлами — использование протокола System Message Block (SMB), применяющегося в системе Windows;
- принтеры. В настоящее время компьютеры выводят больше бумажных копий данных, чем когда-либо раньше. Некоторые пользователи распечатывают все приходящие к ним письма и подшивают их. Хотя о рациональности таких действий можно поспорить, все равно следует признать, что это отличный способ создания резервных копий;
- приложения. Система Unix может служить хорошей базой для работы приложений. В стандартной среде сервера приложений

пользователи сначала регистрируются, а затем запускают программу, например СУБД. С появлением Java и других похожих технологий термин «сервер приложений» приобрел новый смысл. Система Unix может служить центральным хранилищем для приложений, написанных на Java и представленных в виде файлов .class (скомпилированные Java-программы) и архивов JAR (Java Archive), которые копируются на клиент-машину, например ПК;

• данные. В наше время пользователей часто даже не интересует, какие приложения они используют. Они просто обращаются к данным. Очень важно обеспечить безопасность и целостность данных. В их распоряжении могут оказаться серверы, собирающие данные и преобразующие их в другой формат; такие серверы называются серверами данных;

• Web-документы. Unix очень часто используется для публикации Web-страниц. На работу Web-сервера влияет производительность сети и файловой системы. Если Web-сервер доступен из Интернета, то вопросы защиты приобретают особое значение.

Сервисы, предоставляемые системой, вероятно, будут сочетанием перечисленных ранее типов сервиса. Например, сервер данных может также выполнять функции Web-сервера. Такая система преобразует данные и представляет их в формате Web-документа.

Среда Web очень похожа на среду разработки ПО тем, что они обе нуждаются в хранении различных версий документов. Как для HTML и других Web-документов, так и для исходных кодов программ следует обеспечить средства управление версиями. Средства, обеспечивающие контроль за новыми реализациями программ, хорошо работают и с Web-документами. Некоторые подобные пакеты работают в Unix; среди них можно отметить систему SCCS (Source Code Control System — система управления исходными кодами), которая поставляется с многими версиями Unix, и свободно распространяемый продукт RCS (Revision Control System — система управления реализациями).

Помимо нагрузки сервисов, работу которых администратору необходимо обеспечивать, может быть нагрузка по объему работы. Администрирование 10 систем Unix в корне отличается от администрирования 1 000 систем, а обслуживать пять пользователей гораздо проще, чем обслуживать 5 000 пользователей.

Каждый узел чем-то отличается от остальных. Особенности работы администратора зависят от перечня сервисов, объема ресурсов (данных, пользователей, транзакций и т.д.) и типа рабочей среды.

Для того чтобы успешно справиться с ролью администратора, необходимо хорошо знать систему и ее отличие от других систем.

1.3. Правила, регламенты и стратегия администрирования в ИС

1.3.1. Основные положения стратегии администрирования

Для реализации основных задач ИС администрирование обязано организовать, структурировать и систематизировать обслуживание пользователей. Учитывая декларативный принцип любой системной организации управления (см. подразд. 1.1), вся стратегия администрирования должна быть первоначально построена на основе правил и регламентов.

Документально оформленные, доведенные до сведения всех сотрудников правила и регламенты необходимы для нормального функционирования любой организации.

Они должны быть соответствующим образом оформлены, утверждены руководством и проверены юристами. Лучше это сделать до того, как возникнет необходимость обращения к подобным документам для решения какой-нибудь острой проблемы. Желательно, чтобы в каждой организации были следующие документы:

- правила административного обслуживания;
- регламенты прав и обязанностей пользователей;
- правила для администраторов (пользователей с особыми привилегиями);
- правила создания «гостевых» учетных записей.

Для систематизации практического опыта можно использовать различные регламенты, оформленные в виде контрольных списков и инструкций. Эти документы полезны как для новых администраторов, так и для ветеранов.

Преимущества, получаемые при использовании регламентов:

- рутинные задачи всегда выполняются одинаково;
- уменьшается вероятность появления ошибок;
- работа по инструкциям выполняется администратором гораздо быстрее;
- изменения самодокументируются;
- корректность действий администратора можно соизмерять с неким эталоном.

В современных системах почти все стандартные задачи документированы в форме контрольных списков и инструкций. В Unix они называются «run books» или «checklists» и доступны в оперативном режиме или хранятся в печатном виде. Написанием и поддержкой этих инструкций занимается дополнительная группа системных администраторов (не входящая в состав основного штата системных администраторов, обслуживающих технику и использующих эти инструкции). Тем не менее такая организация и стандартизация в конечном счете окупаются.

В перечень таких регламентов входят:

- подключения компьютера;
- подключения пользователя;
- настройки и конфигурирования компьютера;
- установки библиотеки TCP-оболочек на компьютер;
- настройки резервного копирования для нового компьютера;
- защита нового компьютера;
- перезапуск сложного программного обеспечения;
- восстановления Web-серверов, которые не отвечают на запросы или не предоставляют данных;
- разгрузки очереди и перезагрузки принтера;
- модернизации операционной системы;
- инсталляции пакета прикладных программ;
- инсталляции программного обеспечения по сети;
- модернизации наиболее важных программ (sendmail, gcc, named и т.д.);
- резервные копирования и восстановления файлов;
- выполнение аварийной остановки системы (всех компьютеров; всех, кроме наиболее важных, компьютеров и т.д.).

Некоторые положения инструкций диктуются особенностями ПО, с которым вы работаете, либо правилами, принятыми в тех или иных сторонних группах, например у поставщиков услуг Интернета. Соблюдение некоторых положений является обязательным, особенно если вы должны обеспечить секретность данных пользователей. В частности, управление интернет-адресами, именами компьютеров, идентификаторами пользователей и групп, регистрационными именами должно осуществляться единообразно для всех компьютеров организации. Для больших структур (в частности, транснациональных корпораций) такой подход реализовать не просто, но если удастся это сделать, управление значительно упростится.

Средства, которые облегчают управление хостами и пользовательскими учетными записями, можно получить по сети, например программы на узле ftp.xor.com. Также ни в коем случае нельзя предоставлять нескольким пользователям одно и то же регистрационное имя. Это правило гораздо легче внедрить, если сразу же устранить соблазн коллективного использования имени. Хорошая альтернатива несанкционированному применению одного и того же имени — «гостевой» компьютер с либеральными правилами создания учетных записей. Однако сейчас, когда некоторые службы (AOL, Hotmail, Yahoo и др.) предоставляют адреса электронной почты и существует доступ к Интернету из библиотек, интернет-кафе, такой метод не эффективен.

Многие вопросы регламента относятся не только к локальной административной группе, например:

- нарушения системы защиты;

• управление экспортом в NFS;
• критерии выбора паролей;
• удаление регистрационных имен;
• защита материалов знаком авторского права (например, для файлов MP3 и DVD);
• программное пиратство.

Обеспечение связи между административными группами в крупных организациях — один из важнейших факторов предотвращения проблем и создания атмосферы доверия и сотрудничества. Некоторые группы администраторов применяют для общения такие средства, как MUD и MOO. При разумном использовании, безусловно, будут полезны и другие методы, особенно если часть персонала работает дома.

1.3.2. Правила и регламенты администрирования

В правилах для администраторов (и других лиц с особым статусом) должны быть сформулированы руководящие принципы использования предоставленных привилегий и соблюдения секретности пользовательских данных. Трудно, конечно, ответить на жалобу пользователя о том, что почта не работает, не видя «отскочивших» сообщений, но копии заголовка в большинстве случаев хватает для определения сути проблемы и способа ее устранения.

В системе Unix, например, применяют следующие правила.

Если для доступа в систему с правами root применяется программа типа sudo, то администраторам следует выбирать надежные пароли и не делить учетные записи с кем попало. Регулярно проверяйте пароли системных администраторов при помощи программы crack. Кроме того, важно, чтобы они не использовали команду sudo tcsh, поскольку нарушится способность sudo регистрировать события и выполняемые команды.

Некоторые системные администраторы злоупотребляют своими возможностями. Таким сотрудникам лучше предложить другие должности.

В ряде организаций обладание паролем root является символом занимаемого положения. Иногда этот пароль есть у инженеров, которым он не нужен или не должен выдаваться.

Другой проверенный метод — поместить пароль root в конверт и спрятать его в известном месте. Администраторы обычно пользуются в своей работе программой sudo; если по какой-либо причине им понадобится пароль root, то они вскроют конверт. После этого пароль root меняется и прячется в новый конверт. Конечно, вскрыть конверт ничего не стоит, но доступ к тому месту, где он хранится, имеют только администраторы.

Большое значение имеют правила и регламенты, которые необходимы в экстренных случаях. Для этого необходимо заблаговременно решить вопрос о том, кто будет руководить работой в случае нарушения защиты. Заранее определяется субординация; имена и телефоны должностных лиц держатся вне системы. Может оказаться так, что лучшим руководителем в подобной ситуации будет администратор сети, а не директор вычислительного центра (обычно он не подходит для этой роли).

Для общения и получения документов обычно пользуются сетью. В случае инцидента с защитой доступ к сетевым средствам может быть затруднен или вообще окажется невозможным. Сведения о своих связях и методиках держатся также вне сети. Нельзя забывать о том, где можно взять последние дамп-ленты и какие команды нужное использовать для восстановления без обращения к файлу /etc/dumpdates. Нужно избегать расспросов со стороны представителей средств массовой информации, особенно если инцидент получает развитие.

У хакеров в настоящее время распространено взламывание Web-узлов. Для системных администраторов компании, предоставляющей услуги Web-хостинга, такой взлом — очень большая неприятность. Тут же начинаются телефонные звонки от обеспокоенных клиентов, средств массовой информации (СМИ) и партнеров компании. Кто будет отвечать на все эти звонки? Что он скажет? Кто возьмет на себя ответственность за исправление ситуации? Какими будут обязанности каждого из членов персонала? Если ваш бизнес на виду у широкой общественности, то все это нужно очень тщательно продумать и, возможно, провести учения.

Мероприятия по нейтрализации нарушений защиты в ИС будут рассмотрены далее.

Правила работы по администрированию в аварийных ситуациях требуют четкого планирования действий всего персонала организации. Действия персонала в случае аварии нужно планировать заранее. Наиболее сложные аварии случаются на ноутбуках руководителей.

Приведем несколько типовых аварий и непредвиденных ситуаций:

- нарушение защиты (60 % нарушений защиты обычно происходит внутри организации);
- внешние воздействия на технику: скачки напряжения и отключение питания, поломки кондиционеров и вентиляторов, потопы, ураганы, землетрясения, метеоры;
- человеческие ошибки: удаленные или поврежденные файлы и базы данных, потерянная конфигурационная информация (возможно, ваша система зеркалирования данных работает с такой скоростью, что ошибка успевает распространится в ней до того, как вы сообразите, что произошло);

• неожиданный выход из строя аппаратного обеспечения: отказ сервера, поломка жесткого диска, нарушение работы сети.

В любой из этих ситуаций необходим доступ к копиям важной информации, хранящейся в компьютерах и на внешних носителях. Для оперативного доступа к таким копиям нужно использовать независимый компьютер с богатым набором всевозможных утилит и инструментальных средств, специально настроенный и оборудованный для использования системными администраторами. На нем должен работать собственный сервер имен, должен быть полный файл /etc/hosts. Все необходимые для его работы файлы должны храниться на нем, а не где-то в сети. К нему должен быть непосредственно подключен принтер и т.д. На резервной машине следует хранить и иметь под рукой в распечатанном виде следующие данные:

• план действий персонала в случае аварии, в котором должно быть указано, кого и когда оповещать и что говорить;

• номера телефонов обслуживающих организаций и клиентов;

• важнейшие номера телефонов (персонала, полиции, пожарной службы, начальника, агентства по трудоустройству);

• сведения об аппаратном обеспечении и конфигурации программного обеспечения: таблицы разделов дисков, аппаратные установки компьютеров, номера прерываний, номера каналов DMA и т.д.;

• ленты с резервными копиями и расписание резервного копирования, использовавшееся для их создания;

• карты сети;

• серийные номера программного обеспечения, лицензионные данные и пароли;

• контактная информация производителей или продавцов дисков, которые должны быть восстановлены немедленно.

При составлении плана аварийных мероприятий обычно предполагается, что административный персонал будет на месте и он в состоянии справиться с ситуацией. Однако в реальности люди болеют, переходят на другие должности, уходят в отпуск и увольняются. Поэтому стоит заранее продумать, где можно быстро найти дополнительный персонал. (Если система не очень устойчива, а персонал неопытен, то недостаточное количество администраторов уже само по себе рискованно.)

Одним из решений может быть договор с местной консультационной компанией или другой организацией, в которой всегда имеются свободные системные администраторы. Но самое главное — обеспечение надежной работы системы; при необходимости нужно нанять достаточное число администраторов.

План аварийных мероприятий лучше проверить заранее. Необходимо основательно готовиться к выживанию в случае аварии. Возможно, стоит оставить кое-что из запасов, например фонари

с аккумуляторами (есть очень удобные фонари — они вставляются розетку и зажигаются, когда отключается электричество, так что их сразу легко найти).

Необходимо также проверить генераторы и источники бесперебойного питания (ИБП), убедиться, что все важные устройства подключены к ИБП, их батареи в порядке и механизм включения питания работает. Для проверки ИБП достаточно вынуть вилку из розетки, а для того, чтобы проверить, все ли важное оборудование к ним подключено, нужно отключить питание в здании или в комнате и убедиться, что все работает.

Как правило, электричество отключается ненадолго, но на всякий случай батареи должны обеспечивать 2 ч работы, чтобы было время правильно выключить технику. Некоторые ИБП оборудованы последовательными портами или интерфейсом Ethernet, позволяющим отключать не самые важные машины через 5 мин после отключения питания (тайм-аут настраивается).

Даже из краткосрочного отключения питания можно извлечь некоторую пользу, например добавить на сервер еще один диск или выполнить какую-то пятиминутную работу, которую вы давно запланировали. Некоторые неудобства будут приняты как нечто само собой разумеющееся. Люди обычно спокойнее воспринимают дополнительную пятиминутную задержку после отключения электричества, чем пятиминутное плановое отключение системы, о котором их оповестили за неделю. Если есть старые машины, которыми уже никто не пользуется, не включайте их, пока кто-нибудь не пожалуется на их отсутствие. Иногда отсутствие такой машины может оставаться незамеченным в течение нескольких недель.

Системы охлаждения часто оборудованы датчиками температуры со средствами оповещения о ее повышении. Лучше задать такую верхнюю границу температуры, чтобы после сигнала хватило времени выключить технику, прежде чем она перегреется и выйдет из строя. Хорошо хранить в машинной комнате обычный термометр или термометр, работающий от батареи. Нужно иметь в виду, что, как только отключится питание, все электронные индикаторы окажутся бесполезными.

Особенно опасно воздействие непредвиденных обстоятельств: резкое возрастание трафика, ошибки администраторов и т. д. Например, когда провайдеры услуг Интернета объединяются в более крупные компании или приобретаются крупными компаниями, нарушаются их тщательно разработанные планы поддержания избыточных подключений к Интернету. Объединяясь, компании часто объединяют и свои сети. Поэтому может оказаться, что имеющиеся два независимых соединения с Интернетом теперь выходят на общий оптоволоконный кабель.

Когда CNN или Sladshot объявляет, что Web-узел отключен, пользователи могут ринуться смотреть, как дела, в результате чего

трафик возрастет настолько, что может разрушить то, что только что было отремонтировано. Если Web-узел не рассчитан на 25%-е увеличение трафика, то целесообразно использовать простое ПО, балансирующее нагрузку. Оно может просто направлять лишние обращения на сервер, возвращающий одну и ту же страницу: «Извините, узел слишком загружен и в данный момент мы не можем обработать ваш запрос».

Другой способ — использование программы tripwire для согласования действий системных администраторов, особенно если разные группы администраторов отвечают за разные аспекты работы одной машины. Например, заплаты СУБД Oracle и заплаты операционной системы могут конфликтовать друг с другом, и поставившая одну из них группа администраторов может даже не подозревать, что причиной проблемы являются действия второй группы. Сведения, собранные программой tripwire, могут очень пригодиться и организации, предоставляющей административные услуги, если ее специалистам нужно восстановить систему клиента после неудачных действий его собственных администраторов. Эта программа легко определяет, что и когда изменилось, и поможет доказать местным системным администраторам, что именно их действия явились причиной неполадок.

1.3.3. Особенности реализации технологий администрирования в ИС

Системные администраторы обычно не отвечают за то, что пользователи хранят на машинах, которые они обслуживают. Провайдеры услуг Интернета чаше всего просто направляют всех, кто к ним подключается, к своим клиентам. Вся ответственность за действия клиентов возлагается на самих клиентов, а не на провайдеров или организации, предоставляющие услуги провайдерам. Целью такой политики является защита провайдеров от ответственности за spam и прочие неприятности, такие как хранение пользователями на своих узлах запрещенных материалов. Необходимо знать соответствующие законодательные акты.

Полезная юридическая информация имеется на узле www.mibh.net. Там есть сведения о незаконных действиях, нарушениях интеллектуальной собственности и нарушениях правил использования продуктов и услуг. Вы найдете на этом узле список запрещенных действий, ограничений, описание процедур регистрации жалоб и кое-что об ответственности.

В то же время существует угроза конфиденциальности, которую представляют провайдеры услуг Интернета. За обеспечение и регулирование конфиденциальности работы в Интернете взялась компания Predictive Networks, которая с помощью провайдеров планирует наблюдать за работой в сети и собирать информацию о

посещаемых пользователями URL, ключевых словах, вводимых в программы поиска ресурсов, и т.д. На основе этой информации она будет формировать цифровую подпись и пользовательский профиль, а также использовать его для того, чтобы подбирать интернет-ресурсы и рекламу персонально для пользователя.

Компания Predictive Networks утверждает, что эта информация будет анонимной и можно доверять всем, кто вовлечен в процесс ее сбора: сотрудникам компании Predictive Networks, сотрудникам своего интернет-провайдера, а также тем, кто размещает рекламу и ресурсы. Можно запросить копию своей цифровой подписи, но за это придется заплатить, а также отказаться от использования этого «сервиса», но тогда подключение к Интернету будет стоить дороже или провайдер даже сможет расторгнуть с пользователем договор. Информацию по этому вопросу можно посмотреть на Web-узле компании Predictive Networks (www.predictivenetworks.com), а также в статье из «PRIVACY Forum Digest» (V09, #13, www.vortex.com).

Применение для целей анализа информации и администрирования файлов регистрации является необходимым приемом. При этом целесообразно использовать для защиты официально заверенные бумажные документы, так как документы, представленные в электронной форме, не всегда могут возыметь должное действие. Некоторую пользу могут принести штампы времени в файлах регистрации, однако только в том случае, если на компьютере работает Network Time Protocol (NTP), синхронизирующий его часы с реальным временем. Правила безопасности помогут обнаружить злоупотребления.

Несанкционированное использование компьютерных систем фирмы связано с нарушением не только правил фирмы, но и законов государства. Несанкционированное использование является преступлением, влечет за собой уголовную и гражданскую ответственность и подлежит наказанию, предусмотренному законодательством.

Также рекомендуется помещать в файл /etc/motd (сообщение дня) предупреждение о действующих правилах. Оно может выглядеть следующим образом:

> В случае реального или предполагаемого инцидента с системой защиты вводимая вами с клавиатуры информация будет контролироваться.

Для некоторых типов соединений сообщение дня не отображается (например, во время сеанса ftp). Пользователи могут также воспрепятствовать выводу этого сообщения на экран, создав в своих начальных каталогах файл .hushlogin. Можно сделать так, чтобы пользователи прочли это уведомление хотя бы один раз — для этого нужно включить его в файлы запуска, выдаваемые новым пользователям.

Необходимо обязательно указать, что сам факт использования учетных записей пользователей равносилен согласию соблюдать установленные правила. Нужно объяснить, где можно получить экземпляры правил, и поместить основные документы на соответствующей доске объявлений, провести особые меры, которые будут приняты в случае их несоблюдения.

Проблемы в администрировании возникают и при защите авторских прав. Они появляются, например, при использовании возможностей службы Napster при применении формата DVD для просмотра фильмов и проигрывания музыки и в других случаях.

Содержимое диска в формате DVD шифруется по технологии CSS (Content Scrambling System). Это делается для того, чтобы диски могли проигрываться только лицензированными и одобренными плеерами. Эти плееры, как и лицензированное ПО для проигрывания, имеют ключ для раскодирования дисков.

Надо учитывать, что есть и другие случаи информационного противоборства, уже имеющие системный характер. Так, компания CyberPatrol разработала ПО для фильтрации данных, получаемых из Интернета. Религиозные организации распространяют это программное обеспечение в семьях, имеющих детей, в школах и библиотеках, чтобы оградить детей от того, чего им видеть не нужно. Компания A Canadian and a Swede разработала программу cphack, позволяющую расшифровывать списки блокировки, создаваемые ПО CyberPatrol. Целью этой разработки была необходимость узнать, какие Web-узлы заблокированы, каков уровень ошибок и какие невидимые программы присутствуют в системе. Ее сотрудники сообщили, что все, кто критиковал ПО CyberPatrol, заблокированы по всем категориям.

Владелец компании CyberPatrol подал в суд на авторов этой программы, утверждая, что лицензия CyberPatrol запрещает инженерный анализ ПО компании. Он получил предварительное судебное заключение, запрещающее распространение ПО, но авторы программы cphack продали ее владельцу компании за 1 долл. и согласились выполнить это постановление. Похоже, что авторы отступили. Владелец компании пытается доказать свои права на программу, выпущенную как общедоступное ПО (т.е. с лицензией GNU Public License).

Многие компании оплачивают меньшее количество копий программных пакетов, чем на самом деле используют. Если об этом становится известно, то компания теряет гораздо больше, чем сэкономила на приобретении недостающего числа лицензий. Другие компании получают демо-версию дорогого пакета и взламывают ее (меняют дату на компьютере, определяют лицензионный ключ и т.д.), чтобы пакет продолжал работать по истечении демонстрационного срока. Как системный администратор должен реагировать на предложения нарушить лицензионное соглашение

и установить нелицензионные копии продукта на дополнительные машины? Что ему делать, если он обнаружит, что на обслуживаемых им компьютерах работает пиратское ПО? Как быть с условно-бесплатными программами, за которые так никогда и не заплатили?

Это сложный вопрос. К сожалению, руководство не всегда поддерживает администратора, предлагающего либо удалить нелицензионные копии пакетов, либо оплатить их. А ведь часто именно системный администратор подписывает лицензионное соглашение, требующее удалить демонстрационные копии после определенной даты, тогда как решение их не удалять принимает руководитель.

Необходимо помнить, что речь идет о личной и профессиональной честности как администратора сети, так и руководителя организации.

Безопаснее всего ситуация, когда организация, являясь подписчиком всех телеконференций, не подвергает цензуре их статьи и не сокращает иерархию телеконференций на основании их содержания. Другое дело, когда для сокращения появляются основания технического характера (например, нет места на диске). Если иерархию телеконференций нужно сократить, сделайте это ближе к вершине дерева. Легче оправдать отказ от всей категории alt, чем объяснить, зачем удалили alt.sex.fetish.feet и оставили alt.sex.bestiality.hamsters.

Этот подход распространяется и на другие отношения с внешним миром. С юридической точки зрения, чем больше администратор сети контролирует использование Интернета пользователями, тем бóльшую ответственность он может понести за их действия и публикации. Если он к тому же знает о противоправной, подсудной деятельности, то закон обязывает расследовать ее и доложить о результатах в соответствующие органы.

По этой причине некоторые компании ограничивают данные, которые они вносят в журналы доступа на своих Web-узлах, сокращают время хранения журналов и не все их данные записывают в архивы и резервные копии. Для реализации подобной политики существует даже специальное ПО (например, Squid web cache), определяющее уровень протоколирования доступа, что позволяет системным администраторам разрешать возникающие проблемы и при этом не нарушать конфиденциальности действий пользователей.

Системные администраторы должны знать правила, действующие во всех подразделениях организации, и обеспечивать их неукоснительное соблюдение. При этом нужно учитывать, что не имеющие законной силы и противоречивые правила — это еще хуже, чем их отсутствие (как с практической, так и с юридической точек зрения).

Контрольные вопросы

1. По каким признакам классифицируются информационные СУ?
2. Каковы основные характеристики ИС по уровням управления?
3. Опишите функции систем по уровням управления.
4. Сформулируйте основные задачи административного управления в ИС.
5. Перечислите основные этапы типовой технологии мониторинга состояния информационных СУ.
6. Приведите перечень документов по обеспечению административного обслуживания и дайте комментарии к ним.
7. Приведите перечень регламентов системного администратора.
8. Перечислите правила администрирования в системе Unix по различным областям их применения.
9. Проанализируйте особенности реализации технологий администрирования при работе с Интернетом.