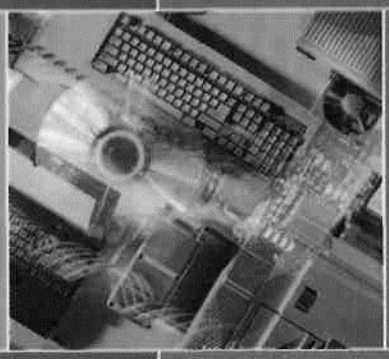
Высшее профессиональное образование

С. А. Клейменов
В. П. Мельников
А. М. Петраков

АДМИНИСТРИРОВАНИЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Учебное пособие



Информатика и вычислительная техника

ACADEMIA

ВЫСШЕЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАНИЕ

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»

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

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 СОКРАЩЕНИИ

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 слабоетруктурированное 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 названиями «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 од ной 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 решении, 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.

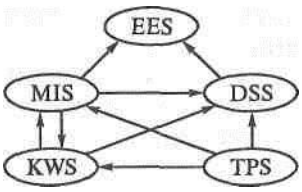
Обработчики данных обычно имеют образование, которое по уровню ближе к обработке, чем к созданию информации. Они состоят прежде всего из секретарей, бухгалтеров или менеджеров, чья работа заключается главным образом в использовании или распространении информации.

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 информаци онными 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 большую 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.

Глава 2

ПРОГРАММНОЕ И ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ СОВРЕМЕННЫХ ИС И ТЕХНОЛОГИЙ УПРАВЛЕНИЯ ОРГАНИЗАЦИЕЙ

2.1. Структура информационного обеспечения и программные средства ИС управления

2.1.1. Общие положения по структурной организации информационного обеспечения в ИС управления

Предприятие — это устойчивая формальная социальная структура, которая берет ресурсы из окружающей среды и обрабатывает их, чтобы произвести продукцию. Техническое представление сосредоточивается на трех элементах организации предприятия: капитал и рабочая сила (первичные факторы производства); внешняя среда.

Организация преобразовывает их в изделия и услуги посредством производства. Изделия и услуги используются окружающей средой, которая поставляет дополнительный капитал и рабочую силу как входы в цепи обратной связи. Организация более устойчива и долговечна, чем неформальная группа. Она имеет внутренние правила и процедуры, должна соблюдать законы.

Большое значение имеет поведенческое представление организации, совокупности прав, привилегий, обязательств и ответственностей. Схема поведенческого представления формальной организации представлены на рис. 2.1.

Наиболее реалистичное поведенческое представление организации предполагает, что создание новых ИС или переоборудование старых ИС влияет намного больше, чем техническая перестановка машин или рабочих. Некоторые ИС изменяют организационный баланс прав, привилегий, обязательств, ответственностей и чувств, который установился за длительный период времени.

Сегодня ИС помогают создавать и распространять знания и информацию в организации через новые системы работы. Системы «знания» и приложения обеспечивают компаниям доступ к данным и системам коммуникаций, связывающим разветвленное предприятие. Организации зависят от систем и не могут пережить даже случайную их аварию. Организации создают ИС, чтобы стать более эффективными и сохранять деньги. Они могут быть источником конкурентоспособного преимущества.

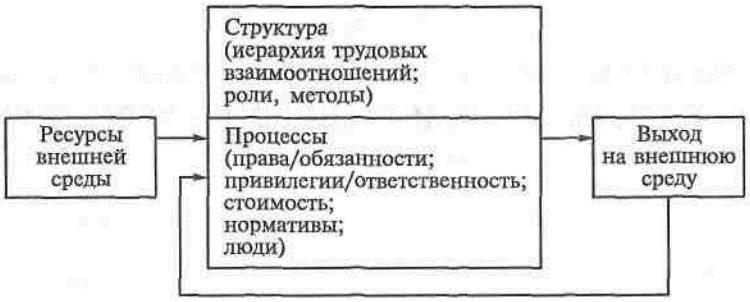


Рис. 2.1. Схема поведенческого представления формальной организации

С экономической точки зрения ИС могут рассматриваться как средства производства, которые могут свободно заменять рабочую силу. Они заменяют рабочую силу, которая исторически имеет возрастающую стоимость.

Другое финансовое воздействие ИС заключается во внутренних затратах управления. Фирмы зависят от затрат организаций, стоимости контролирующих и руководящих служащих. Размеры фирмы увеличиваются, затраты организации повышаются, потому что владельцы должны расходовать все больше усилий на контроль за служащими.

Исследование поведенческой теории нашло несколько доказательств того, что ИС автоматически преобразовывают организации. Исследования сложных связей, с помощью которых организации и ИС взаимно влияют друг на друга, показали, что информационные технологии (ИТ) в ИС могут изменять иерархию принятия решений в организациях, снижая затраты на приобретение информации и расширяя ее использование.

Еще одно изменение во взаимодействии ИС и организаций следует из возрастающей степени интеграции и области действия системы и приложений. Построение систем в настоящее время затрагивает большую часть организации, чем это было в прошлом. В то время как ранние системы производили в значительной степени технические изменения, которые влияли на часть персонала, современные системы вызывают управленческие изменения и установленные взаимосвязи. При изменении технологии в организации (например, в ПО) происходит изменение других компонентов: в кадрах — изменяются методы работы, необходимы преобразования структуры организации.

Информационные системы могут стать мощными инструментами и для создания более конкурентоспособных и эффективных организаций. ИС могут использоваться, чтобы перепроектировать организации, трансформируя их структуру, область действия, сред-

ства сообщения и механизмы управления работой, трудовыми процессами, изделиями и услугами.

Информационные системы с сетевой структурой дают возможность компаниям координировать работу географически распределенных подразделений в виде виртуальных корпораций (виртуальных организаций). Виртуальные организации используют сети, чтобы связывать людей, имущество и идеи, соединяя их с поставщиками и клиентами, чтобы создавать и распределять новые изделия и услуги без ограничений, присущих традиционным организационным границам.

Современная технология передачи данных предоставила многим организациям более гибкие способы работы, расширив возможности этих организаций реагировать на изменения рынка. ИС могут придавать большим и маленьким организациям дополнительную гибкость, чтобы преодолевать некоторые ограничения. Маленькие организации могут использовать ИС, чтобы приобретать часть сил и возможностей больших организаций.

Начиная с первых использований в бизнесе ИС прогрессивно заменили ручной труд на автоматизированные действия в трудовых и технологических процессах. Электронные трудовые процессы уменьшили стоимость эксплуатации во многих компаниях, заменив бумажные документы и установившуюся практику ручного труда.

Информационные технологии в ИС реорганизуют процесс управления, обеспечивая мощные новые возможности помощи менеджерам в стратегии, планировании и управлении. Например, стало возможным получение информации для менеджеров относительно организационного выполнения вплоть до уровня определенных изделий из любой организации в любое время. Новая интенсивность информации делает возможными точное планирование, предсказание и контроль. Распределяя информацию через электронные сети, новый менеджер с помощью администратора сети может эффективно связываться с тысячами служащих и даже управлять обширными целевыми группами.

Бизнес с использованием Интернета возник сразу после открытия сети гражданским организациям и пользователям. С самого начала это было предоставление доступа, электронной почты и места для размещения информации. Дополнительным толчком к росту числа пользователей и деловой активности стала разработка спецификаций языка описания гипертекстовых страниц HTML (Hyper-Text Markup Language), протокола их передачи по сети HTTP (Hyper-Text Transfer Protocol), а также программы для просмотра страниц гипертекста — так называемого броузера. Благодаря этим инновациям информация в Интернете получила современный вид. Размещение информации в Интернете стало на вполне законных основаниях называться электронной публикацией. Как

следствие возникла необходимость в таких услугах, как дизайн, верстка, программирование. Появились агентства Web-дизайна, которые занимаются созданием информационных ресурсов клиента в Интернете «под ключ». Электронная публикация открыла дорогу интернет-изданиям, интернет-рекламе и всему тому, что люди привыкли видеть на бумаге.

С появлением возможности безналичной электронной оплаты товаров и услуг и использования глобальной сети для проведения транзакций по всему миру появилось такое уникальное явление, как электронная коммерция. Многие Web-каталоги, существовавшие на тот момент в рекламных и информационных целях, были дополнены возможностью немедленного приобретения товара.

В развитых странах электронная коммерция в виде продаж товаров и услуг с использованием доступа по сети широко представлена не только благодаря высоким темпам технического прогресса, но и ввиду подготовленности населения к подобному виду сервиса. Дело в том, что в развитых странах десятилетиями практикуется приобретение товаров по каталогам, под заказ с доставкой на дом.

В настоящее время фирмами широко используется частичная или полная передача отдельных бизнес-функций и даже частей бизнес-процесса сторонним лицам и (или) организациям. Это явление получило название «аутсорсинг» (от *англ.* outsourcing — процесс получения чего-либо из внешних источников). Широкое развитие на Западе аутсорсинг получил по ряду причин.

Во-первых, это рост интенсивности конкурентной борьбы во всех секторах рынка и связанная с ней необходимость достижения наивысшей эффективности всех операций компании, стремящейся к завоеванию стабильного и долговременного преимущества над конкурентами.

Во-вторых, это стремление компаний быть глобальными, т.е. быть представленными своей продукцией и услугами по всему миру. Для этого, в первую очередь, необходимо отсутствие жесткой «привязки» к определенной территории.

В-третьих, это увеличение роли малых предприятий в мировом бизнесе. Аутсорсинг дает возможность глобального присутствия какой-либо компании на рынках многих стран без необходимости практически пропорционального роста персонала для обслуживания новых рынков сбыта и (или) производственных мощностей.

Новый подход к организации ИТ управления предприятий с разделением полномочий между его подразделениями получил название «динамическая сетевая организация», или «организация с модельной структурой». Координация действий осуществляется небольшим центральным офисом или брокером. Главное отличие такой структуры в том, что основные операции, такие как произ-

водство, разработка новой продукции, сервис, бухгалтерский учет, не собраны под одной крышей, а выполняются отдельными организациями (подразделениями) по контракту или по какой-либо другой договоренности.

Для связи с партнерами и подразделениями широко используются возможности глобальной сети, такие как электронная почта и видеоконференции.

Несмотря на то что в области применения сетевых технологий компьютерщикам «все карты в руки», самой первой компанией, которая в ходе расширения и глобализации бизнеса применила модульную структуру и добилась оглушительного успеха, была Nike — лидер американского рынка по производству и продаже спортивной одежды и инвентаря. Укрупненная структура сетевой организации на примере подразделения спортивного инвентаря компании Nike приведена на рис. 2.2.

Сетевая, или модульная, структура дает множество преимуществ. В первую очередь, это возможность сконцентрировать усилия персонала на решении нескольких основных задач, заказывая выполнение других функций, таких как доставка, бухгалтерский учет, а также производство, специалистам вне компании.

Важнейшим преимуществом является присутствие организации во многих странах мира, а также возможность завоевывать рыночные позиции везде, где есть такая возможность. Сетевая организация консолидирует ресурсы по всему миру с целью добиться наилучшего качества продукции при максимально низкой ее стоимости, что является одним из решающих факторов для достижения устойчивого преимущества над конкурентами.

Первый, наиболее существенный, недостаток сетевой структуры — слабый непосредственный контроль над всеми процессами.

Второй недостаток — сильная зависимость от работы смежников. Если нанятая фирма провалит заказанные поставки, работы,

Рис. 2.2. Укрупненная структура сетевой организации на примере подразделения спортивного инвентаря компании Nike

услуги, уйдет из бизнеса или сгорит завод, производящий конкурентную продукцию, то весь бизнес окажется под угрозой провала.

Третий недостаток — сложность работы с удаленными работниками в силу малой преданности общему делу.

При каждой смене линии продукции или рыночной ниши сетевая фирма вынуждена «перетасовывать» сотрудников для достижения оптимального набора квалификаций (skill mix).

Большое внимание новым ИТ уделяется в организации информационной поддержки удаленных сотрудников с использованием электронной почты.

Зачастую у сотрудника, не находящегося в офисе, возникает серьезная проблема «оторванности» от работодателя, коллектива, рабочей группы. Возникает чувство незащищенности, сотрудник не сдает работу вовремя и начинает искать более надежное рабочее место в офисе, с собственным рабочим местом и прочими атрибутами, удовлетворяющими его стремление к стабильности.

Для решения задач информационной поддержки удаленных сотрудников необходимо использовать систему управления базой данных, которая могла бы содержать индексацию и обрабатывать запросы к записям сеансов видеоконференций между сотрудниками. В целом подобные задачи не являются особенно сложными. Хранить записи видеофрагментов в текстовой информации способна практически любая современная система управления базами данных (СУБД), такая как Oracle, Informix или Lotus Notes.

2.1.2. Структуры компьютерных и телекоммуникационных систем и сетевых технологий

Информатизация на базе внедрения компьютерных и телекоммуникационных технологий является реакцией общества на потребность в существенном увеличении производительности труда в информационном секторе общественного производства, где сосредоточено более половины трудоспособного населения. Например, в информационной сфере США занято более 60 % трудоспособного населения, в России — около 40 %. В настоящее время в сетевых технологиях наибольшее распространение получили локальные и глобальные компьютерные сети, интегрированные сети учреждений и телекоммуникации сотовой связи с расширенным спектром услуг цифровой связи.

Компьютерная сеть — это совокупность компьютеров и различных устройств, обеспечивающих информационный обмен между компьютерами в сети без использования каких-либо промежуточных носителей информации.

Все многообразие компьютерных сетей можно классифицировать по группе признаков:

1) территориальная распространенность;
2) ведомственная принадлежность;
3) скорость передачи информации;
4) тип среды передачи.

По территориальной распространенности сети могут быть локальными, глобальными и региональными. *Локальные* — это сети, перекрывающие территорию площадью не более 10 м^2; региональные — сети, расположенные на территории города или области; глобальные — сети, расположенные на территории государства или группы государств, например всемирная сеть «Интернет».

По принадлежности различают ведомственные и государственные сети. *Ведомственные* сети принадлежат одной организации и располагаются на ее территории. *Государственные* сети — это сети, используемые в государственных структурах.

По скорости передачи информации компьютерные сети подразделяются на низко-, средне- и высокоскоростные.

По типу среды передачи компьютерные сети подразделяются на коаксиальные сети, сети на витой паре, оптоволоконные сети с передачей информации по радиоканалам, в инфракрасном диапазоне.

В классификации сетей существует два основных термина: LAN и WAN.

LAN (Local Area Network) — локальные сети, имеющие замкнутую инфраструктуру до выхода на поставщиков услуг. Термин LAN может описывать и маленькую офисную сеть, и сеть уровня большого завода, занимающего несколько сотен гектаров (около шести миль (10 км) в радиусе); используются высокоскоростные каналы. Их часто относят к интегрированным сетям учреждений и организаций.

WAN (Wide Area Network) — глобальная сеть, покрывающая большие географические регионы, включающие в себя как локальные сети, так и другие телекоммуникационные сети и устройства. Пример WAN — сеть с коммутацией пакетов (Frame Relay), через которую могут «разговаривать» между собой различные компьютерные сети.

Схема объединения компьютеров в сетях представлена на рис. 2.3.

С точки зрения ИТ связи и переработки информации наиболее интересны в настоящее время глобальные компьютерные сети.

Для подключения к сетям передачи данных, работающим по протоколу X.25, использовались модемы, реализующие под управлением с помощью специальных телекоммуникационных программ, таких как BITCOM, COMIT, PROCOM, MITEZ и т.д. Эти программы, работая под операционной системой MS-DOS, обеспечивали установление соединения с удаленным компьютером и обмен с ним информацией.

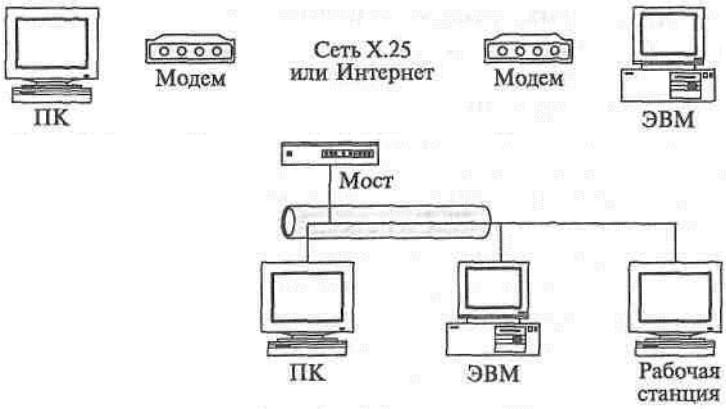


Рис. 2.3. Схема объединения компьютеров в сетях

С уходом MS-DOS их место заняло встроенное в операционные системы коммуникационное ПО. Примером могут служить средства Windows 95 или удаленный доступ (RAS) в Windows NT.

В России крупнейшими глобальными сетями считаются сеть «Спринт» (современное название Global One), сеть «Инфотел», сети «Роснет» и «Роспак», работающие по протоколу X.25, а также сети Relcom и «Интернет», работающие по протоколу TCP/IP.

В качестве сетевого оборудования применяются центры коммутации, которые для сетей X.25 часто исполняются как специализированные устройства фирм-производителей Siemens, Telenet, Alcatel, Ericsson, а для сети с TCP/IP используются маршрутизаторы фирм Cisco и Decnis.

Наибольшее распространение в настоящее время получила сеть «Интернет» — старейшая глобальная сеть. Интернет предоставляет различные способы взаимодействия удаленных компьютеров и совместного использования распределенных услуг и информационных ресурсов.

Интернет работает по протоколу TCP/IP. Основным «продуктом», который можно найти в Интернете, является информация. Эта информация собрана в файлах, которые хранятся на хост-компьютерах, и она может быть представлена в различных форматах. Формат данных зависит от того, каким сетевым сервисом вы воспользовались и какие возможности по отображению информации есть на персональном компьютере (ПК). Любой компьютер, который поддерживает протоколы TCP/IP, может выступать в качестве хост-компьютера.

Ключом к получению информации в Интернете являются адреса ресурсов. При пересылке сообщений по электронной почте используются почтовые адреса (mail addresses) и адреса хост-ком-

пьютеров (host names) для соединения с ними и получения файлов с информацией.

Интернет представляет собой глобальную компьютерную сеть, содержащую гигантский объем информации по любой тематике, доступной на коммерческой основе для всех желающих, и предоставляющую большой спектр информационных услуг. В настоящее время Интернет представляет собой объединение более 40 000 различных локальных сетей, за что она получила название «сеть сетей». Каждая локальная сеть называется узлом, или сайтом, а юридическое лицо, обеспечивающее работу сайта, — провайдером. Сайт состоит из нескольких компьютеров — серверов, каждый из которых предназначен для хранения информации определенного типа и в определенном формате. Каждый сайт и сервер на сайте имеют уникальные имена, посредствам которых они идентифицируются в Интернете.

Для подключения к Интернету пользователь должен заключить контракт на обслуживание с одним из провайдеров в его регионе.

World Wide Web (WWW) — всемирная информационная паутина. Эта система в настоящее время является наиболее популярной и динамично развивающейся. Информация в WWW состоит из страниц (документов). Страницы могут содержать графику, сопровождаться анимацией изображений и звуком, воспроизводимым непосредственно в процессе поступления информации на экран пользователя. Информация в WWW организована в форме гипертекста. Это означает, что в документе существуют специальные элементы — текст или рисунки, называемые гипертекстовыми ссылками (или просто ссылками).

Gopher-система — система, являющаяся предшественником WWW. В настоящее время она утрачивает свое значение, хотя пока и поддерживается в Интернете. Просмотр информации на Gopher-сервере организуется с помощью древовидного меню, аналогичного меню в приложениях Windows или аналогично дереву каталогов (папок) файловой системы. Меню верхнего уровня состоит из перечня крупных тем (например: «Экономика», «Культура», «Медицина» и др.). Меню следующих уровней детализируют выбранный элемент меню предыдущего уровня.

FTP (File Transfer Protocol) — система, служащая для пересылки файлов. Работа с этой системой аналогична работе с системой NC. Файлы становятся доступными для работы (чтение, исполнения) только после копирования на собственный компьютер.

Компьютер, подключенный к Интернету и использующий для связи с другими компьютерами сети специальный протокол TCP/IP, называется хостом. Для идентификации каждого хоста в сети имеются два способа адресации, всегда действующие совместно.

Первый способ адресации, называемый IP-адресом, аналогичен телефонному номеру. IP-адрес хоста назначается провай-

дером, состоит из четырех групп десятичных цифр (четырех байтов), разделенных точками, заканчивается точкой.

Аналогично телефонам каждый компьютер в Интернете должен иметь уникальный IP-адрес. Обычно пользователь свой IP-адрес не использует. Неудобство IP-адреса заключается в его безликости, отсутствии смысловой характеристики хоста и трудной запоминаемости.

Второй способ идентификации компьютеров называется системой доменных имен DNS (Domain Naming System). DNS-имена назначаются провайдером и, например, имеет вид: win.smtp.dol.ru.

Протокол Frame Relay (FR) — это протокол, который описывает интерфейс доступа к сетям быстрой коммутации пакетов. Он позволяет эффективно передавать крайне неравномерно распределенный по времени трафик и обеспечивает высокие скорости прохождения информации через сеть, малые времена задержек и рациональное использование полосы пропускания.

По сетям FR возможна передача не только собственно данных, но и оцифрованного голоса.

Интернет предоставляет следующие услуги:

1) поиск файлов с помощью системы Archie. Archie — первая поисковая система, необходимая для нахождения нужной информации в Интернете;

2) списки рассылки. Список рассылки — это средство, предоставляющее возможность вести дискуссию группе пользователей, имеющих общие интересы;

3) телеконференции. Телеконференции в Интернете предоставляют возможность вести дискуссии (при помощи сообщений) по тысячам размещенных тем.

Все остальные услуги, предоставляемые сетью «Интернет», можно условно подразделить на две группы: обмен информацией между абонентами сети и использование баз данных сети.

К числу услуг связи между абонентами относятся:

• Telnet — удаленный доступ. Дает возможность абоненту работать на любой ЭВМ сети «Интернет», как на своей собственной, т.е. запускать программы, менять режим работы и т.д.;

« FTP (File Transfer Protocol) — протокол передачи файлов. Дает возможность абоненту обмениваться двоичными и текстовыми файлами с любым компьютером сети;

• NFS (Network File System) — распределенная файловая система. Дает возможность абоненту пользоваться файловой системой удаленного компьютера, как своей собственной;

• электронная почта — обмен почтовыми сообщениями с любым абонентом сети «Интернет». Существует возможность отправки как текстовых, так и двоичных файлов. На размер почтового сообщения в сети «Интернет» накладывается следующее ограничение — размер почтового сообщения не должен превышать 64 Кбайт;

• новости — получение сетевых новостей и электронных досок объявлений сети и возможность помещения информации на доски объявлений сети. Электронные доски объявлений сети «Интернет» формируются по тематике. Пользователь может по своему выбору подписаться на любые группы новостей;

• Rsh (Remote Shell) — удаленный доступ. Аналог Telnet, но работает только в том случае, если на удаленном компьютере стоит ОС UNIX;

• Rexec (Remote Execution) — выполнение одной команды на удаленной UNIX-машине;

• Lpr — сетевая печать. Отправка файла на печать на удаленном (сетевом) принтере;

• Lpq — сетевая печать. Показывает файлы, стоящие в очереди на печать на сетевом принтере;

• Ping — проверка доступности удаленной ЭВМ по сети;

• Talk — дает возможность открытия «разговора» с пользователем удаленной ЭВМ. При этом на экране одновременно виден вводимый текст и ответ удаленного пользователя;

• Iptunnel — дает возможность доступа к серверу локальной вычислительной сети (ЛВС) NetWare, с которым нет непосредственной связи по ЛВС, а имеется лишь связь по сети «Интернет»;

• Whois — адресная книга сети «Интернет». По запросу абонент может получить информацию о принадлежности удаленного компьютера, о пользователях;

• Finger — получение информации о пользователях удаленного компьютера.

Кроме перечисленных услуг сеть «Интернет» предоставляет также следующие специфические услуги:

• Webster — сетевая версия толкового словаря английского языка;

• факс-сервис — дает возможность пользователю отправлять сообщения по факсимильной связи, пользуясь факс-сервером сети;

• электронный переводчик — производит перевод присланного на него текста с одного языка на другой. Обращение к электронным переводчикам происходит посредством электронной почты;

• шлюзы — дают возможность абоненту отправлять сообщения в сети, не работающие с протоколами TCP\IP (Fido, Goldnet, AT50).

К системам автоматизированного поиска информации в сети «Интернет» относятся следующие системы:

• Gopher — наиболее широко распространенное средство поиска информации в сети «Интернет», позволяющее находить информацию по ключевым словам и фразам. Работа с системой Gopher напоминает просмотр оглавления; при этом пользователю предлагается пройти сквозь ряд вложенных меню и выбрать

нужную тему. В Интернете в настоящее время свыше 2 000 Gopher-систем, часть из которых является узкоспециализированной, а часть содержит более разностороннюю информацию. В случае возникших затруднений можно воспользоваться службой VERONICA. VERONICA осуществляет поиск более чем в 500 системах Gopher, освобождая пользователя от необходимости просматривать их вручную;

• WAIS — еще более мощное средство получения информации, чем Gopher, поскольку оно осуществляет поиск ключевых слов во всех текстах документов. Запросы посылаются в WAIS на упрощенном английском языке. Это значительно легче, чем формулировать их на языке алгебры логики, и это делает WAIS более привлекательной для пользователей-непрофессионалов. В сети «Интернет» существует более 300 WAIS-библиотек. Но поскольку информация представляется преимущественно сотрудниками академических организаций на добровольных началах, большая часть материалов относится к области исследований и компьютерных наук;

. WWW — система для работы с гипертекстом. Потенциально она является наиболее мощным средством поиска. Гипертекст соединяет различные документы на основе заранее заданного набора слов. Например, когда в тексте встречается новое слово или понятие, система, работающая с гипертекстом, дает возможность перейти к другому документу, в котором это слово или понятие рассматривается более подробно. WWW часто используется в качестве интерфейса к базам данных WAIS, но отсутствие гипертекстовых связей ограничивает возможности WWW до простого просмотра, как у Gopher. WWW — это относительно новая и динамично развивающаяся система. Установлены несколько демонстрационных серверов, в том числе Vatican Exibit в библиотеке Конгресса США и мультфильм о погоде «Витки спутника» в Мичиганском государственном университете. В качестве демонстрационных также работают серверы into.funet.fi (Финляндия); into.cem.ch (Швейцария) и eies2.njit.edu (США).

Практически все услуги сети построены по принципу клиент-сервер.

Все ПО сети также можно подразделить на клиентское и серверное. При этом ПО сервера занимается предоставлением сетевых услуг, а клиентское ПО обеспечивает передачу запросов серверу и получение ответов на него.

В эру глобального информационного общества соответствующего коренного улучшения телекоммуникационного обслуживания населения можно достигнуть путем предоставления широкого пакета новых услуг сетей сотовой подвижной связи нового, третьего по счету, поколения информационных технологий связи, называемого 3G (или просто Third Generation). К этому набо-

ру услуг относится не только цифровая телефонная связь, но и высокоскоростной доступ в Интернете, и даже передача видеоизображения (доступная скорость передачи информации для высокоподвижных абонентов — до 384 кбит/с; для фиксированной связи в пределах микросот — до 2 Мбит/с.

Коммерческие сети CDMA One с 1996 г. стали быстро развиваться. В настоящее время сети CDMA One имеются в Северной и Южной Америке, Австралии, Юго-Восточной Азии, Африке и на Ближнем Востоке.

Существует мнение специалистов, что сети CDMA One будут обгонять по темпам роста самые массовые в настоящее время сети GSM. Скоро весь мир перейдет на широкополосные сети CDMA (CDMA 2000, W-CDMA и др.). При этом доля сетей других стандартов в рынке сотовой связи будет несущественна.

CDMA (Code Division Multiple Access) — система множественного доступа с кодовым разделением — стала самой многообещающей системой, появившейся на мировом рынке. Десятилетия назад эта технология использовалась в военной связи (США), а в настоящее время известна всем как глобальный цифровой стандарт для коммерческих систем коммуникаций.

Первая российская сеть сотовой связи на основе CDMA была развернута АО «Связь информ» в Челябинске в конце 1996 г.

Сеть CDMA, где базовые станции работают на одних и тех же радиоканалах, не похожа на сети других технологий и функционирует как единый организм. Три основных параметра сотовой сети (покрытие, качество и емкость) в системе CDMA взаимосвязаны и влияют друг на друга. Таким образом, операторы имеют возможность обеспечения оптимальным обслуживанием заданной территории, варьируя параметры сети.

Как окончательно подтверждено Международным советом электросвязи (МСЭ), в наиболее массовых североамериканских и западно-европейских подвижных системах связи 3G с использованием радиоинтерфейсов, называемых CDMA 2000 и W-CDMA (работающих в радиодиапазоне 1,9...2,2 ГГц), будет широко использована технология мультидоступа с кодовым разделением каналов МДКР (или CDMA).

К предоставлению услуг по высокоскоростной передаче данных всем операторам предполагается идти двумя путями: революционным (путем развертывания новой телекоммуникационной инфраструктуры) или эволюционным (путем усовершенствования уже существующих цифровых сотовых сетей 2G в 2G+ с помощью набора специальных технологий: протокол WAP, стандарты HSCSD, GPRS, технология EDGE и др.). Поскольку развертывание совершенно новой сетевой инфраструктуры (3G) дорого и требует наличия свободного диапазона радиочастот (а это напрямую связано с абонентской емкостью и стоимостью сети),

МСЭ решил расширить возможности национальных операторов сотовой связи.

Новой сотовой информационной технологией связи, основанной на стандарте CDMA, является применение цифровой сотовой сети «Сонет», дающей возможность предоставления полного перечня современных услуг связи:

1) бесплатное подключение, нулевая стоимость минуты разговора при внесении только абонентной платы;

2) в 8— 10 раз большая емкость сети по сравнению с традиционными аналоговыми сотовыми сетями (снимается проблема перегрузки сети);

3) высококачественное воспроизведение речи, сопоставимое с качеством проводных каналов, путем преобразования речевых сигналов в цифровую форму и устранение фоновых сигналов — «идеальная слышимость»;

4) высокая степень конфиденциальности благодаря встроенному алгоритму кодирования — абсолютная защита от несанкционированного доступа и прослушивания;

5) высокое качество передачи речи и данных с минимальной средней выходной мощностью — наименьшее воздействие на организм человека;

6) широкий спектр дополнительных услуг при использовании цифрового контрольного канала — передача данных до 14,4 кбит/с;

7) передача не только голоса, но и любой другой информации при высокой помехозащищенности — передача факса и данных.

В настоящее время производство оборудования цифровых сотовых систем связи CDMA освоено различными производителями: Ericsson, Motorola, NEC, Nortel, Samsung и др.

Абонентское оборудование выпускается еще большим количеством компаний, к списку которых кроме перечисленных ранее необходимо добавить такие компании, как LG, Nokia, Qualcomm, Sony и т.д.

2.2. Техническое обеспечение ИС и технологий управления

2.2.1. Общие положения построения ИС и технологий управления

Производственные и хозяйственные предприятия, организации, фирмы, корпорации, банки представляют собой сложные системы. Под *системой* понимается совокупность связанных между собой и с внешней средой элементов, функционирование которых направлено на реализацию конкретной цели или полезного результата. В соответствии с этим определением практически каж-

дый социально-экономический объект (СЭО) или его часть можно рассматривать как систему, стремящуюся в своем функционировании к достижению поставленной цели.

В условиях функционирования любая область деятельности организации может рассматриваться как сложная система, реализующая комплекс мероприятий по удовлетворению спроса потребителей на продукцию и услуги посредством купли-продажи или обмена.

Важнейшая функция — управление, без которой немыслима целенаправленная деятельность любой социально-экономической, организационно-производственной системы (предприятия, фирмы, организации).

Управление связано с обменом информацией между компонентами системы, а также с окружающей средой. Процесс управления предполагает получение сведений о состоянии системы в каждый момент времени, о достижении (или не достижении) заданной цели, с тем чтобы воздействовать на систему и обеспечить выполнение управленческих решений. Особенно это важно в технологиях социального менеджмента, которые в настоящее время наиболее эффективны при управлении СЭО. Таким образом, система управления СЭО и соответствующая информационная система может быть названа социально-экономической информационной системой управления.

Социально-экономическая информационная система управления (СЭИСУ) — совокупность внутренних и внешних потоков прямой и обратной информационной связи СЭО, а также методов, средств, специалистов, участвующих в процессе обработки информации и выработке управленческих решений.

Управление как совокупность целенаправленных действий реализуется в соответствии с целью функционирования СЭО и принципами принятия решений в конкретных ситуациях.

Управляющие воздействия формируются на основе накопленной и функционирующей в системе управления информации, а также сведений, поступающих по каналам прямой и обратной связи из внешней среды.

Поскольку информация фиксируется и передается на материальных носителях, необходимы действия человека и работа технических средств по восприятию, сбору информации, ее записи, передаче, преобразованию, обработке, хранению, поиску и выдаче. Эти действия обеспечивают нормальное протекание информационного процесса и входят в технологию управления.

Применение технических средств для получения информации в ходе наблюдения за деятельностью объекта, сбора данных, их регистрации, передачи по каналам связи потребовало дальнейшего углубленного изучения информационных процессов.

Для выработки в сложных экономических системах эффективных управляющих воздействий необходимо наряду с созданием соответствующих алгоритмов управления переработать значительные объемы разнообразной информации. Именно этим вызвана необходимость разработки автоматизированных информационных систем (АИС) управления.

Автоматизированные информационные системы различаются по типу основной деятельности объекта (социально-экономические, технологические, административные и т.д.), по сферам, функциональной направленности (финансовые, налоговые, страховые, банковские, бухгалтерские, маркетинговые и т.д.), по методам решения задач (экспертные, имитационные, оптимизационные, информационно-соответствующие, телекоммуникационные) и т.д.

С позиции технологии и выполняемых функций типовая АИС СЭО может состоять из нескольких элементов (рис. 2.4).

Элементы образуют автоматизированную информационную технологию обработки данных (АИТ ОД) — системно организованную для решения задач управления совокупность методов и средств реализации операций сбора, регистрации, передачи, накопления, поиска, представления, обработки и защиты процессов переработки информации на базе применения развитого программного обеспечения, используемых средств вычислительной техники и связи.

Содержание элементов АИТ ОД в АИС СЭО позволяет выявить подсистемы, обеспечивающие технологию функционирования системы.

Технологическое обеспечение АИТ ОД состоит из подсистем автоматизации информационного обслуживания решений задач с применением ЭВМ и других технических средств управления в установленных режимах работы.

По составу технологическое обеспечение АИТ ОД одинаково для различных систем, что позволяет реализовать принцип их совместимости в процессе функционирования. Обязательными элементами для АИТ ОД является правовое, организационное, информационное, лингвистическое, программное, математическое, техническое и эргономическое обеспечение.

Правовое обеспечение представляет собой совокупность правовых норм, регламентирующих правоотношения при создании и внедрении АИС СЭО.

Правовое обеспечение на этапе функционирования АИТ ОД включает в себя:

- определение их статуса в конкретных отраслях государственного управления;
- правовое положение о компетенции звеньев АИС и СЭО и организации их деятельности;

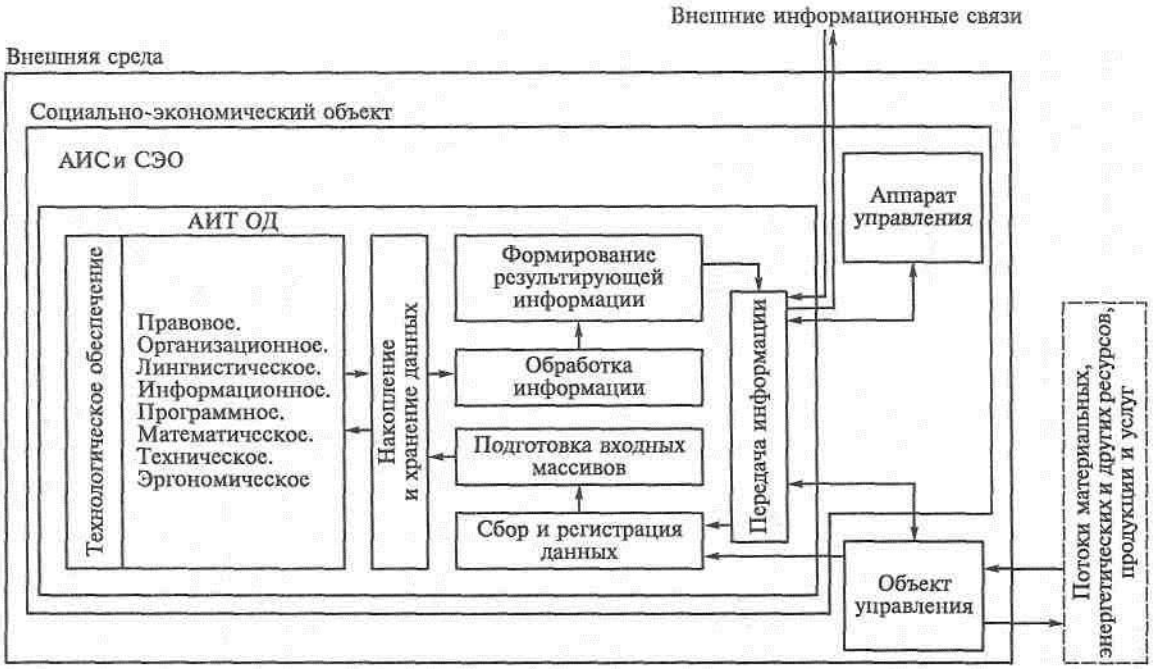


Рис. 2.4. Типовая структура АИС и ТСЭО

• права, обязанности и ответственность персонала, порядок создания и использования информации в АИТ ОД, процедуры ее регистрации, сбора, хранения, передачи и обработки;

• порядок получения и использования электронно-вычислительной техники и других технических средств;

• порядок создания и использования математического и программного обеспечения.

Организационное обеспечение представляет собой комплекс методического и документационного обеспечения, регламентирующий деятельность персонала АИТ в условиях функционирования АИС.

Информационное обеспечение представляет собой совокупность проектных решений по объемам, размещению, формам организации информации, циркулирующей в АИТ ОД. Оно включает в себя совокупность показателей, справочных данных, классификаторов и кодификаторов информации, унифицированные системы документации, специально организованные для автоматического обслуживания, массивы информации на соответствующих носителях, а также персонал, обеспечивающий надежность хранения, своевременность и качество технологии обработки информации.

Лингвистическое обеспечение объединяет совокупность языковых средств для формализации естественного языка, построения и сочетания информационных единиц в ходе общения персонала со средствами вычислительной техники. С помощью лингвистического обеспечения осуществляется общение человека с машиной. Оно включает в себя информационные языки для описания структурных единиц информационной базы АИТ ОД (документов, показателей, реквизитов и т.д.); языки управления и манипулирования данными информационной базы, языковые средства информационно-поисковых систем; языковые средства автоматизации проектирования, диалоговые языки специального назначения и другие языки, а также систему терминов и определений, используемых в процессе разработки и функционирования автоматизированных систем управления.

Программное обеспечение включает в себя совокупность программ, реализующих функции и задачи АИС СЭО и обеспечивающих устойчивую работу комплексов технических средств. В его состав входят общесистемные и специальные программы, а также инструктивно-методические материалы по применению средств программного обеспечения и персонал, занимающийся его разработкой и сопровождением на весь период жизненного цикла АИС.

Математическое обеспечение — это совокупность математических методов, моделей и алгоритмов обработки информации, используемых при решении функциональных задач и в процессе ав-

томатизации проектировочных работ в АИС СЭО. Математическое обеспечение включает в себя средства моделирования процессов управления, методы и средства решения типовых задач управления, методы оптимизации управленческих процессов и принятия решений (методы многокритериальной оптимизации, математического программирования, математической статистики, теории массового обслуживания и т.д.).

Техническое обеспечение представляет собой комплекс технических средств сбора, регистрации, передачи, обработки, отображения, размножения информации, оргтехники, обеспечивающих работу АИС и АИТ. Центральное место в комплексе технических средств принадлежит персональным электронно-вычислительным машинам (ПЭВМ). Структурными элементами технического обеспечения являются также методические и руководящие материалы, техническая документация и обслуживающий персонал.

Эргономическое обеспечение — совокупность методов и средств, используемых на разных этапах разработки и функционирования АИС. Оно предназначено для создания оптимальных условий высокоэффективной деятельности человека в АИС. В состав эргономического оснащения АИТ ОД входит комплекс различной документации, содержащей эргономические требования к рабочим местам, информационным моделям, условиям деятельности персонала.

Являясь человекомашинной системой, в рамках которой реализуется информационная модель, формализующая процессы обработки данных в условиях новой технологии, АИТ ОД замыкает через себя прямые и обратные информационные связи между объектом управления (ОУ) и аппаратом управления (АУ), а также вводит в систему потоки внешних информационных связей.

Функции АИТ ОД определяют ее структуру, которая включает в себя следующие процедуры: сбор и регистрация данных; подготовка информационных массивов; накопление и хранение данных; обработка информации с помощью технологического обеспечения; формирование результирующей информации; передача данных от источников возникновения к месту обработки, а результатов — к потребителям информации для принятия управленческих решений.

Сбор и регистрация информации для различных СЭО значительно отличаются. Наиболее сложной эта процедура является в автоматизированных управленческих процессах промышленных предприятий, фирм, где производятся сбор и регистрация первичной учетной информации, отражающие в основном производственно-хозяйственную деятельность объекта.

В процессе сбора фактической информации производятся измерение, подсчет, взвешивание материальных объектов, подсчет

денежных купюр, получение временных и количественных характеристик работы отдельных исполнителей.

Сбор и регистрация данных производятся с помощью машинного кодирования. Процедура машинного представления (записи) информации осуществляется на машинных носителях с помощью кодов, принятых в ПЭВМ.

Обработка экономической информации в АИТ ОД производится централизованно и децентрализованно. В местах возникновения первичной информации организуются автоматизированные рабочие места специалистов той или иной управленческой службы (отдела материально-технического снабжения и сбыта, отдела главного технолога, конструкторского отдела, бухгалтерии и т.д.).

В ходе решения задач на ЭВМ в соответствии с машинной программой формируются результатные сводки, которые печатаются машиной или отображаются на экране. Печать сводок может сопровождаться процедурой тиражирования, если документ с результатной информацией необходимо предоставить нескольким пользователям.

Хранение и накопление экономической информации вызвано многократным ее использованием, применением условно-постоянной, справочной и других видов информации, необходимостью комплектации первичных данных до их обработки.

С хранением и накоплением непосредственно связан поиск данных, т.е. выборка нужных данных из хранимой информации, включая поиск информации, подлежащей корректировке либо замене. Процедура поиска выполняется автоматически на основе составленного пользователем или ПЭВМ запроса на нужную информацию.

Передача информации осуществляется различными способами: с помощью курьера, пересылкой по почте, доставкой транспортными средствами, дистанционной передачей по каналам связи (электронная почта, Интернет, мобильные средства связи и т.д.).

Принятие решения в автоматизированной системе организационного управления, как правило, осуществляется специалистом с применением или без применения технических средств, но в последнем случае — на основе тщательного анализа результатной информации, полученной на ПЭВМ. Задача принятия решений осложняется тем, что специалисту приходится выбирать из множества допустимых решений наиболее приемлемое, сводящее к минимуму потери ресурсов (временных, трудовых, материальных и т.д.).

Автоматизированная информационная система СЭО реализует решение функциональных задач управления, совокупность которых составляет так называемую функциональную часть деятельности СЭО как системы. Состав, порядок и принципы взаимо-

действия функциональных подсистем, задач и их комплексов устанавливаются с учетом достижения цели, стоящей перед СЭО. Основными факторами выделения самостоятельных подсистем (декомпозиции) комплексов задач являются:

- относительная самостоятельность каждой из них;
- наличие соответствующего набора функций и функциональных задач с четко выраженной локальной целью;
- минимизация числа включенных в подсистему элементов;
- наличие одного или нескольких локальных критериев, способствующих оптимизации режима работы подсистемы и согласующихся с глобальным критерием оптимизации действия АИС СЭО и системы в целом.

2.2.2. Структуры информационных систем и технологий в сферах деятельности предприятий

Многообразие деятельности современных предприятий и фирм для информационных систем и технологий ставит на повестку дня применение комплексного подхода к вопросам формирования их инфраструктур и содержания по объектово-процессорному назначению.

Опираясь на методологию информатизации и структурирования ИС и учитывая, что в данной книге невозможно привести и описать множество структурных схем и технологий в различных видах деятельности для предприятий, целесообразно рассмотреть некоторые примеры построения информационных систем и технологий с точки зрения формализации задач администрирования.

В структурах информационных систем и технологий управления можно условно выделить три категории управленческой деятельности:

1) стратегическое планирование — процесс принятия решений по целям организации, изменению этих целей и использованию ресурсов для достижения этих целей, а также по стратегиям, обусловливающим получение, использование и размещение этих ресурсов;

2) управленческий контроль — процесс, посредством которого обеспечивается получение ресурсов и их эффективное использование для достижения общих целей организации;

3) оперативное управление и контроль — процессы обеспечения эффективного и квалифицированного выполнения конкретных задач.

Эти категории деятельности примерно соответствуют обязанностям управляющих высшего, среднего и низового звена, а информационная управляющая система (ИУС) должна представлять

информацию, соответствующую различным требованиям, предъявляемым к каждой из категорий.

Информация для управленческого контроля необходима управляющим и высшего, и среднего звена. Естественно, она должна поступать как из внутренних, так и из внешних источников.

Информация для целей оперативного управления, которая касается повседневной деятельности, должна быть очень точной, узкой и самой конкретной. Она должна поступать почти исключительно из внутренних источников.

Кроме того, руководителям нужна специфическая информация, относящаяся к области их конкретной профессиональной деятельности. Так, управляющему по сбыту требуется информация о торговых сделках, вкусах потребителя, конкурентоспособности новых товаров и т.д. Детальная информация о технических условиях на новое изделие, которая принципиально важна для управляющего производством, не является существенной для принятия решений, касающихся сбыта. Действительно, если ИУС будет регулярно выдавать такую информацию управляющему по сбыту, то это будет мешать ему в работе и отнимать время.

Содержание и реализация управленческой информации в ИУС по категориям и уровням управления приведены в табл. 2.1.

На работу ИУС оказывают влияние изменения внутренних и внешних обстоятельств. Любое изменение в структуре организации обычно означает, что какую-то конкретную информацию нужно будет направлять по другому адресу.

Руководящие работники не могут предвидеть, какая именно информация им может понадобиться. Изменения банковского процента, возможное слияние компаний, объявление конкурентов о выпуске нового изделия может заставить управляющего разыскивать соответствующие данные и собирать «по крохам» необходимую ему для принятия решения информацию. Даже рутинный анализ оперативных данных может породить самые неожиданные вопросы.

Внешняя среда представляет собой метасистему, состоящую из множества организационных систем. Одной из таких организационных систем является предприятие. Системы, осуществляющие в отношении предприятия явное или неявное управление, являются управляющими.

В метасистеме существует глобальное информационное поле России (рис. 2.5), создаваемое продуктами деятельности физических и юридических субъектов, а также результатами отражения одних материальных объектов и явлений в других, которые можно рассматривать как ведомственные информационные накопители (ВИН), независимые информационные накопители (НИН) и точечные источники информации (ТИИ).

Таблица 2.1

Содержание и реализация управленческой информации в ИУС по категориям и уровням управления

Уровень управления	Категории управленческой деятельности	Содержание информации в ИУС	Реализация информации в ИУС
Высшее звено управления (стратегическое планирование)	Увеличение производительности, рост, накопление и использование ресурсов; выживание всей организации	Данные о среде и тенденции, прогнозы, сводные отчеты об операциях, уведомления об исключительных проблемах	Установление организационных целей, политики, ограничений, принятие решений, касающихся стратегических планов и управления всей организацией
Среднее звено управления (управленческий контроль)	Размещение ресурсов в соответствии с распределенными заданиями, установление оперативных планов, контроль операций	Сводки о результатах операций и уведомления об исключительных ситуациях, относящихся к делу действиях и решениях других руководителей среднего звена	Установление оперативных планов и политики, контроль процедур, составление уведомлений об исключительных ситуациях, составление оперативных сводок по распределению ресурсов, о действиях и решениях для других управляющих среднего звена
Нижнее звено управления (оперативное управление и контроль)	Производство товаров или услуг в пределах бюджетов, установление потребности в ресурсах, перевозке и хранении материалов	Свободные отчеты о взаимодействиях, подробные отчеты по проблемам, оперативные планы и политики, процедуры контроля, действия и решения связанных между собой управляющих	Составление уведомлений об исключительных ситуациях и сообщений о состоянии работы, определение потребности в ресурсах, составление рабочих календарных планов

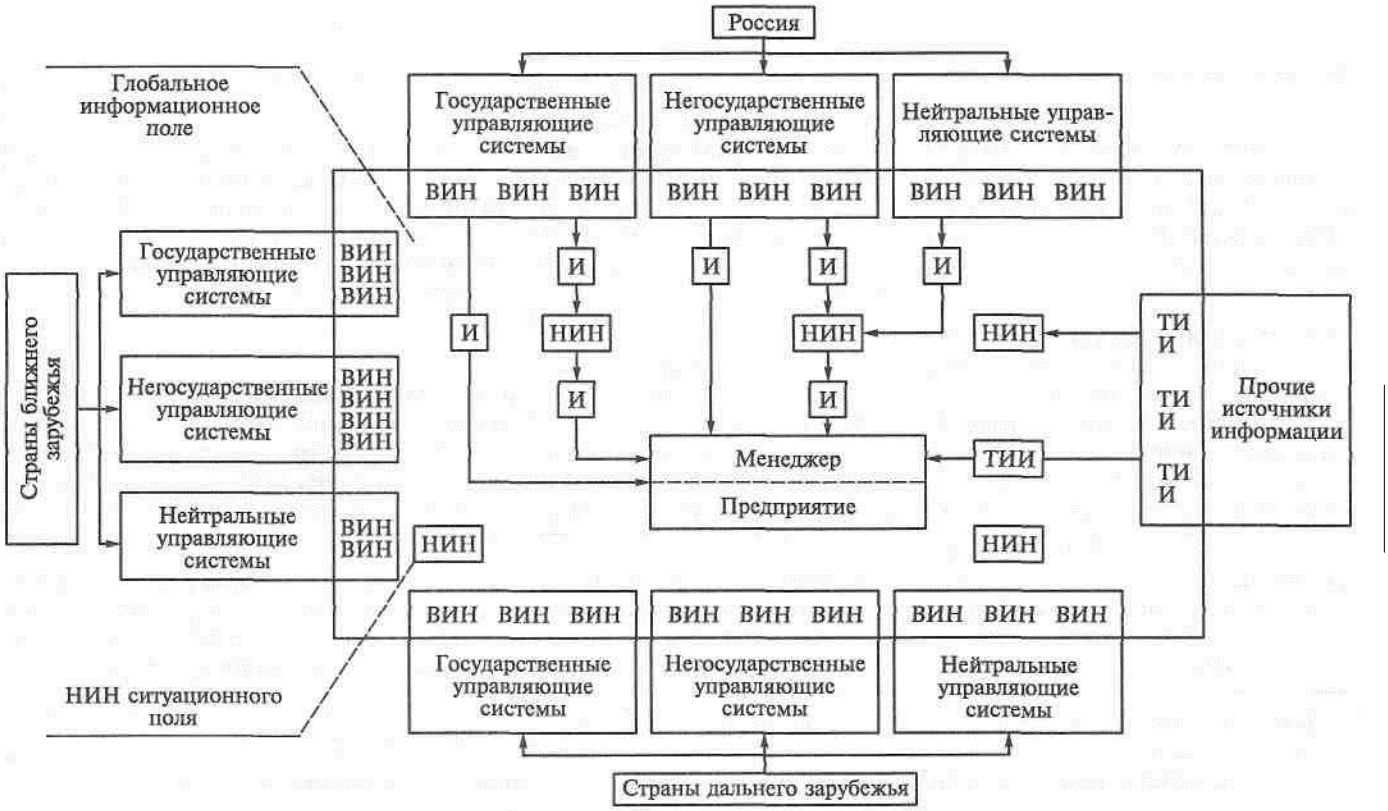


Рис. 2.5. Структура глобального информационного поля России в метасистеме (И — информация)

В глобальном информационном поле можно выделить ситуативное информационное поле, точечные источники информации которого определяют регламентированное поведение предприятия.

Управляющие системы изготавливают и выпускают в информационное поле точечные источники информации, разные по содержанию (законы, распоряжения, рекомендации, учебники и т.д.), форме (книги, статьи в газетах и журналах, письма, файлы, базы данных и т.д.), на различных материальных носителях (бумага, магнитный диск, лента и т.д.).

Точечные источники информации, предназначенные для управляющего воздействия на поведение предприятия, называются информационными продуктами (ИП), а не предназначенные — информационными изделиями (ИИ). Как правило, управляющая система изготавливает конкретный ИП, предназначенный для множества предприятий, в единственном экземпляре. Другие системы, не имеющие статуса управляющих, изготавливают информационные копии этих ИП, т.е. такие информационные продукты, которые должны восприниматься предприятием как ИП, изготовленные непосредственно управляющими системами.

Глобальное информационное поле наполняется множеством копий управляющих ИП, которые могут быть относительно равномерно распределены в пространстве или скапливаться в отдельных точках этого пространства.

Собранные в отдельных местах ИП образуют в информационном поле информационные накопители в виде библиотек, архивов, отделов нормативной или иной документации, которые могут быть внутри или вне создающих их управляющих систем (они соответственно называются ВИН и НИН).

В метасистеме можно выделить государственные, негосударственные и нейтральные управляющие системы. Последние посылают в глобальное информационное поле свои информационные изделия, которые по внешнему виду, структуре и технологии изготовления не отличаются от ИП.

В глобальном информационном поле происходят постоянные движения (между источниками, накопителями и потребителями), дубликационное размножение, размножение с искажением, уничтожение информационных продуктов и изделий. Здесь большое значение имеет функциональная деятельность системного администрирования. Фактически мониторинг этих процессов и является его задачами.

На рис. 2.5 физическая граница предприятия как обособленной системы является также границей, отделяющей его от внешней части глобального информационного поля, так как материальные ИП находятся в информационных накопителях, которые сами являются оргсистемами.

Рассмотрим некоторые примеры информационного и технического обеспечения управления в деятельности предприятия.

2.2.3. Информационная система и технология управления финансами предприятия

Постоянно растущий интерес к современным технологиям управления предприятием коснулся и сферы управления финансами. Основное внимание концентрируется, как правило, в следующих направлениях:

- инвестиционное планирование в рамках проектов модернизации предприятия, открытия новых направлений деятельности, когда прогнозируются объемы необходимых финансовых вложений, сроки возврата инвестиций, общая экономическая эффективность проекта;
- среднесрочное и текущее финансовое планирование (бюджетирование) в рамках года, квартала, месяца: формирование плана прибылей и убытков, бюджета движения денежных средств и прогнозного баланса предприятия; контроль их выполнения в течение периода и анализ исполнения по его завершении;
- тесно связанное с бюджетированием управление задолженностью предприятия: планирование погашения задолженности бюджетам различных уровней и внебюджетным фондам; установление и контроль лимитов возникновения и погашения дебиторской и кредиторской задолженностей;
- управление платежами: прогнозирование графика поступлений денежных средств, установление регламента прохождения заявок на платежи, составление платежного календаря и оперативное управление текущими платежами.

Для полноценной поддержки функций управления финансами информационная система и технологии предприятия должны удовлетворять следующие требования:

- централизованное хранение всей необходимой информации в единой базе данных и поддержание ее в актуальном состоянии в режиме, близком к реальному времени, так как без полных и достоверных данных о текущем состоянии невозможно рассчитать оптимальные плановые показатели;
- наличие отдельного, независимого от бухгалтерского, оперативного учета возникновений и погашений обязательств предприятия: отгрузок продукции, поставок материалов, платежей и поступлений денежных средств; бухгалтерский учет является «посмертным» по объективным причинам, а для целей управления требуются оперативные данные, пусть еще и не подтвержденные документами;
- комплексное обеспечение всех основных потребностей финансовых служб предприятия, так как реализация только бюдже-

тирования или только календаря платежей разрывает взаимосвязанные процессы и не дает воспользоваться преимуществами интегрированных решений;

• отсутствие жесткой регламентации форм планирования и порядка их формирования, возможность реализации в системе как методических рекомендаций консультантов, так и особенностей учета и планирования конкретного предприятия.

Большинство представленных сейчас на рынке корпоративных информационных систем и технологий имеют в своем составе модули или отдельные функции финансового планирования и управления и в основном удовлетворяют перечисленным требованиям. Так, в системе управления «Парус», ориентированной на средние и крупные предприятия, в приложении «Управление финансами» реализованы функции бюджетирования, управления задолженностью и календарного планирования платежей. Благодаря общей базе данных на СУБД Oracle в «Управлении финансами» доступны данные приложений управления логистикой, производством, бухгалтерским учетом; в свою очередь, результаты финансового планирования используются в других приложениях. Наличие общего оперативного учета движения материальных ценностей и денежных средств обеспечивает единство и согласованность действий коммерческой и финансовой служб, независимость их от регламента отработки документов бухгалтерией.

Структуру управления финансами предприятия рассмотрим на примере подсистемы Системы планирования ресурсов предприятия (ERP-система). В общем случае управление финансами можно представить в виде четырех функциональных уровней:

1) финансовое планирование деятельности предприятия (финансовый план);

2) финансовый контроль деятельности (бюджеты и бюджетный контроль);

3) контроль за финансовыми процессами (контроль за процессами учета);

4) реализация финансовых процессов (ведение финансовых операций — бухгалтерский учет).

Два верхних уровня (1 и 2) в большей степени зависят от типа деятельности предприятия, так как на этих уровнях определяются особенности организации управленческого учета предприятия.

Два нижних уровня (3 и 4) представляют собой процессы, в достаточной степени независимые от типа деятельности. (В качестве примера можно привести стандартные операции по регистрации входящих и исходящих счетов, банковских выписок, операций с основными средствами и т.д.).

В финансовых подсистемах ERP-систем предполагается наличие двух способов составления финансового плана:

• «снизу вверх»;

•«сверху вниз».

При использовании способа «снизу вверх» соответствующие части финансового плана формируются в низовых подразделениях, после чего система осуществляет их агрегирование.

При использовании способа «сверху вниз» основные показатели смет определяются на верхнем уровне предприятия, после чего происходит их детализация на уровнях.

Все финансовые планы и бюджеты базируются на основе счетов главной книги, заранее описанной в системе управленческой структуры предприятия (центров финансовой ответственности, единиц затрат и т.д.), определяющей интегральный показатель сметы за выбранный период в соответствии со структурой объектов аналитического (управленческого) учета.

Управление движением денежных средств (ДДС) как основная задача казначейства или финансового управляющего реализуется в системе для планирования и контроля входящих и исходящих денежных потоков и формализации процедур расчетов.

Формирование прогноза ДДС системой обеспечивается на основе различных документов (счета-фактуры закупок, счета-фактуры продаж, заказы на закупку, заказы на продажу, заказы по проектам, поручения и т.д.). Формализация и упорядочение процедур расчетов организовывается путем определения в системе стандартных способов и операций по расчетам.

Контроль за процессами учета и учет операций (по участкам бухгалтерского учета) на счетах главной книги предполагает, как правило, две операции: «не разнесенная операция (документ)» и «разнесенная операция (документ)».

Стандартными модулями подсистемы управления финансами, реализующими функции перечисленных ранее четырех уровней, объединенных в финансовый и управленческий учет, являются:

Основное назначение	*— Финансовый учет*
General Ledger	— Главная книга
Accounts Receivable	— Счета к получению
Accounts Payable	— Счета к оплате
Multi Currency	— Многовалютность
Fixed Assets	— Основные средства
Consolidation	— Консолидация

Основное назначение	*— Управленческий учет*
Financial Budget System	— Система финансовых планов и бюджетов
Cash Management	— Управление денежных средств
Cost Allocation	— Распределение затрат
Cost Accounting	— Учет затрат
Cost Price Calculation	— Калькуляция себестоимости
Financial Statements	— Финансовые отчеты

В настоящее время в условиях наметившегося экономического подъема предприятия все шире используют современные ИТ, которые не только позволяют решать многочисленные задачи внутреннего управления, но и предоставляют возможность эффективно взаимодействовать с окружающей бизнес-средой. Одной из таких универсальных ИТ, созданной с применением новых интернет-технологий, стала разработанная в Судостроительном банке система удаленного управления расчетными счетами предприятий Sbank.ru. В ней реализована схема ускоренного проведения платежей.

Весь документооборот между предприятием и банком ведется в электронном виде с передачей документов по каналам Интернета в режиме реального времени. При этом системой предусмотрено как ведение рублевых счетов предприятий и совершение по ним операций, так и ряд других услуг, связанных с покупкой и продажей валюты, ее переводом и т.д.

Главной особенностью программного решения является возможность сквозной передачи расчетных документов, подготовленных бухгалтером в учетной системе предприятия, по каналам Интернета непосредственно в автоматизированную систему банка. Разработанный специалистами Судостроительного банка универсальный интерфейс, основанный на международном стандарте Open Financial Exchange, позволяет эффективно обмениваться с любыми учетными системами.

Для взаимодействия с наиболее известными системами автоматизации финансово-хозяйственной деятельности подготовлены типовые настройки конфигурации.

При использовании Интернета в качестве среды для передачи расчетных документов у бухгалтера отпадает необходимость делать визиты в офис банка. Передачу в режиме реального времени удаленных распоряжений на совершение операций выполняет система, а планирование графика отправки документов — бухгалтер предприятия в соответствии со своим индивидуальным рабочим планом.

Для поступающих в банк данных через систему электронных расчетных документов, в отличие от бумажных, не требуется предварительная их обработка перед применением в автоматизированной банковской системе, что позволяет банку предоставлять предприятиям режим продленного операционного дня.

В системе Sbank.ru реализована многоуровневая система комплексной информационной безопасности от несанкционированного доступа к передаваемым документам и возможной их фальсификации с применением прогрессивных международных методов криптографической защиты. Вопросы обеспечения ИБ управления рассмотрены в гл. 4.

Интерактивное взаимодействие между банком и предприятием через Интернет обусловило пересмотр традиционной модели деловых отношений.

Новая форма расчетного обслуживания, поддерживаемая технологиями, процессами и структурой, позволяет предоставлять предприятиям, подключенным к системе Sbank.ru, качественный банковский сервис независимо от их территориального расположения.

Другой вариант построения структуры информационной системы и технологий управления финансами может быть представлен на примере версии 5.8 «Галактика-Финансы». В этой версии задачи финансового управления решаются с помощью модулей «Управление бюджетом», «Платежный календарь», «Финансовый анализ» (рис. 2.6). Модули связаны между собой и полностью интегрированы в систему «Галактика». Основное преимущество системного подхода заключается в том, что анализ и принятие управленческих решений базируется на учетном слое данных. Работа непосредственно с оперативными данными позволяет обеспечить контроль над ситуацией и принятие решений в реальном времени.

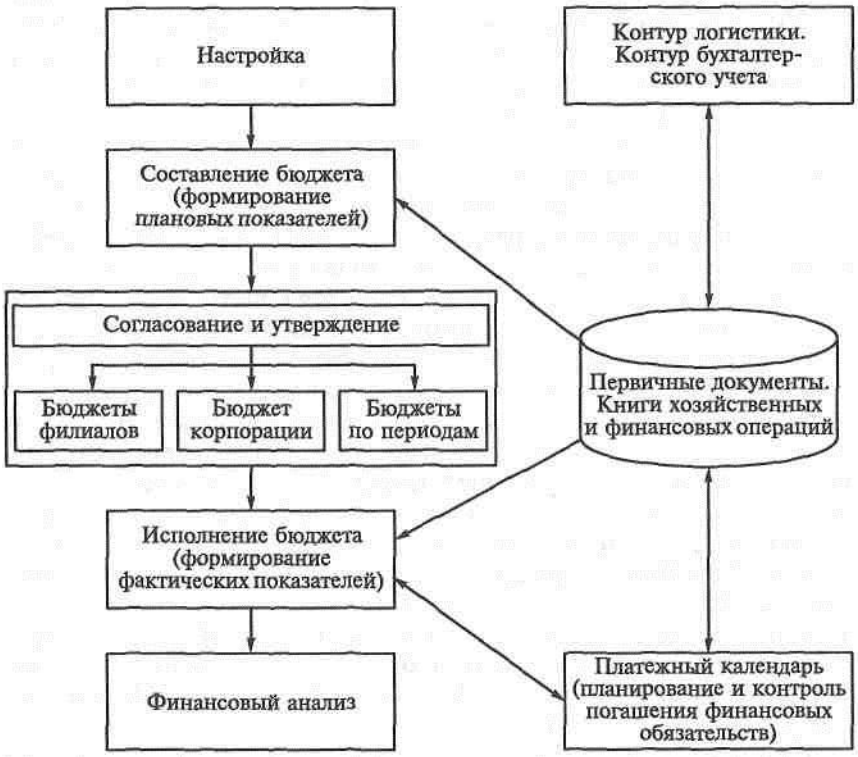


Рис. 2.6. Информационные потоки управления финансами версии 5.8 «Галактика-финансы»

Все модули финансового блока имеют развитую настройку, что позволяет учесть специфику хозяйственной деятельности конкретного предприятия и максимально точно отслеживать и анализировать бизнес-процессы.

Центральным процессом «Финансового контура» является «Управление бюджетом». Это универсальный инструмент для бюджетирования благодаря возможностям формирования произвольной аналитики и привязки иерархии аналитик к статьям бюджета.

Модуль «Платежный календарь» позволяет осуществлять оперативный финансовый менеджмент по принципу скользящего планирования путем циклического выполнения анализа и балансировки. Балансировка заключается в ежедневном пересчете платежного календаря на основании фактических данных о движении платежных средств и принятии управленческих решений, которые позволяют согласовывать поступление и расход платежных средств. Такими решениями могут быть, например, замена или конвертация платежного средства, использование заемных средств, договоренность с контрагентом о переносе срока платежа и др.

Новая редакция модуля «Финансовый анализ», в отличие от существующей в предыдущих версиях системы «Галактика», а также от аналогичных продуктов других производителей, обеспечивает не только ведение отчетности по международным стандартам, но и сопоставимость полученных показателей, приведение их к любому выбранному стандарту. Предоставляется возможность ввода произвольного набора показателей для проведения любого выбранного вида анализа, включая экономический анализ хозяйственной деятельности. Есть возможность получения пространственных сопоставлений через пересчеты по индексам. Входные данные могут поступать в модуль «Финансовый анализ» как из любого модуля системы «Галактика», так и путем экспорта из внешних программ.

2.2.4. Информационные системы и технологии управления проектами и программами

Понятие «проект» обозначает комплекс взаимосвязанных мероприятий, предназначенных для создания новых продуктов или услуг. Проект обладает новизной и неповторимостью и имеет строго определенные во времени начало и окончание. Основные этапы развития методов управления проектами в России включают в себя:

- истоки управления;
- применение ЭВМ для управления отдельными проектами;
- управление организацией (мультипроектное управление);

«интегрированные системы управления;

• современные методы профессионального управления проек тами.

Применение профессионального метода управления проектами нужно для успешного достижения целей и результатов проекта с требуемым качеством, в установленные сроки, в рамках бюджета и для удовлетворения участников проекта.

Технологии управления проектами начинаются со стадий планирования, которые являются наиболее важным процессом управления проектами, так как определяют всю деятельность предприятия по их осуществлению.

Планирование представляет собой циклический процесс. Он начинается с наиболее общего определения целей, движется к более детальному описанию того, когда, как и какие работы должны быть выполнены для достижения поставленных целей. По мере продвижения проекта от концепции к завершению появляется дополнительная информация об условиях, влияющих на ход работ.

Конкретная структура планов, применяемых на разных уровнях и стадиях планирования проекта, зависит от стандартов и подходов, принятых в отрасли и в организациях, осуществляющих проект.

В общем виде на уровне управления проектом можно выделить следующие виды планов:

. концептуальный план;

• стратегический план реализации проекта;

• тактические (детальные) планы.

Разные уровни управления в организации в разной степени вовлечены в разработку данных планов.

Входными данными для разработки плана проекта являются:

• договорные требования;

• описание доступных ресурсов;

• оценочные и стоимостные модели;

• документация по аналогичным разработкам.

Типовые системы календарного планирования обеспечивают основной набор функциональных возможностей.

Традиционно ПО для управления проектами подразделяется на профессиональные системы и системы для массового пользователя. Основные различия между системами проявляются в реализации функций ресурсного планирования и многопроектного планирования и контроля. Профессиональные системы предоставляют более гибкие средства реализации этих функций, но требуют больших затрат времени на подготовку и анализ данных и высокой квалификации пользователей. Пользовательские пакеты отличаются простотой использования и высокой скоростью получения результата.

Основными преимуществами использования АИС ПО для управления проектами являются:

• централизованное хранение информации по графику работ, ресурсам и стоимостям;

• возможность быстрого анализа влияния изменений в графике, ресурсном обеспечении и финансировании на план проекта;

• возможность распределенной поддержки и обновления данных в сетевом режиме;

• возможность автоматизированной генерации отчетов и графических диаграмм, разработки документации по проекту.

Характерным примером для представления структуры информационной системы и технологии управления проектами является система Open Plan. Она является лидером в области профессиональных систем управления проектами и обеспечивает:

• открытое масштабируемое решение для всего предприятия;

• мощные средства многопроектного планирования и контроля;

• средства организации многопользовательского режима работы с проектами, распределенного иерархически по уровням управления;

« гибкие средства структуризации проектов, стандартизации среды и функций управления проектами, настройку на задачи конкретного пользователя.

Возможности системы Open Plan заключается в следующем:

• составление календарного плана работ;

• управление ресурсами (финансы, исполнители, механизмы, материалы);

• анализ затрат;

• анализ рисков;

• мультипроектный анализ.

Open Plan используется в профессиональной (Professional) и настольной (Desktop) версиях. И профессиональная, и настольная версии системы включают в себя полный комплект функций по управлению проектами. Пользователями этой системы в организации являются как профессиональные менеджеры, осуществляющие согласование и оптимизацию планов проектов, анализ рисков, прогнозирование, так и рядовые участники проектов, выполняющие сбор, уточнение и актуализацию данных, готовящие отчеты.

Модель данных в Open Plan определяет структуру стандартных экранов (представлений). При создании нового проекта Open Plan автоматически включает набор стандартных представлений в его записную книжку. Когда вы открываете определенное представление, Open Plan показывает данные проекта в разрезе этого представления.

Учитывая широкий спектр возможностей Open Plan, рассмотрим только типы представлений, отображающие информацию о проекте:

• диаграмма Ганта — совмещается с электронной таблицей перечня работ и позволяет представлять различные форматы данных, удобных для получения информации о ресурсах, временных и стоимостных характеристиках проекта в целом или его отдельных частей, а также для редактирования иерархической структуры плана проекта и параметров отдельных задач;

• сетевая диаграмма — отображает сетевую модель в графическом виде как множество вершин, соответствующих работам, связанных линиями, представляющими взаимосвязями между работами. Является часто моделью сетевого графика работ;

• таблица работ — это табличное представление информации о временных и стоимостных характеристиках проекта в целом или отдельных его частей;

• гистограмма затрат — один из вариантов представления результатов анализа затрат;

• гистограмма рисков — один из способов ознакомления с результатами анализа рисков. Гистограмма рисков дает детальную картину вероятностного распределения высчитанных дат для ключевых работ в проекте.

Построение информационной системы и технологий календарного планирования и контроля, как правило, разбивается по подсистемам: планирование, контроль, структура проекта. Примером может служить подсистема «управление основной тематикой» (УОТ) на этапе планирования хода работ по разработке, производству и испытаниям летательных аппаратов в конструкторском бюро.

Подсистема УОТ используется для решения задач управления ходом работ в подразделениях конструкторского бюро (КБ), производства и летно-испытательного комплекса. Она создана для дальнейшего повышения качества управления ходом выполнения тем и заданий генерального конструктора путем более четкой организации управления с использованием ЭВМ и повышения личной ответственности участников работ на всех уровнях. Подсистема регламентирует:

• порядок планирования работ по темам и формирование планов подразделений;

• порядок оперативного управления ходом выполнения работ;

• права и обязанности каждого участника работ в данной подсистеме;

• форму и порядок прохождения документов, предусмотренных подсистемой;

• сроки исполнения документов подсистемы и правила их заполнения пользователями.

Видоизмененную структуру управления проектами применяют компании, которые занимаются оптовой торговлей продуктов питания и нуждаются в корпоративной информационной системе и технологиях (КИСиТ).

КИСиТ предназначается для автоматизации следующих сфер деятельности компаний:

- бухгалтерский и финансовый учет;
- управление закупками и поставками;
- анализ товарно-денежных потоков;
- взаимодействие центрального офиса компаний со структурными подразделениями и филиалами.

Перечисленные сферы деятельности относятся прежде всего к управленческим функциям компаний. Из этого следует, что автоматизации должны подвергнуться не только бизнес-процессы основной деятельности, но и система управления компаний. Разработке технического задания на КИСиТ предшествует работа по диагностике компании, реинжинирингу бизнес-процессов (на первом этапе) и проектированию системы управления компанией (на втором этапе).

Каждая функция управления реализуется через элементы системы, образуя, таким образом, матрицу системы управления. Главная задача построения системы управления проектами заключается в синтезе полной и непротиворечивой матрицы функций и элементов системы управления. Усилия по построению системы управления дадут результат только в том случае, если будут подчинены четко сформулированным целям. Следовательно, необходимым условием построения эффективной системы управления является наличие сформулированных целей и задач, четко определяющих качественные и количественные требования к системе управления.

Центральным содержанием первого этапа проекта является построение модели бизнеса «как должно быть» и ее сравнение с моделью «как есть». Для того чтобы сравнение было адекватным и на его основании можно было строить план изменений, необходимо описывать обе модели в единых терминах и методологии.

При моделировании деятельность организации рассматривается как система, состоящая из взаимодействующих между собой бизнес-процессов (потоков работ). Эффективное взаимодействие бизнес-процессов осуществляется через подсистемы управления. Результатом работы бизнес-процесса должно являться формирование пакета заказов для других бизнес-процессов.

Основное производство организации опирается на собственные производственные мощности. Если их нет, то под термином «основное производство» понимается поставка товара в точки, где он будет реализован оптовым или розничным покупателям, т. е. туда, где товар станет готовой продукцией.

В бизнес-процесс «поддержание и обеспечение деятельности» входят:

- закупка товаров;
- работа по эксплуатации основных фондов;

• транспортирование товаров и связанные с ним операции;
• складские операции.

Группа работ «Расчеты» является завершающей для всей последовательности построения бизнеса организации, так как именно здесь формируется основной результат — чистый денежный поток (прибыль минус инвестиции, производственные затраты и налоги).

Одной из наиболее распространенных технологий, применяемых для проведения анализа и структурирования бизнес-процессов и в целом для КИСиТ, является технология IDEFO.

IDEFO-методология основана на следующих положениях.

1. Графическое представление методом блочного моделирования. Графика «блоков и дуг» IDEFO-диаграммы отображает производственную операцию в виде блока, а интерфейсы входа-выхода в (из) операции представляются дугами, соответственно входящими в блок или выходящими из него. Описание производственных операций и взаимодействия блоков друг с другом производится посредством интерфейсных дуг, выражающих «ограничения», которые, в свою очередь, определяют, когда и каким образом операции выполняются и управляются.

2. Краткость графического представления объектов, процессов и связей. Документация архитектуры производственной системы для полноценного охвата должна быть точной. Двухмерная форма графического языка, применимого в IDEFO, имеет требуемую точность без потери возможности выразить такие взаимоотношения, как интерфейс, обратная связь, ошибочные пути и т.д.

3. Передача информации осуществляется использованием:

• диаграмм, основанных на простой графике блоков и дуг;
• меток на естественном языке для описания блоков и дуг, а также глоссария и сопроводительных текстов для определения точного значения элементов диаграммы;
• постепенного представления деталей, при котором на верхнем уровне иерархии показаны основные функции, а на следующих уровнях происходит их более подробное уточнение;
• схемы узлов в иерархии диаграмм, обеспечивающих возможность составления перечня (индекса) размещенных на них деталей;
• ограничений для облегчения чтения каждой диаграммы шестью подфункциями.

4. Строгость и точность. Выполнение правил IDEFO требует достаточной строгости и точности, чтобы удовлетворить принципам архитектуры ICAM, не накладывая в то же время чрезмерных ограничений на аналитика.

Методология IDEFO может использоваться для моделирования широкого круга систем, где под системой понимается любая комбинация средств аппаратного и ПО, а также людей.

Результатом применения методологии IDEFO является модель. Модель состоит из диаграмм, фрагментов текста и глоссария, которые имеют ссылки друг на друга. Диаграммы — главные компоненты модели. На диаграммах все функции производственной системы и интерфейсы представлены как блоки (функции) и дуги (интерфейсы). Место соединения дуги с блоком определяет тип интерфейса. Управляющие производством данные входят в блок сверху, в то время как материалы и информация, которые подвергаются производственной операции, показаны с левой стороны блока; результаты выхода показаны с правой стороны блока. Механизм (человек или автоматизированная система), который осуществляет операцию, представляется дугой, входящей в блок снизу.

Блоки и дуги в IDEFO-модели используются для представления связей между несколькими подфункциями на схеме технологического процесса пошагового моделирования (рис. 2.7).

Эта схема является подчиненной моделью и показывает конкретные интерфейсы, управляющие каждой подфункцией, а также источники и адресаты этих интерфейсов. Так, функция *B* зависит от двух входов и двух управлений и производит два выхода, от одного из которых зависит функция *C*.

Структуры ИТ моделирования с помощью IDEFO предусматривают построение IDEFO-модели. Оно начинается с представления всей системы в виде простейшей компоненты — одного блока и дуг, изображающих интерфейсы с функциями вне системы. Поскольку единственный блок представляет всю систему как единое целое, имя, указанное в блоке, является общим. Это верно и для интерфейсных дуг — они также представляют полный набор внешних интерфейсов системы в целом.

В IDEFO есть свои правила постепенного добавления деталей в процессе декомпозиции. Модуль всегда делится не менее чем на три, но не более чем на шесть подмодулей. Верхний предел — шесть — позволяет использовать иерархию для описания более сложных объектов. Нижний предел — три — гарантирует введение достаточного количества деталей, чтобы полученная декомпозиция представляла интерес.

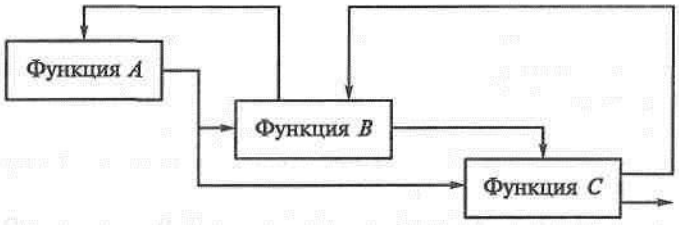


Рис. 2.7. Структурная схема пошагового моделирования в IDEFO

Для координации коллективной работы в КИСиТ методология **IDEFO** включает в себя методы разработки и критического анализа моделей большим коллективом, а также методы интеграции подсистем в IDEFO-архитектуру. Кроме того, в методологию **IDEFO** входят вспомогательные процедуры, например правила и способы ведения библиотек. Некоторые из этих правил и способов, такие как процедура рецензирования — цикл «автор—рецензент», используются и в других IDEF-методологиях.

Создание IDEFO-модели является основной компонентой «скоординированной коллективной работы». В модели «динамический процесс» требуется обычно участие более чем одного человека. При разработке проекта авторы создают первоначальные схемы, которые передаются участникам проекта для рассмотрения и замечаний. Порядок требует, чтобы каждый эксперт, у которого есть замечания к схеме, сделал их письменно и передал автору схемы. Этот цикл продолжается до тех пор, пока схемы, а затем и вся модель не будут приняты.

2.2.5. Построение информационных систем и технологий документооборота

Информационная система и технологии являются одним из основных в ИСУ предприятиями и организациями. Основная их функция и задачи заключаются в подготовке и реализации процессов переработки документальной информации синхронно всему жизненному циклу деятельности организации и ее продукции. Современный подход системной реализации ИТ делопроизводства базируется на применении систем электронного документооборота. К ним предъявляется множество требований в рамках проявлений свойств, присущих сложной информационной системе. Но имеется ряд дополнительных требований, которые также формируют ее структуру построения.

Из дополнительных требований можно выделить следующие.

Масштабируемость. Желательно, чтобы система документооборота могла поддерживать как пять, так и 5 тыс. пользователей и ее способность наращивать мощность определялась только мощностью аппаратного обеспечения, на котором она установлена. Выполнение этого требования может быть обеспечено с помощью поддержки индустриальных серверов БД, производства, например компаний Sybase, Microsoft, Oracle, Informix, которые существуют практически на всех возможных программно-аппаратных платформах, обеспечивая тем самым максимально широкий спектр производительности.

Распределенность. Основные проблемы при работе с документами возникают в территориально-распределенных организаци-

ях, поэтому архитектура системы документооборота должна поддерживать взаимодействие распределенных площадок.

Модульность. Возможно, что заказчику может не потребоваться сразу внедрение всех компонентов системы документооборота, а иногда круг решаемых заказчиком задач меньше всего спектра задач документооборота. Поэтому очевидно, что система должна состоять из отдельных модулей, интегрированных между собой.

Открытость. Система документооборота не может и не должна существовать в отрыве от других приложений (например, часто необходимо интегрировать систему с прикладной бухгалтерской программой).

Структуризация системы документооборота определяется комплексом ее целей назначения и иерархией их построения. Задачи и соответственно необходимая система автоматизации определяются стадией жизненного цикла документа и целями его назначения, которые необходимо поддерживать. Жизненный цикл состоит из двух основных стадий:

1) разработка документа, которая может включать в себя собственно разработку содержания документа, оформление документа, утверждение документа. Если документ находится на стадии разработки, то он считается неопубликованным и права на него определяются правами доступа конкретного пользователя;

2) стадия опубликованного документа, которая может содержать: активный доступ, архивный документ краткосрочного и долгосрочного хранения, уничтожение документа.

Когда документ переходит на вторую стадию, он считается опубликованным и на него остается только одно право — доступ на чтение. В качестве примера опубликованного документа приведем шаблон стандартного бланка предприятия. Кроме права доступа на чтение могут существовать права на перевод опубликованного документа в стадию разработки.

В зависимости от конкретной стадии жизненного цикла документы, с которым имеют дело архивные системы, подразделяются на статические и динамические.

Статические архивы документов (или просто архивы) — это системы, которые обрабатывают только опубликованные документы.

Динамические архивы (или системы управления документами) работают как с опубликованными документами, так и с теми документами, которые находятся в разработке.

Единство правил документирования управленческих действий на всех уровнях управления обеспечивается применением унифицированных систем документации **(ГОСТ** 6.38 — 90). Виды и разновидности документов, необходимых и достаточных для работы учреждений, определяются в соответствии с фундаментальным назначением каждого документа в глоссарии.

Составление текстов управленческих документов является выраженное средствами делового языка описание содержания управленческих действий.

При оформлении документов необходимо соблюдать правила, обеспечивающие юридическую силу, качественное и оперативное исполнение документа.

Для организационно-распорядительных документов установлен 31 реквизит в соответствии с ГОСТ 6.38 — 90.

Обязательными реквизитами документов являются: наименования учреждения — автора документа, название вида документа, текст, заголовок к тексту, дата и индекс документа, подпись, отметка об исполнении документа, место создания или издания документа, код организации — автора, код формы документа.

Применение бланков при подготовке документов повышает культуру управленческого труда, придает информации официальный характер, облегчает исполнение и дальнейшее использование документа.

Служебные документы составляются на бланках форматов А4 и А5, отпечатанных типографским способом, в соответствии с ГОСТ 9327 — 60. Для отдельных видов документов допускается применение формата А3.

Заголовок — это краткое изложение содержание документа. Он должен быть максимально кратким и емким, точно передавать смысл текста, грамматически согласовываться с названием документа.

Датой документа является дата его подписания, утверждения или события, которое зафиксировано в документе. Даты подписания, утверждения, согласования, а также даты, содержащиеся в тексте, оформляют цифровым способом.

Подготовленные проекты документов перед подписанием в ряде случаев согласовываются с заинтересованными учреждениями, структурными подразделениями, отдельными должностными лицами. Это делается для подтверждения их согласия с содержанием документа. Согласование проводится внутри учреждения и вне его.

Движение документов в учреждении с момента их получения или создания до завершения исполнения, отправки или сдачи в дело образуют документооборот.

Ошибочно доставленная корреспонденция пересылается по принадлежности. Документы сортируются на регистрируемые и нерегистрируемые.

Этот набор постоянной и переменной информации документа, так же как и последовательность его оформления, представляется в файле «Документы» и может использоваться как типовой для любых видов документации.

2.3. Интеграция, инсталляция и автоматизация ИТ управленческой деятельности

Наиболее важной целью разработки технических средств групповой работы является создание интегрированной среды работы с удаленными сотрудниками, которая является неотъемлемой частью функционирования сетевой корпорации.

С середины 1990-х гг. тема интегрированных систем управления (ИСУ) стала появляться в теории и практике управленческого учета и планирования крупнейших российских предприятий.

Это было связано с началом работ на крупнейших сырьевых гигантах России по инсталляции полнофункциональных программных (автоматизированных) пакетов, посредством которых в аналогичных западных корпорациях решают вопросы сквозного (от уровня высшего руководства до низовых звеньев управления) учета товарно-материальных и финансовых потоков и выработки единой хозяйственной политики. Однако реальные результаты внедрения полнофункциональных программных пакетов на большинстве российских предприятий оказались очень незначительными.

ИСУ представляет собой комплексный механизм управления компанией, состоящий из следующих основных блоков.

Аналитический блок — система формализованной обработки учетных данных для целей принятая управленческих решений. Аналитический блок ИСУ основывается на модели оптимального бюджетирования.

Учетный блок — система документооборота для информационного обеспечения управленческих решений (управленческий, маркетинговый и финансовый учет).

Организационный блок — структура управления (функции и регламент координации, соподчинения и контроля деятельности управленческих служб) для обеспечения процесса управленческого и финансового планирования.

Программно-технический блок — программный продукт, поддерживающий аналитический, учетный и организационный блоки. Для ИСУ можно использовать адаптированные стандартные пакеты (R/3, BAANIV, Oracle Applications и др.). В этом случае ИСУ существует в форме традиционного (бумажного) документооборота.

При реализации программно-технического блока сбор и обработка учетных данных (включая движение информации по вопросам внутрикорпоративного регламента работы) осуществляются средствами ПО, что качественно повышает быстродействие и детализацию учетной и планово-аналитической работы.

Рассмотрим подробнее указанные компоненты ИСУ:

Аналитический блок ИСУ. Модель оптимального бюджетирования — стратегический программный продукт, базирующийся на учетно-аналитических разработках последнего поколения:

• учета, планирования и анализа по видам деятельности (Activity-Based Costing);

• теории стоимости фирмы (Welfare of the Finn Theory).

Планирование и учет по видам деятельности ABC-costing предполагают сопоставление в планово-аналитической и учетной деятельности затрат и видов деятельности предприятия, приведших к образованию данных затрат (в традиционных системах планирования и учета затраты калькулируются по местам их возникновения).

Теория стоимости фирмы обеспечивает построение интегральных моделей хозяйственной деятельности, при котором любое управленческое решение рассматривается в контексте влияния на величину рыночной стоимости фирмы (в акционерном обществе — на сумму текущей рыночной стоимости акций).

Так, в рамках данных моделей можно:

• количественно определить сравнительную эффективность от распределения прибыли в прирост финансовых резервов и закупку основных средств и, соответственно, пропорции оптимального распределения прибыли;

• обеспечить расчет оптимальной величины и структуры привлеченных источников финансирования; рассчитать оптимальную величину и структуру выпуска и реализации продукции с учетом эластичности спроса по различным рынкам сбыта, функции затрат по различным производственным линиям, капиталоемкости отдельных видов продукции и прочих факторов и т.д. В отличие от АСУП, основанных на традиционных моделях бюджетирования, система оптимального бюджетирования позволяет решать следующие задачи, актуальные для деятельности любого крупного производственного объединения:

• возможность расчета совокупного (системного) эффекта от осуществления конкретных управленческих мер, связанных с движением ресурсов компании (например, сбыт определенного физического объема готовой продукции, увеличение цены реализации, освоение капитальных вложений по конкретному инвестиционному проекту, увеличение финансовых резервов, взятие кредита, проведение дополнительной эмиссии акций, погашение кредита и др.). В ИСУ расчет производится путем формализации основных функциональных взаимосвязей между бюджетными (плановыми) параметрами;

• возможность соизмерения видов деятельности компании и обусловленных осуществлением данных видов деятельности затрат и тем самым четкое количественное выявление текущих и перспективных резервов снижения себестоимости и повышения финансовых результатов компании. Обеспечение непрерывности процесса «план-факт анализ — планирование на следующий бюджетный период» независимо от запаздывания сводной финансовой отчетности за прошедший бюджетный период;

• четкое разграничение издержек планирования и издержек выполнения плана (спецификация ответственности плановых органов и производительных подразделений по отклонениям фактических показателей от плановых);

• возможность формализации задачи оптимального распределения средств между целями повышения производительной эффективности и улучшения финансовой стабильности;

• возможность количественного расчета оптимального инвестиционного бюджета;

• возможность соизмерения эффективности управленческих мер, относящихся к разным временным периодам, и оптимизации планового процесса по времени осуществления;

• выбор оптимальных показателей материального стимулирования, количественный расчет оптимальных коэффициентов и баз начисления в системе премирования;

• возможность количественного соизмерения произведенных в данном бюджетном периоде затрат, эффекта от исполнения бюджетов затрат и себестоимости произведенной, отгруженной и реализованной продукции;

• обеспечение корректной системы описания отклонений по стадиям финансового цикла и получение достоверной оценки фактической стоимости оборотных активов при ведении нормативного учета затрат;

• обеспечение алгоритма формализованного решения вопроса по выбору оптимального метода платежа.

Учетный блок ИСУ. Учетный блок реализует систему внутреннего и внешнего документооборота, обеспечивающую сбор данных для целей управленческого и финансового планирования, а также составления сводной финансовой отчетности по российскому плану счетов и в соответствии с требованиями GAAP. Учет в ИСУ может производиться как в форме бумажного документооборота, так и посредством внедрения программного продукта (системы R/3, BAAN IV и др.).

Организационный блок ИСУ. Организационный блок — это:

• количество и ресурсы управленческих служб компании;

• функциональное распределение деятельности управленческих служб;

• регламент деятельности управленческих служб (система соподчинения и координации) для обеспечения следующего динамического (постоянно повторяющегося) процесса.

Организационный блок ИСУ состоит из трех основных элементов:

• система движения информации для плановых и контрольных целей;

• система соподчиненности различных звеньев организационной структуры в процессе сбора и обработки информации и при-

нятия управленческих решений (в первую очередь, высшего менеджмента, центрального аппарата контролеров, менеджмента подразделений и плановых служб подразделений);

• система управления по центрам ответственности (центры управленческих затрат, нормативных затрат, доходов, прибыли, инвестиций); на основе этого определяется «степень свободы» руководства различных подразделений и строится система материального стимулирования в контексте системы управления затратами.

В практическом плане внедрение соответствующей организационной структуры включает в себя два основных момента:

• создание новых служб и изменение функций существующих плановых служб компании для адекватного обеспечения процесса управленческого и финансового планирования;

• разработку внутренних положений, регламентирующих ответственность различных подразделений в процессе функционирования ИСУ. Важнейшим моментом данных внутренних положений является для каждой службы перечень так называемых стандартных процедур (routines), описывающий их ежедневные функции в процессе сбора и анализа учетной информации, а также устанавливающий ответственность за ненадлежащее исполнение этих функций.

Программно-технический блок ИСУ. Качественное повышение эффективности функционирования ИСУ компанией достигается за счет использования комплексных программно-технических решений, составляющих программно-технический блок системы. В результате инсталляции программно-технического блока становятся возможными оперативная и достоверная оценки состояния компании, централизованное управление финансовыми ресурсами и сквозной контроль материальных потоков, что выражается в контроле издержек на всех стадиях производственного цикла, от поступления основного сырья и вспомогательных материалов на склад до выпуска готовых изделий.

ИСУ компанией основывается на следующих положениях.

1. Использование модели оптимального бюджетирования в качестве аналитического блока ИСУ.

Применение модели оптимального бюджетирования является основой ИСУ как программно-аналитического продукта последнего поколения (1980 —1990-е гг.). В отличие от традиционных систем управления ИСУ, основанная на модели оптимального бюджетирования, позволяет решать ряд актуальных для деятельности любого крупного предприятия проблем учета и планирования при ведении хозяйственной деятельности.

2. Построение программно-технического блока системы на базе одного из существующих на рынке стандартных пакетов полной функциональности.

3. Внедрение систем управленческого и финансового планирования по принципу «сверху вниз» (т. е. от управляющей компании к дочерним предприятиям).

Существует два варианта построения единой системы управленческого и финансового учета и планирования компании:

1) «сверху вниз». Система управления строится на уровне головной компании (холдинга) и постепенно «спускается» (детализируется) на уровень дочерних предприятий;

2) «снизу вверх». Система управления строится на уровне отдельных фрагментов холдинга (например, на ряде дочерних предприятий) и в дальнейшем интегрируется на уровне холдинга.

Как показывает мировой опыт, второй вариант является, безусловно, более затратным и, соответственно, менее эффективным:

В настоящее время имеется ряд существенных обстоятельств, обусловливающих важность внедрения ИСУ на крупных промышленных предприятиях России.

Во-первых, для большинства крупных российских промышленных компаний характерны:

- достаточно сложная система распределения полномочий между головной компанией и производственными подразделениями, дочерними и зависимыми предприятиями, т.е. разделения показателей хозяйственной деятельности на планируемые из центра (дирекции, управляющей компании холдинга) и определяемые на местах;
- многообразие товарно-материальных и финансовых потоков, определяемое наличием элементов вертикальной (по стадиям технологического цикла) и горизонтальной (региональное и диви-зиональное разделение труда) интеграции;
- многообразие рынков сбыта, отличающихся по своей емкости и эластичности спроса по цене;
- многообразие видов деятельности (производство, услуги, торговля, строительство) и, как следствие, необходимость дополнительного разграничения по видам деятельности в системе управленческого учета и планирования;
- усложненная система контроля и стимулирования деятельности подразделений, которая в идеале должна охватывать все факторы хозяйственной деятельности, контролируемые подразделениями, и обеспечивать унификацию (т. е. равенство стимулирования различных подразделений за одинаковый вклад в финансовые результаты компании);
- различный характер производственного процесса по различным видам деятельности и, как следствие, различные способы учета затрат и финансовых результатов (так, в рамках одной компании одновременно могут вестись попроцессный, попередельный и по-заказный методы учета (в зависимости от вида деятельности));
- недостаточное качество информационного обеспечения процесса принятия управленческих решений (недостаточная полно-

та, достоверность и оперативность получения данных менеджерами всех уровней управления);

• недостаточная регламентированность документооборота и, как следствие, снижение эффективности систем учета и контроля деятельности компании.

Во-вторых, в настоящее время большинство крупных российских промышленных компаний (особенно в топливно-энергетическом комплексе) активно сотрудничают с зарубежными партнерами в производственной и финансовой сферах. Одним из условий продолжения широкомасштабного сотрудничества с западными партнерами является ведение учета в соответствии с нормами GAAP в целях удовлетворения требований зарубежных акционеров, кредиторов и контракторов. Внедрение интегрированной системы управления позволит компании эффективно решить данную задачу, так как ИСУ основывается на новейших разработках в области управленческого планирования и информационных технологий, применяемых крупными компаниями Западной Европы и США. Одной из основных предпосылок ИСУ является ведение управленческого и финансового документооборота в соответствии с международными нормами учета и отчетности.

Таким образом, внедрение интегрированной системы управления в российских промышленных компаниях:

• создаст предпосылки для качественного улучшения процесса управленческого планирования и контроля деятельности компании со стороны высшего и среднего руководства;

• обеспечит должное представление о результатах деятельности компании западным партнерам и, тем самым, окажет положительный эффект в сфере расширения сотрудничества с зарубежными предприятиями и организациями.

Контрольные вопросы

1. Опишите роль ИС управления в функционировании предприятий.
2. Как классифицируются ИС по организационным уровням? Дайте им характеристики по применению.
3. Сформулируйте особенности сетевых систем управления и их администрирования.
4. Приведите классификацию сетей и охарактеризуйте их.
5. Приведите системы автоматизированного поиска информации в Интернете.
6. Раскройте технологическое обеспечение АИТ ОД в АИС СЭО.
7. Опишите уровни СУ предприятиями на примере EPR-системы.
8. Что такое Open Plan?
9. Раскройте основное содержание методологии IDEFO.
10. Обоснуйте необходимость внедрения ИСУ на предприятиях России.

Глава 3
МЕТОДОЛОГИЯ ПОСТРОЕНИЯ АДМИНИСТРИРОВАНИЯ И ЕГО СРЕДСТВА

3.1. Организационные и программные структуры администрирования

3.1.1. Конфигурация системы администрирования

Для того чтобы любая ИС работала с максимальной отдачей, ее следует должным образом администрировать (хотя разработчики ИС стремятся создавать системы, требующие наименьшего набора функций, инструментальных средств и методов их администрирования). К одной из таких современных систем можно отнести систему Unix и ее версии. Взяв за основу принципиальные подходы Unix к структурированию таких систем, рассмотрим их организацию и архитектуру построения и функционирования.

Методология построения таких систем ориентируется на большое количество небольших компонентов и команд. Фактически это набор мелких команд, спроектированных для совместной работы. Вместо того чтобы выполнять большую программу управления пользователями, система должна предоставлять различные команды, которые можно использовать для управления учетными записями пользователей. Эта дифференциация команд позволяет более эффективно создавать необходимые сценарии. Достигнуть успеха в администрировании Unix-компьютера можно, если научиться составлять в одно целое команды при формировании сценариев. Достигнув в этом вопросе мастерства, трудно обходиться без эффективно работающих сценариев, даже для выполнения своей персональной работы. Например, для использования бесплатного почтового ящика электронной почты Интернета при резервировании важных файлов можно по соответствующему сценарию предварительно автоматически определить файлы, подлежащие дублированию, скомпоновать и сжать их, а затем переслать на требуемый электронный адрес. Весь этот процесс легко запрограммировать тремя или четырьмя командными строками на языке сценария оболочки.

Унифицированная файловая система, составленная из различных физических устройств (жестких дисков, гибких магнитных

дисков и компакт-дисков и др.) рассматривается как часть единой файловой системы. Управление устройствами и управление файлами являются важными составными частями системного администрирования. Установление квот, архивирование файлов, которые больше не используются, добавление дискового пространства — вот виды деятельности, которые имеют отношение к файловой системе.

Среда, которая дает возможность многим пользователям одновременно регистрироваться в системе, обеспечивает легкую поддержку системой многих пользователей без специального программного обеспечения сервера, которое требуется в некоторых других системах (Windows NT). Управление учетными записями пользователей является одной из наиболее трудоемких задач системного администрирования. Позволить пользователям получить преимущества через интерактивную регистрацию, сеансы X Window или файловый сервис и в то же время защитить систему и ее сервисы от злоупотреблений пользователями — главная функция Unix.

Защита пользователей от влияния других, потенциально недружественных, пользователей связана с рассмотрением различных вопросов безопасности. Они особенно важны, если система подключена к Интернету. Около 10 лет назад Интернет был дружественной средой, однако положение изменилось. В настоящее время, когда существует широкий доступ к Интернету, система открыта для пользователей с быстродействующими подключениями к Интернету, которые пытаются взламывать чужие системы. Хотя для них это потенциально ценный опыт обучения, им необходимо защитить систему от несанкционированных вторжений.

Способность одновременно выполнять много приложений (программ или процессов) даже при простаивающей системе — важное свойство Unix. Она выполняет намного больше процессов, чем Windows NT. В терминах администрирования системы это означает, что нужно сделать так, чтобы система никогда не была перегружена слишком большим количеством процессов, поддерживая выполнение только тех из них, которые действительно необходимы.

Обобщенную структуру администрирования ИС можно представить в виде схемы (рис. 3.1). По этой схеме конфигурируются как техническая, так и программно-организационная реализация, но она является условной, так как все входящие в систему администрирования конфигурации очень сильно интегрированы между собой и часто взаимозаменяемы по функциональным возможностям обеспечения пользователей.

Рабочие станции, называемые также графическими, функционируют как пользовательские настольные системы. Большинство рабочих станций используется для работы с большими мониторами и значительным объемом ОЗУ. Однако такое положение быст-

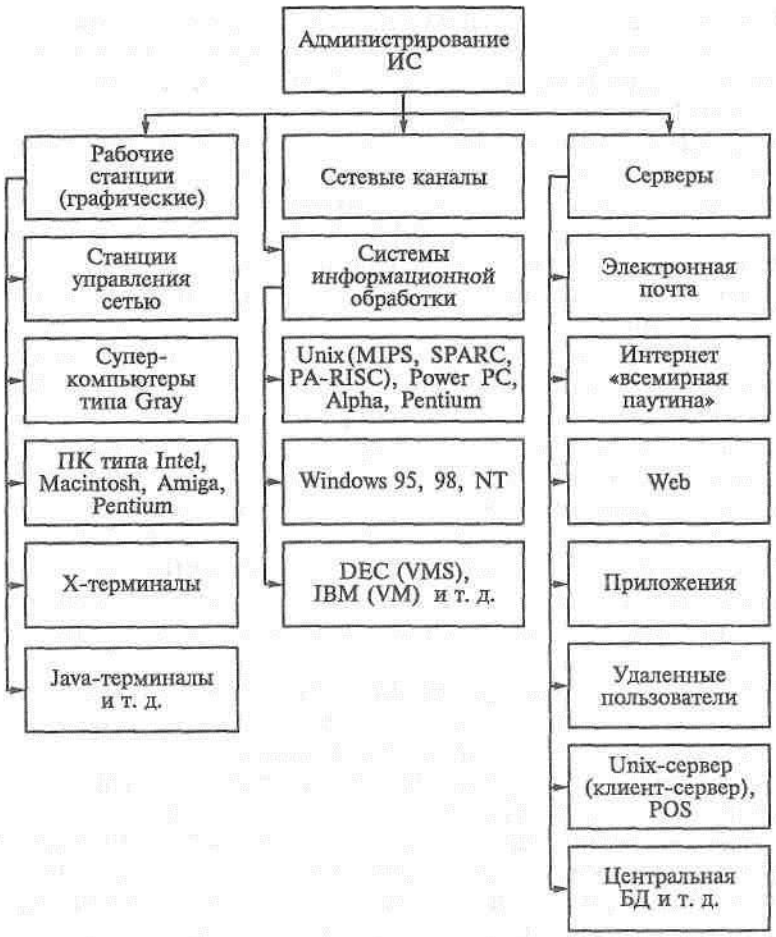


Рис. 3.1. Обобщенная структура администрирования ИС

ро изменяется с ростом популярности Linux, FreeBSD, SCO Unix, Solaris X86 и всех разновидностей программных продуктов для Unix, привязанных к аппаратным средствам Intel. Теперь, когда процессоры Pentium способны обеспечивать мощность обработки информации, сравнимую с мощностью процессоров SPARC, персональные компьютеры становятся рабочими станциями. При одинаковой рабочей нагрузке требования к памяти и ресурсам центрального процессора рабочей станции Unix меньше, чем при использовании этого же компьютера под управлением Windows любой версии начиная с 3.1.

Совсем недавно тенденция к замене настольных систем Unix компьютерами с Windows NT или Windows 9X была очень силь-

ной. Теперь же появилось новое прикладное ПО, которое обеспечит в Unix-системе такой же уровень функциональности, какой имеется в любой Windows-системе. Многие крупные корпорации, например Lotus Development, также привязали свои популярные программные продукты (Domino R5) к Unix. Рабочие станции Unix сохраняют сильные позиции в системах автоматизированного проектирования и системах автоматизированного управления производством (САПР/АСУП), разработки ПО, финансов и научной визуализации. Почти вся графика Unix пришла из системы X Window с трехмерной визуализацией, добавленной OpenGL и другими расширениями.

При этом администрирование рабочих станций не остается таким же, как в сервере. В типичном случае рабочая станция не предлагает таких сетевых сервисов, как файловый сервис, анонимная передача файлов по ftp-протоколу и т.д. Здесь должны администрироваться только базовые сервисы — обслуживание файлов, учетных записей, программных средств и т.д.

Другим основным использованием Unix является *платформа для управления сетью.* В данном случае слово «сеть» имеет общий смысл и может означать что угодно — от маршрутизатора до набора серверов, которые не обязательно работают под управлением Unix.

Управление сетью означает, что необходимо регулярно опрашивать каждый нужный узел для проверки его состояния и сбора статистики, получать предупредительные сообщения от этих узлов и выполнять все виды других работ, связанных с управлением и мониторингом сети. Платформа, используемая для удовлетворения таких потребностей, должна быть очень устойчивой и гибкой. Unix идеально удовлетворяет этим требованиям, и большая часть коммерческого программного обеспечения для управления сетью выполнена в расчете на использование Unix-систем.

Станции управления сетью требуют конфигурации достаточной мощности, так как они выполняют громоздкие графические приложения. Часто для своей работы приложения станций сетевого управления требуют несколько гигабайтов дискового пространства, несколько сотен мегабайтов памяти, ускоренных графических адаптеров и мощного центрального процессора. Иногда эти станции также используются для того, чтобы сетевые менеджеры с удаленных станций могли запускать графические приложения и получать на своих мониторах их вывод — это требует еще больше ресурсов.

Unix-системы работают *на большом разнообразии рабочих станций* — от суперкомпьютеров Cray до настольных компьютеров, таких как ПК на базе микропроцессоров Intel, компьютеры Macintosh и Amiga. Сейчас даже предпринимаются усилия по привязке бесплатной версии Unix (Linux) к переносимым устройствам,

работающим под ОС Palm. Рабочие станции Unix и серверы производятся фирмами Sun Microsystems, Hewlett-Packard, IBM, Digital Equipment Corp. и Silicon Graphics. Помимо приобретения всей системы, т.е. аппаратного и ПО, можно также приобрести только ПО Unix, которое будет выполняться на персональных компьютерах Intel и других системах, у таких производителей, как SCO и BSDI.

В настоящее время Unix работает на большом разнообразии компьютерных архитектур, включая RISC (Reduced Instruction Set Computer — компьютер с сокращенным набором команд) и CISC (Complex Instruction Set Computer — компьютер со сложным набором команд), как это представлено в табл. 3.1. Некоторые архитектуры, такие как PowerPC, работают со многими версиями Unix (IBM AIX, Sun Solaris, Linux и т.д.) наряду с другими операционными системами (MacOS, BeOS и т.д.).

X-терминалы предоставляют пользователям графическую часть рабочей станции Unix без обязательной платы за полностью укомплектованную систему. X-терминал использует мощность сервера (как правило, Unix-сервера) для обслуживания приложений, работающих с графическими дисплеями. Большинство поставщиков X-терминалов в настоящее время модифицируют свои продукты так, чтобы они были как X-, так и Java-терминалами.

Кроме выполнения общего конфигурирования, X-терминалы не нуждаются в администрировании.

Термин «открытая система», как и термин «клиент-сервер», является синонимом Unix. Выбирая открытую систему вроде Unix, пользователь не попадает в зависимость от какого-либо конкретного поставщика. Он остается свободным от решений, навязанных коммерческим поставщиком, поэтому если у него возникают проблемы, сохраняется возможность перехода на продукцию другого поставщика. Unix представляет собой одну из наиболее открытых операционных систем, существующих в настоящее время.

Таблица 3.1

Основные архитектуры, поддерживаемые Unix

Архитектура процессора	Компания
MIPS	Silicon Graphics
SPARC	Sun Microsystems
PA-RISC, CISC	Hewlett-Packard
PowerPC	IBM
Alpha	Digital Equipment
Pentium	Intel

Однако не все Unix-системы одинаковы. При администрировании приходится сталкиваться с незначительными различиями в конфигурировании, запуске и останове Unix-систем, полученных от различных поставщиков.

При такой широкой поддержке архитектур процессоров многие версии Unix со временем разделились между собой, особенно в системном администрировании. Здесь никогда не наблюдалось такой хорошей стандартизации, как в базовых командах Unix. Названные различия привели к разделению рынка Unix, создав тем самым возможности для наступления конкурирующих систем, таких как Windows NT.

С середины 1980-х гг. компания AT&T, обладавшая правами собственности на торговую марку Unix (которые впоследствии несколько раз перепродавались), начала унифицировать основные версии Unix, ее собственную версию AT&T System V Unix и версию BSD. Получившаяся System V версии 4 объединила в себе свойства обоих названных систем и сформировала базис для последующих реализации Unix, таких как Solaris 2.x фирмы Sun.

Фирма Sun переименовала старые версии своей SunOS 4.x, созданные на основе BSD, в Solaris 1.x. Большинство администраторов, говоря о системах SunOS 4, называют их SunOS, а не Solaris 1; при этом общий термин Solaris они используют для обозначения систем семейства Solaris 2.

Большая часть версий Unix не имеет слова «Unix» в своем названии из-за давних лицензионных проблем, составляющих предмет спора с компанией AT&T — создателем системы Unix. Это приводит к некоторым недоразумениям относительно того, что является, а что не является системой Unix. Известны такие названия версий Unix, как SunOS (Sun), Solaris (также Sun), HP-UX (Hewlett-Packard), Irix (Silicon Graphics) и AIX (IBM).

Кроме коммерческих продуктов сообщество Unix создало и бесплатные версии системы Unix, такие как Linux, FreeBSD и NetBSD.

Основная причина существования всех этих версий связана с переносимостью ПО Unix. Unix была одной из первых операционных систем, написанных в основном на языке программирования высокого уровня C. В то время большинство ОС писались в кодах ассемблера, что делало их очень трудными для преобразования кода под другие архитектуры. Вследствие того, что Unix была написана в основном на языке C, ее перенос на другие архитектуры намного облегчился. Поэтому почти с самого начала Unix работала на совершенно различных платформах.

В дополнение к System V версии 4 производители ПО, собравшись вместе, создали семейство стандартов, назвав его POSIX, которое определяет, какие функции должны обеспечивать Unix-системы и Unix-подобные системы. Windows NT тоже соответствует некоторым стандартам POSIX.

Для того чтобы еще больше унифицировать версии Unix, основные производители этого ПО определили около 1160 интерфейсов (в основном, это вызовы функций на языке C), которые они поддерживают через свой стандарт Spec 1160.

Производители ПО Unix также определили стандарт общей среды рабочего стола, или CDE, который обеспечивает графический интерфейс пользователя, используемый на рабочих станциях Unix и X-терминалах. Все основные производители ПО Unix, за исключением Silicon Graphics, поддерживают CDE.

Переходя от одной версии Unix к другой, можно обнаружить разницу в командах и способах администрирования систем. Например, принтеры в системах Solaris подключаются другим способом, чем в системах, которыми управляет FreeBSD. При этом ни один из этих способов не имеет преимуществ по сравнению с другим; просто они разные и у каждого из них свои преимущества и недостатки.

Для нейтрализации подобных отличий производители ПО Unix заметно активизировались, создавая дружественные к пользователю системные интерфейсы администрирования, которые обеспечивают уровень функциональности, сравнимый с функциональностью панели управления в Windows. Даже при использовании IRIX или Linux, которые предоставляют наиболее завершенные графические приложения системного администрирования, приходится запускать Xterm и вводить команды. Наилучшим подходом, по-видимому, является смешанный (например, кое-что делать с помощью графического интерфейса пользователя (GUI), а кое-что — с помощью команд).

С ростом популярности *Windows NT среди настольных систем* большая часть усилий в Unix-системах связана с серверами. Серверы предоставляют такие сервисы, как электронная почта, Web, выполнение приложений, а также интерактивные сеансы удаленных пользователей. Большая часть поставщиков услуг Интернета использует Unix-серверы.

Широкий диапазон услуг, оказываемых серверами, делает задачу их администрирования достаточно трудной. Можно добиться полного успеха в ее решении «одним махом», но, скорее всего, придется делать маленькие шаги — один за одним в нужном направлении. В конечном итоге можно получить стабильно работающую систему.

Электронная почта, поддерживаемая Unix с момента ее возникновения, обеспечивает средство связи даже в том случае, если пользователи находятся на разных континентах. Если говорить о пользователях, находящихся в России, Японии, Корее, Европе и Северной Америке, то различия во временных зонах затрудняют планирование времени для речевого общения. Факсимильные устройства могут передавать изображения документов, однако нельзя

послать по факсу файл документа. С помощью электронной почты можно передать файл документа. Пользователи могут посылать документы и отвечать на сообщения в течение своего рабочего дня. Пользователи в других временных зонах могут читать эти сообщения также в свое рабочее время. Временное различие может иметь место не только в Северной Америке, где разница во времени между Калифорнией и Нью-Йорком составляет 3 ч, но и в России, где разница в часовых зонах достигает 7 ч. Кроме того, используя электронную почту, не надо беспокоиться о таких вещах, как занятая телефонная линия либо отсутствие бумаги в удаленном факсимильном аппарате.

Хотя по мере подключения новых систем обслуживаемый поток информации значительно возрастает, распространение стандартных протоколов Интернета значительно облегчает работу системного администратора. Обычно при администрировании почтового сервера ожидается обработка сообщений электронной почты, поступающих в адрес администратора почтового сервиса, обработка спэма (как входящего, так и исходящего), рассмотрение других вопросов, не связанных с самой системой. И все же эти вопросы также являются частью правильного системного администрирования.

Почти каждая ОС поддерживает работу Web-броузеров. Хранение информации в Web-форматах, особенно в формате HTML, обеспечивает возможность пользователям использовать практически любую ОС при просмотре информации и обмене информацией. Web предоставляет в распоряжение пользователей один из лучших и самых легких способов обмена информацией.

Обмен данными через Web-броузер оказался очень удобным в работе компаний, совершивших корпоративные приобретения. Можно столкнуться со случаем, когда различные подразделения недавно объединенной компании используют конфликтующие программные средства, такие как Microsoft Word, WordPerfect и FrameMaker в различных ОС, включая MacOS, Windows и Unix. Здесь для пользователей необходимо найти способ обмениваться информацией о проектах, находящихся на разных стадиях развития. Эту задачу решает ПО Web-сервера в системе Unix.

Почти каждый прикладной текстовый процессор может сохранять информацию в формате HTML, и почти каждая система может просматривать Web-данные. Порекомендовав пользователям записывать данные в HTML-формате, а затем перемещать документы с Web-сервера в Intranet, можно гарантировать, что разрозненные части объединенной компании смогут работать вместе.

В *системах клиент-сервер* необходимо администрировать ресурсы, затрачиваемые И С на обслуживание сетевых подключений к серверу, в том числе мониторинг информационных потоков в сети, использование серверной частью приложения памяти, ресурсов

центрального процессора, а также параллельного доступа, пиковых периодов загрузки и многих других параметров.

Термин «система клиент-сервер» часто используется как условное наименование Unix-сервера, работающего с Windows-клиентами и заменяющего мэйнфрейм. Unix завоевала большой сегмент рынка заменителей мэйнфреймов в значительной степени вследствие того, что вся система клиент-сервер часто стоит меньше, чем одногодичное обслуживание мэйнфрейма и его приложений.

Традиционная архитектура мэйнфрейма напоминает централизованную обработку информации. В противоположность этому система клиент-сервер распределяет задачи, которые ранее выполнялись на мощном мэйнфрейме, между Unix-серверами и большим количеством клиентов. Перемещая пользовательский интерфейс от простых терминалов к таким интеллектуальным клиентам, как персональные компьютеры, работающие под управлением Windows или MacOS, система клиент-сервер снижает стоимость обработки информации при обслуживании большего количества пользователей.

Современные системы клиент-сервер часто включают в себя три или четыре уровня (в отличие от двух первичных уровней: клиента и сервера), построенных на промежуточном ПО с использованием технологий Web или Java.

Также известные как *POS {Point-Of-Sale — пункт продаж),* системы для пунктов продаж стремятся достигнуть максимального дохода при низких затратах. Большинство POS-инсталляций в конфигурациях для розничной продажи включают в себя промежуточный Unix-сервер с недорогими терминалами, заменяющими кассовые аппараты.

При администрировании в POS-системах необходимо следить за такими деталями, как количество дискового пространства, используемого временными файлами (экранные запросы, сообщения и т.д.), память и другие, так как POS-система используется в ходе многочисленных интерактивных сеансов. Время реакции системы в этих системах также важно — вы ведь не хотите, чтобы кассир был вынужден сказать клиенту: «Пожалуйста, подождите. Система сообщит вам, сколько это будет стоить, приблизительно через 4 мин». Ключевыми моментами в достижении хорошего времени реакции являются низкая загруженность системы, достаточный объем памяти и большое количество дискового пространства для размещения временных файлов. Если несколько POS-си-стем подключены к серверу центральной базы данных, то также потребуются неперегруженный сетевой канал и правильно настроенный сервер БД.

Особую роль в конфигурации системного администрирования играет взаимодействие различных используемых систем, особенно это касается стыковки Unix и Windows.

Системы Windows 95, 98 и NT имеют в своем составе программу Telnet, которая делает возможным подключение через сеть и интерактивные сеансы работы в системах Unix. Ориентированное на конкретный ПК ПО X Windows обеспечивает возможность для ПК работать подобно рабочей станции Unix и выполнять графические программы Unix. Платформно-независимые средства создания сценариев, такие как Perl и Tel, могут выполняться в системах, работающих под управлением Unix, Windows и MacOS. При этом протоколы совместного использования файлов позволяют Windows-системам просматривать диски системы Unix, и наоборот.

При использовании дополнительных программных средств Windows-система поддерживает сетевую файловую систему (NFS). ПО NFS-клиента для Windows делает возможным для ПК просмотр файлов, сохраняемых на дисках системы Unix (почти каждая версия Unix поддерживает NFS). Если установка ПО сетевого клиента на каждой настольной Windows-системе покажется слишком трудоемким или дорогим делом, то можно установить Windows-ориентированное ПО сервера в системе Unix. Один такой пакет, названный Samba, является бесплатным. С помощью Samba можно получить доступ к дискам, принтерам и даже проводить аутентификацию, точно так же, как предоставляет эти услуги NT-сервер. При этом запросы отрабатываются Unix.

Поскольку Unix поддерживает большинство сетевых протоколов, можно легко конфигурировать Unix-системы в качестве серверов электронной почты для клиентов, работающих в среде Windows. Большинство клиентов электронной почты для Windows поддерживают почтовый протокол POP3.

3.1.2. Администрирование систем Unix в различных средах

Основными задачами системного администрирования являются следующие:

. запуск и остановка системы;

е добавление и удаление учетных записей пользователей;

• защита пользовательских данных от разрушения либо со стороны других пользователей, либо в результате аппаратных сбоев;

• управление и добавление периферийных устройств, таких как диски, принтеры и т.д.;

• поддержка сетевых соединений между системами;

• обеспечение стабильной работы системы и предоставление нужных сервисов.

При обслуживании рабочих сред Unix использует многочисленные системы. При этом некоторые из них управляются Unix, а некоторые — нет.

Задачи, для которых используется каждая отдельная Unix-система, определяют, какой объем системного администрирования потребуют применяемые системы. Например, системы обработки информации в режиме реального времени нуждаются в специальных предупредительных мерах, гарантирующих отсутствие каких-либо перерывов в информационном потоке. В таких системах, как системы мониторинга цен на бирже, даже одноминутный перерыв в обслуживании может повлечь за собой значительные потери.

Если недостаточное планирование и ошибки в реализации механизмов отказоустойчивости приведут к дорогостоящему перерыву в работе системы, то срыв работы дорого обойдется и администратору системы. Вот почему всегда нужно планировать работу в расчете на наихудшее развитие событий. Основной предпосылкой в этом случае должно быть то, что не нужно гадать — произойдет катастрофа или нет, а нужно думать только о том, когда она произойдет. Необходимо проводить мониторинг внешних информационных источников, даже если они и не находятся под нашим контролем, чтобы можно было, по крайней мере, предупредить пользователей о том, что данные будут временно недоступны.

Для определения объемов администрирования необходимо рассмотреть вопросы уровня обслуживания. Пользователи ожидают предоставления им определенного уровня услуг. Если не предоставить им этот уровень услуг, даже если проблема вне вашей компетенции, то очень высоки шансы, что виновным сочтут именно администратора. Например, биржевой маклер, который получает информацию с задержкой, не может работать столь же эффективно, как его коллеги, получающие информацию с точностью до секунды.

В розничной торговле время задержки реакции системы часто означает, что клерк в магазине не может просмотреть данные по складским запасам, которые хранятся в компьютере центрального офиса. Время задержки реакции системы в этом случае может быть связано с состоянием местной системы магазина, состоянием системы центрального офиса либо состоянием канала связи, который их соединяет. Если один из этих элементов откажет, то клерк в магазине лишится обслуживания. В случае отказа подобной системы потенциальная сделка подвергается опасности, потому что отдельные магазины не смогут проверить, имеется ли данная продукция на складе. Вся система должна оставаться полностью работоспособной во время работы магазинов.

В зависимости от количества магазинов, охваченных системой, время ее простоя может оказаться дорогостоящим. Администратору подобной системы нужно продумать общий проект системы. Возможно, нужно найти способ дублирования данных центральной системы на системе каждого магазина (это система с потен-

циалом асинхронного получения данных). Система каждого магазина может поддерживать файл регистрации данных о сделках и передавать все данные в центральный офис в нерабочие часы. Подобный подход решает проблему непрерывности работы магазинов, однако он порождает новые проблемы, например возможность продажи большего количества наименований товара, чем есть на складе. Это заставит покупателя ожидать получения товара дольше, чем будет необходимо в случае, когда товар есть на складе.

Общий проект системы имеет огромное влияние на задачи, которые необходимо решать системному администратору. Если можно повлиять на процесс проектирования всей системы, то нельзя отказываться от этой возможности. Вопросы, связанные с администрированием системы, должны всегда рассматриваться на совещаниях, посвященных разработке системы. Соображения по проекту рассматриваемой системы, которые следует представить, должны охватывать реализацию хорошего резервирования БД, установку реплики сервера БД на случай отказа первичного сервера, а также постоянное поддержание работоспособности каналов связи со всеми потребителями.

Иногда уровень обслуживания становится трудным для реализации. Например, многие компании демонстрируют растущую тенденцию к размещению своих Web-серверов, почтовых серверов, а также других интернет-серверов на ресурсах внешних компаний. В таких случаях контракты, заключаемые между клиентами и компаниями, осуществляющими такое размещение (hosting), часто включают в себя соглашение об уровне сервиса, который должна обеспечивать размещающая компания. Это соглашение определяет такие вопросы, как частота и длительность простоев для проведения регламентных работ, которые должны проводиться в оговоренное время и в указанные даты, количество транзакций в день, которые размещающая компания должна обеспечить при уровне готовности системы в 99,9 %, и другие подобные вопросы. В описанных ситуациях необходимость достижения уровня обслуживания, зафиксированного в таком соглашении, будет непростой задачей. Ключом к успеху в этом случае будет правильное проектирование и соответствующее упреждающее администрирование системы.

Системное администрирование предполагает поддержку работы пользователей с компьютерами. Деятельность пользователей имеет свои особенности в различных средах, соответственно изменяются ваши задачи при поддержке этой деятельности.

Последующие разделы содержат информацию о часто встречающихся типах среды и об их особенностях при администрировании. В табл. 3.2 приведены особенности различных типов сред.

Образование. В среде «образование» системные администраторы имеют дело с большим числом пользователей, причем состав

Таблица 3.2

Особенности различных типов сред

Среда	Особенности для администрирования
Образование	Много пользователей, мало выделенных систем
Инженерные разработки и научные исследования	Графические рабочие станции, управление изменяющимися заказами, управление большими объемами данных, совместное редактирование больших файлов данных, установка экспериментального (часто нестабильно работающего) ПО
Разработка программного обеспечения	Защита исходного кода, управление различными версиями файлов, поддержка нескольких различных версий Unix
Системы управления предприятием	Своевременный доступ к данным
Финансы	Управление транзакциями, своевременное выполнение транзакций, обеспечение доступа к информации
Интернет-провайдеры	Проблемы соединений (иногда отсутствие соединения), защита, типичная для Интернета, работа с различными типами пользователей, поддержка начинающих пользователей

пользователей часто меняется. Они должны выделить несколько главных направлений, на которых следует сосредоточить внимание.

Колледжи и университеты часто имеют свои компьютерные центры. Как правило, это комнаты, в которых находятся терминалы и компьютеры, подключенные к сети. Иногда можно найти рабочие станции на базе Unix. За пользователем не закреплен определенный компьютер, и обычно он каждый раз регистрируется в системе с другой машины. В этом среда учебных заведений отличается от офисной среды, где у каждого сотрудника есть постоянное рабочее место с персональным компьютером или терминалом.

В некоторых университетских городках (кампусах) каждая комната в общежитии обеспечивается доступом к Интернету.

Как бы ни была организована работа с компьютерами в университете или колледже, администратор сети будет иметь дело с большим числом пользователей, работающих на разных машинах. Поэтому придется ограничивать объем дискового пространства, доступный пользователю.

Большинство пользователей работают с ресурсами недолгое время. Студенты приходят, прослушивают курсы и уходят. Каждую осень приходят новые студенты и их приходится регистрировать в системе. В конце семестра некоторые институты и колледжи аннулируют права доступа студентов к ресурсам. Это означает дополнительную работу для администратора. С началом нового семестра у него снова появляется много работы, поскольку необходимо зарегистрировать много новых пользователей.

Как среди преподавателей, так и среди студентов существуют пользователи, не знакомые с компьютерами. Администратору придется потрудиться, проверяя, все ли пользователи знают, как входить в систему, и помогая преподавателям рассылать расписание занятий.

Среди пользователей, особенно студентов, есть и такие, которые очень хорошо знают систему и имеют много свободного времени, чтобы экспериментировать с ней. Это дает некоторые преимущества, поскольку не исключено, что эти студенты помогут администратору с установкой программ. Но это чревато неприятными последствиями, поскольку программы, небрежно написанные, могут поставить под угрозу безопасность системы.

Поскольку большинство колледжей и университетов обучают студентов различным специальностям, администратору придется работать с разнообразным ПО, связанным с общественными и естественными науками, математикой, театром, живописью, музыкой и спортом. Методология свободного распространения ПО для Unix позволит ему удовлетворить интересы пользователей. Если он будет искать в Интернете новые программы и интересные данные и копировать их на сервер, то его популярность среди пользователей возрастет.

В настоящее время почти все университеты и колледжи подключены к Интернету. Большинство из них поддерживают Web-серверы, и поэтому очень много студентов и сотрудников университета имеют возможность создавать свои Web-страницы. В этом случае у администратора могут возникнуть проблемы, связанные с содержимым Web-узлов, особенно если содержание документов оскорбляет чувства других пользователей. К тому же студенты могут скопировать на компьютер учреждения материалы, содержащие запрещенную информацию. Поскольку это является нарушением законодательства, ответственность за эти материалы несет учреждение, на узле которого они расположены. Поэтому такую ситуацию лучше не допускать.

Инженерные разработки и научные исследования. Инженерная и научная среда характеризуется большим числом рабочих мест и тенденцией к использованию графических ресурсов. Это ставит перед системным администратором несколько специфических задач.

Пользователи, занимающиеся инженерными разработками и научными исследованиями, работают с огромным количеством данных. Это могут быть, например, файлы с результатами компьютерного проектирования (CAD-файлы), графики сейсмической активности, данные о воздушных потоках, измерения высоты подъема самолета и т.д.

Администратору придется управлять рабочими станциями с объемом оперативной памяти до 640 Мбайт и со многими гигабайтами дисковой памяти. Поскольку пользователи имеют дело с большими объемами данных, они часто хранят их на совместно используемых устройствах, доступных по сети. При этом резко возрастают требования к качеству сетевой связи.

В рассматриваемой среде пользователи обычно работают на рабочих станциях. Многие из них используют операционную систему Unix, однако в последнее время все большее количество рабочих станций работают под Windows NT.

В среде Unix графические рабочие станции обычно используют систему X Window. Для решения задач трехмерной графики и визуализации требуются высокоуровневые графические системы. Как правило, для решения подобных задач используется такое ПО, как OpenGL компании Silicon Graphics или PEX, 3Э-расширение системы X Window. В последние годы OpenGL доминирует на рынке 3О-систем, тогда как PEX теряет свои позиции.

Знание X Window обязательно для администратора. Необходимо хорошо себе представлять, что надо делать, например, чтобы разрешить доступ к экрану пользователя с удаленной системы с помощью команд xhost или xauth.

Разработка программного обеспечения. Администрирование в среде разработки ПО характеризуется многофункциональными действиями. С самого начала система Unix создавалась как платформа для разработки ПО. Это объясняет популярность данной системы среди разработчиков программ. Со времени своего создания по настоящее время решения, заложенные в основу Unix, продолжают быть востребованными у программистов.

Подобно среде для инженерных разработок и научных исследований, среда разработки ПО обычно представляет собой набор рабочих станций и серверов под управлением Unix. Основные языки программирования: C, C++ и Java. Другие языки, такие как Fortran, Pascal и другие, также используются, но, как правило, средства их поддержки продаются отдельно.

Программное обеспечение состоит, в первую очередь, из текстовых файлов, содержимое которых называется исходным кодом. Эти файлы затем преобразуются в рабочие программы. Программы, написанные на языках C и C++, компилируются в машинный код и компонуются с библиотеками стандартных подпрограмм. Данная среда имеет ряд специфических особенностей.

В результате широкого распространения различных архитектур системы Unix создалась ситуация, когда ни одна из платформ не доминирует над другими. Чтобы не проиграть в конкурентной борьбе, компании, выпускающие ПО, должны поддерживать различные архитектуры.

Поскольку исходный текст программ, написанных на языках C и C++, преобразуется в машинный код, разработчики ПО компилируют свои программы в различных версиях Unix, а также в системах Windows и Macintosh. Для администратора это означает, что ему не удастся организовать свою деятельность так, чтобы работать с одной версией Unix и одним типом системы.

Наличие разнообразных версий Unix означает дополнительную работу для администратора. Чтобы сократить количество различных типов систем, которые приходится поддерживать, надо снабдить всех разработчиков ПО рабочими станциями одного типа, например Sun SPARC. В этом случае работать с системами других производителей будут только сотрудники, занимающиеся переносом 110.

Программы, созданные на языке Java, компилируются в файлы .class, содержащие переносимый байтовый код Java. Это значит, что скомпилированное Java-приложение может работать на различных архитектурах. Некоторые компиляторы Java позволяют компилировать исходный текст программы в машинный код. Такое Java-приложение ведет себя так же, как и приложения C и C++, и должно специально подготавливаться для каждой поддерживаемой архитектуры.

Умение работать с Perl и оболочкой Unix помогает администратору управлять приложениями на различных платформах.

Независимо от используемого языка программирования жизненный цикл любого ПО начинается с исходных текстовых файлов. Большое приложение может содержать сотни (если не тысячи) отдельных файлов, которые, как правило, расположены в одном поддереве системы каталогов. Если приложение достаточно велико, то его текстовые файлы, а также скомпилированные объектные модули и библиотеки будут совместно использоваться несколькими разработчиками.

Большинство инструментов, используемых ПО, предназначено для работы с файлами. В число этих инструментов входят компиляторы, которые превращают исходный код в скомпилированный машинный или байтовый код, текстовые редакторы в которых создаются и редактируются файлы исходного кода, а также редакторы связей, которые компонуют скомпилированный код в исполняемую программу.

Unix обеспечивает средства для работы с файлами. Возможно, понадобится монтировать диски с помощью NFS для того, чтобы разработчики ПО имели совместный доступ к файлам со своих

рабочих станций. Средства автоматического монтирования позволяют пользователю получать доступ к своим файлам с различных систем.

Разработка ПО создает нагрузку сети, дисковой и оперативной памяти. Такие инструменты, как, например, отладчики, которые позволяют разработчикам обнаруживать ошибки, используют большой объем RAM. В основном это происходит из-за того, что в отладчиках поддерживается соответствие между исполняемым машинным кодом и исходным кодом.

Другие инструменты, например популярный текстовый редактор emacs, также требуют много оперативной памяти и создают большую нагрузку на центральный процессор.

Многие инструменты, предназначенные для разработки ПО (например, emacs), распространяются свободно. Разработчики ПО используют многие из этих средств, поэтому вам придется обновлять, компилировать, устанавливать их и заниматься их поддержкой. В некоторых организациях поддерживается внутренний Web-сервер, хранящий информацию для разработчиков программ.

Компиляторы, за исключением продуктов семейства GNU (например, gcc), как правило, являются коммерческими инструментами. Часто для того, чтобы такой инструмент мог работать, на узле должен быть запущен сервер лицензирования.

В отличие от других типов среды в среде разработки программ системному администратору, как правило, не приходится заниматься обновлением ОС. В данной среде подобные работы существенно зависят от цикла разработки продукта. Обычно в течение работы над выпускаемым продуктом доработка системы не приветствуется либо вовсе запрещается. Это означает, что установка обновлений ОС будет запаздывать на год или даже больше. Это создает для администратора новую проблему — ему приходится заниматься поддержкой старого ПО. Производители компиляторов и ОС обычно ставят условие, согласно которому поддержка продукта проводится только в том случае, если будут вовремя устанавливаться дополнения к системе. Сделать это в условиях разработки ПО часто невозможно. Иногда продукт, разработанный для старой версии ОС, отказывается работать на обновленной системе. В этом случае продукт необходимо пересобирать, а это значит, что заказчикам тоже придется обновлять систему. Если постоянные обновления системы являются условием заказчика, то в этом случае у вас не остается выбора.

Поскольку создание любого приложения начинается с написания его исходного кода, текстовые редакторы представляют собой важный инструмент, используемый при разработке. Каждый разработчик отдает предпочтение определенному текстовому редактору, работая с которым он чувствует себя комфортнее. Часто используются такие редакторы, как emacs, xemacs и известный

всем vi, а также редакторы с графическим интерфейсом, такие как nedit, tkedit, редактор SoftBench производства Hewlett-Packard и т.д. Многие из этих редакторов свободно распространяются через Интернет.

Текстовые редакторы emacs и xemacs очень похожи. Оба редактора поддерживают интерфейс X Window, но они делают это по-разному. Неопытный пользователь не заметит разницы, поскольку эти редакторы имеют близкие названия и похожий интерфейс. Однако специалист отметит значительную разницу между этими редакторами.

Для любой компании, производящей ПО, главной ценностью является исходный код продуктов. При этом огромное значение имеют защита и контроль исходного кода, управление версиями.

Большинство разработчиков ПО используют специальные инструменты, предназначенные для управления его версиями. Эти инструменты дают возможность вернуться к ранним этапам разработки продукта и исключить изменения, которые стали источником проблем. К подобным инструментам относятся SCCS, RCS, CVS (Concurrent Version System), ClearCase разработки PureAtria и Perforce фирмы Perforce.

Все эти инструменты помогают обнаружить, кто изменил исходный код, когда внесены изменения и что именно изменено. Все они позволяют вернуть исходный код в то состояние, в котором он был до изменения.

Системы управления предприятием. Администрирование в ИС управления предприятием является наиболее важной и практичной средой функционирования любой системы. На предприятиях основное внимание уделяется обработке информации. Это значит, что системному администратору придется много работать с данными.

Существует множество самых различных корпораций, однако у них есть одна общая черта — системы предприятий в основном работают с данными. Администрируя систему управления предприятием, необходимо поддерживать один или несколько серверов баз данных, таких как Oracle или Informix. Возможно, придется также иметь дело со специальным ПО, предназначенным для аналитической обработки данных (On-line Analytical Processing — OLAP). Использование таких программ сокращает процесс обучения пользователей и предоставляет им новые средства для поиска данных.

В среде предприятия многие пользователи работают на персональных компьютерах под управлением ОС Windows. Эти компьютеры выступают в роли клиентов для серверов Unix, предоставляющих доступ к данным.

Чтобы защитить данные от неизбежных сбоев аппаратуры, необходимо иметь устройство типа RAID (Redundant Array of

Inexpensive Disks — избыточный массив недорогих дисков). Системы RAID обычно дорогостоящие и различаются в зависимости от требуемой надежности уровнем избыточности.

Пользователи, которые принимают ответственные решения, могут использовать ПО, которое помогает им принимать эти решения. Это программы, с помощью которых удобно прослежи-иать возможные направления и тенденции в бизнесе. В промышленном секторе компьютерные модели используются для уменьшения объема данных, необходимых пользователю для предска-занйя потребностей и контроля доставки.

Главной задачей администратора будет обеспечение своевременного доступа к данным. Отсутствие доступа чревато серьезными потерями для корпорации.

В среде предприятия очень пригодятся любые продукты, повышающие надежность, например устройства RAID, бесперебойные источники питания (Universal Power Supplies — UPS), которые помогают бороться с внезапными отключениями энергии, а также высокоэффективные системы Unix. Хорошим примером использования этих продуктов могут быть компании, занимающиеся финансовой деятельностью.

Финансы. Администрирование в финансовой среде имеет много специфических особенностей. Финансовые учреждения, банки, биржи и фондовые организации больше других нуждаются в падежной системе, работающей без сбоев.

Простои системы могут нанести огромный ущерб. Наличие устойчивой связи имеет огромное значение для биржевых брокеров, финансовых менеджеров и других подобных категорий пользователей. Им нужна оперативная информация, и они терпят большие убытки, когда лишены доступа к ней. Поэтому сотрудники, управляющие деловыми транзакциями, часто держат на столе два или несколько мониторов, которые обеспечивают доставку информации из разных источников. Совмещение дан-пых из этих источников в одной многооконной системе позволяет выводить информацию на один монитор, а это, в свою очередь, освобождает место на столе и обеспечивает более эффективную работу.

Иногда деятельность финансовых организаций определяется специальными правительственными требованиями. В частности, могут существовать правила, регламентирующие архивирование данных и время транзакций (например, аннулирование счетов в течение определенного времени). В этих условиях к системам предъявляются еще более жесткие требования, связанные с доступом к данным.

Интернет-провайдеры. Администрирование при работе с интернет-провайдерами должно учитывать особенности работы с Интернетом. В начале развития Интернета в глобальной сети исполь-

зовалась только система Unix, поэтому в настоящее время большинство серверов являются Unix-серверами.

В обслуживании пользователей Интернета часто упоминается операционная система Windows, не принадлежащая к семейству Unix. Поскольку многие пользователи работают в среде Windows, они применяют эту систему для взаимодействия с интернет-серверами. Чтобы управлять системой интернет-провайдера, администратору придется изучить не только Unix. Многие пользователи не умеют работать с сетью, модемом и Интернетом, поэтому приходится тратить много времени на их обучение и предоставление консультаций.

Для того чтобы управлять системой провайдера, необходимо научиться работать в условиях постоянной нехватки ресурсов. Работа с сетью требует большого количества компьютерных ресурсов и приходится искать способы сделать как можно больше с помощью существующей системы.

Интернет-провайдеры предоставляют услуги другим узлам и подключают к глобальной сети пользователей, которые раньше не имели к ней доступа. Они предоставляют следующие основные сервисы:

- подключение по коммутируемой линии. Для подключения к серверу Unix пользователи используют модем и телефонную линию. В большинстве случаев на машине пользователя установлена операционная система Windows (Unix встречается реже). Поэтому администратор обязан свободно ориентироваться в среде Windows, уметь работать с соединениями по коммутируемой линии и протоколом PPP, который чаще всего используется для установления такого соединения;
- работа с Web. Пользователи могут просматривать Web-страницы на своих компьютерах;
- e-mail. Работа с почтой поддерживается посредством сетевых протоколов, таких как POP3, IMAP и SMTP. Работа с почтой на пользовательских компьютерах под управлением Windows отличается от традиционного способа взаимодействия с почтой в системе Unix. При работе в Windows пользователь подключается к почтовому серверу и копирует сообщения на свой компьютер. Подобное взаимодействие поддерживается большинством Web-броузеров, в частности программой Netscape Navigator;
- FTP. Пользователи загружают файлы из сети на свой компьютер. ОС Windows, под управлением которой работает большинство персональных компьютеров, содержит клиент-программу ftp.exe;
- размещение Web-узлов. Пользователи имеют возможность размещать свои Web-узлы на сервере Unix. Чтобы Web-страницы были доступны из Интернета, необходимо установить и поддерживать Web-сервер. Многие провайдеры ограничивают дисковое простран-

ство, которое отводится для персональных или корпоративных Web-страниц;

• доступ через оболочку. В этом режиме пользователи входят в систему посредством Telnet (Windows содержит клиент-программу telnet.exe). Многие запрещают этот тип доступа из соображений безопасности;

• группы новостей Usenet. Доступ к данному сервису осуществляется через Web-броузер или с помощью специального средства просмотра новостей, например программы FreeAgent, работающей в среде Windows;

• прочие интернет-протоколы. Участие в chat-группе. Здесь необходимо учесть, что пользователь может побеседовать с любым безымянным пользователем, который готов представиться кем угодно, но только не тем, кто он есть на самом деле.

Некоторые серверы обеспечивают не полный объем интернет-услуг, а лишь доступ к Web. Как правило, Web-страницы содержат большое число графических изображений, поэтому от администратора потребуется поддержка приложений для создания Web-документов.

Конкуренция между крупными компаниями, такими как AT&T, America Online и другие, привела к тому, что многие провайдеры стали использовать бесплатные версии Unix и Web-серверов.

Свободно распространяемые версии Unix, такие как Linux (www.linux.org), FreeBSD (www.freebsd.org) и NetBSD (www.netbsd.org), представляют собой полноценные ОС, распространяемые по очень низкой цене или бесплатно. Проблемой для администратора может стать сопровождение этого ПО. Можно заключить договор с компанией, специализирующейся на поддержке этой ОС, или искать необходимые сведения в Интернете. Перечисленные ранее ОС создавались сотнями разработчиков со всего мира, которые вносили и продолжают вносить свой вклад в их развитие. Часто бывает так, что проблему, возникшую при работе с Linux, удается решить быстрее для коммерческой версии Unix. Дополнительно к свободному распространению различные компании продают коммерческие версии этих версий, обеспечивая их поддержку. Caldera (www.caldera.com) — одна из организаций, поставляющих коммерческую версию Linux.

Как Linux, так и NetBSD работают на компьютерах архитектуры Intel, а также на некоторых системах RISC, таких как Alpha, SPARC и PowerPC. Эти системы применяют известные коммерческие предприятия, например Yahoo! использует FreeBSD.

Среди Web-серверов Apache (www.apache.org) занял лидирующую позицию, оставив далеко позади конкурирующие продукты, выпущенные Netscape, Microsoft и другими производителями. Apache распространяется бесплатно и работает на большинстве версий Unix, а также на Windows NT.

3.2. Архитектура средств администрирования Windows 2000

Windows 2000 содержит различные средства администрирования компьютеров в сети. Службы терминалов (Terminal Services) предоставляют клиентам доступ к Windows 2000 и Windows-приложениям. Путем терминального доступа администраторы могут удаленно администрировать сетевые ресурсы. Кроме того, Windows 2000 содержит протокол SNMP, который используется для мониторинга и обмена информацией между агентом SNMP и программой управления сетью.

Windows 2000 предоставляет средства локального и удаленного администрирования. Удаленное администрирование подразумевает подключение к компьютеру через сеть для выполнения административных задач. Это позволяет администратору централизованно управлять несколькими компьютерами вместо того, чтобы отдельно настраивать каждый компьютер. Для удаленного администрирования разрешается применять программы сторонних разработчиков или средства из состава Windows 2000.

При включении служб терминалов на компьютере Windows 2000 Server необходимо выбрать один из двух режимов: Application Server (режим сервера приложений) или Remote Administration (режим удаленного администрирования).

Режим сервера приложений позволяет запускать приложения и управлять ими с удаленного компьютера. Интерфейс Windows 2000 и Windows-приложения можно предоставить компьютерам, которые не могут работать в этой ОС. Так как службы терминалов являются встроенным продуктом Windows 2000, разрешается запустить приложение на сервере и предоставить пользовательский интерфейс клиенту, который не может работать в Windows 2000, например компьютеру с Windows 3.11 или Windows CE, подключенному к серверу терминалов.

Для доступа, управления и исправления ошибок клиентов службы терминалов предоставляют *режим удаленного администрирования.* Режим удаленного управления служит для удаленного администрирования серверов Windows 2000 через любое ТСРДР-со-единение, в том числе через удаленный доступ, Ethernet, Интернет, беспроводные сети, ГВС и виртуальные частные сети (VPN). Службы терминалов устанавливаются как один из компонентов Windows.

Использование сервера терминалов имеет большое значение при администрировании системы Windows.

Хотя соединение Remote Desktop Protocol (RDP) автоматически настраивается при установке службы терминалов, можно создать новое подключение. Для каждого сетевого адаптера на сервере терминалов разрешается настроить только одно подключе-

ние, однако можно настроить дополнительные подключения RDP, установив сетевой адаптер для каждого подключения компьютера. Осуществлять подключение необходимо в следующей последовательности:

1) раскройте меню Start \Programs\Administrative Tools и щелкните мышью по ярлыку Terminal Services Configuration *(Настройка служб терминалов);*

2) щелкните правой кнопкой мыши по папке «Connections» («Подключения») и выберите в контекстном меню команду Create New Connection *(Создать подключение).* Откроется окно мастера Terminal Services *Connection (Мастер подключения к службам терминалов);*

3) щелкните по кнопке *Next;*

4) в первом окне мастера укажите тип подключения, например Microsoft RDP 5.0, и щелкните по кнопке Next;

5) выберите уровень шифрования: Low, Medium или High («Низкий», «Средний» или «Высокий»). Можно также задать обычную проверку подлинности Windows. Щелкните по кнопке *Next;*

6) задайте параметры и уровень удаленного управления и щелкните по кнопке *Next;*

7) укажите имя подключения, тип протокола, комментарий и щелкните по кнопке *Next;*

8) выберите один или несколько сетевых адаптеров для данного типа протокола, задайте допустимое количество подключений и щелкните по кнопке *Next;*

9) щелкните мышью по кнопке *Finish.*

Службы терминалов поддерживают не более двух параллельных подключений в режиме удаленного администрирования, которые не требуют лицензии. Клиенты службы терминалов потребляют минимальное количество системных ресурсов.

Предоставление доступа к серверу терминалов необходимо выполнять в следующем порядке:

1) раскройте меню Start\Programs\Adminisirative Tools и щелкните мышью по ярлыку Computer Management *(Управление компьютером);*

2) раскройте узел System Tools\Local Users And Groups\Users (*Служебные программы\Локальные пользователи и группы\Пользова-тели);*

3) дважды щелкните мышью по объекту пользователя, которому надо предоставить доступ;

4) на вкладке Terminal Services Profile пометьте флажок «Allow Logon To Terminal Server» и щелкните по кнопке *О К;*

5) закройте оснастку Computer Management;

6) раскройте меню Start\Programs\Administrative Tools и щелкните мышью по ярлыку Terminal Services Configuration;

7) в папке «Connections» («Подключения») выберите Rdp-Tcp;

Рис. 3.2. Схема взаимодействия SNMP и агентов

8) в меню Action *(Действие)* выберите команду Properties (*Свой ства);*

9) выберите вкладку Permissions *(Разрешения)* и добавьте пользователя или группу, который должен иметь разрешения для доступа к данному серверу терминалов;

10) щелкните мышью по кнопке *О К;*

11) закройте окно Terminal Services Configuration.

Для администрирования ИС в Windows широко используется протокол SNMP. Он предназначен для управления сетью и широко применяется в TCP/IP-сетях. На его основе взаимодействуют программа управления, запушенная администратором, и програм-ма-агент, выполняемая на узле или шлюзе. Протокол SNMP также применяется для мониторинга и управления узлами и шлюзами при работе в Интернете. Служба Microsoft SNMP позволяет выполнять удаленный мониторинг компьютера с Windows 2000; она обрабатывает запросы с одного или нескольких узлов и отправляет информацию об управлении сетью узлам дискретными блоками, называемыми ловушками. После установки службы SNMP утилита Performance Monitor позволяет проверить счетчики производительности TCP/IP.

Этот протокол можно установить и использовать на любом компьютере Windows 2000 с протоколами TCP/IP или IPX/SPX.

Рис. 3.3. Схема системы управления агент SNMP—-служба SNMP

Служба SNMP состоит из систем управления и агентов. Под системой управления подразумевается любой компьютер, на котором выполняется управляющее ПО SNMP. Windows 2000 не содержит систем управления, однако множество продуктов сторонних разработчиков, например Sun Net Manager или HP Open View, разработано специально для этого. Система управления запрашивает информацию у агента.

Установку службы SNMP нужно производить в следующей последовательности:

1) раскройте меню Start\Settings\Control Panel, щелкните мышью по ярлыку Add/Remove Programs и в открывшемся окне щелкните по кнопке Add/Remove Windows Components. Откроется окно мастера компонентов Windows;

2) в перечне компонентов выберите «Management And Monitoring Tools» («Средства наблюдения и управления») и щелкните по кнопке Details *(Состав).* Откроется диалоговое окно Management And Monitoring Tools;

3) пометьте флажок «Simple Network Management Protocol» и щелкните по кнопке *OK;*

4) в окне мастера компонентов Windows щелкните по кнопке *Next.* Мастер установит протокол SNMP;

5) щелкните мышью по кнопке *Finish.*

Под агентом подразумевается любой компьютер с Windows 2000, маршрутизатор или концентратор, на котором выполняется программа-агент SNMP (рис. 3.2). Служба Microsoft SNMP содержит только ПО агента, основная функция которого заключается в выполнении команд системы управления.

Агент Microsoft SNMP позволяет удаленно управлять компьютером с Windows 2000. Агент инициирует только ловушку (trap). *Ловушка* — это сообщение о возникновении на узле некоторого события, переданное системе управления. Программа управления SNMP не обязательно должна выполняться на том же компьютере, что и агент SNMP.

Схема системы управления агент SNMP —служба SNMP приведена на рис. 3.3.

Средствами диспетчера SNMP можно выполнить мониторинг серверов DHCP, Internet Information Server или WINS. Кроме того, после установки службы SNMP утилита Performance Monitor позволяет просмотреть показания счетчиков производительности TCP/IP: ICMP, TCP, IP, UDP, DHCP, WINS, FTP, Network Interface и Internet Information Server. Утилита Performance Monitor подсчитывает:

- активные TCP-соединения;
- UDP-дейтаграммы в секунду;
- ICMP-сообщения в секунду;
- число байт в секунду, проходящих через интерфейс.

3.3. Архитектура ОС Unix и ее администрирование 3.3.1.

Файловая система и ее компоненты

Для обеспечения такого высокого уровня совместимости приложений Unix предоставляет согласованный набор услуг и интерфейсов, функционирующих строго определенным образом, независимо от того, работаете ли вы на персональном компьютере или на многопроцессорном суперкомпьютере, поддерживающем тысячу пользователей. ОС Unix является переносимой; она допускает перестройку самой себя и перенос на новую платформу в течение месяцев. На рис. 3.4 показана обобщенная схема архитектуры ОС Unix.

Хотя ОС Unix можно перенести почти на любую платформу, это не значит, что приложения и команды для одной системы Unix обязательно совместимы на уровне машинных кодов с другой системой. Часто новые пользователи думают, что если Unix работает на компьютере с процессором архитектуры 68040, то она обязательно будет работать и на PowerPC или на модели 1386, либо на компьютере, основанном на RISC-микропроцессорах. Программы на языках С и С++ и большинство сценариев действительно переводятся и перекомпилируются, подстраиваясь под новую архитектуру, но файлы, содержащие двоичный код, отличаются и их нельзя просто переместить из одной архитектуры в другую.

Файлы — это неотъемлемая часть системы Unix. Пользователь получает доступ к программам и данным (даже к аппаратным устройствам) посредством файлов. Ему система Unix покажется обратной древовидной структурой каталогов и файлов, по которой легко проходить и работать. Можно отметить внешнее подобие файловой системы Unix и других файловых систем, используемых, например, системой MS DOS, но при ближайшем рассмотрении окажется, что это подобие только внешнее. Тем не менее при хорошем знакомстве с DOS можно быстро освоить успешное использование файловой системы Unix.

На рис. 3.5 изображена часть дерева каталогов системы Unix. Корневой узел дерева всегда обозначается символом «/» (этим символом обозначается корневой каталог). В отличие от MS DOS, в которой есть отдельные названия дисков (A, B, C и т.д.), ваша система Unix определяет местоположение любого файла по отно-

Рис. 3.4. Обобщенная схема архитектуры ОС Unix

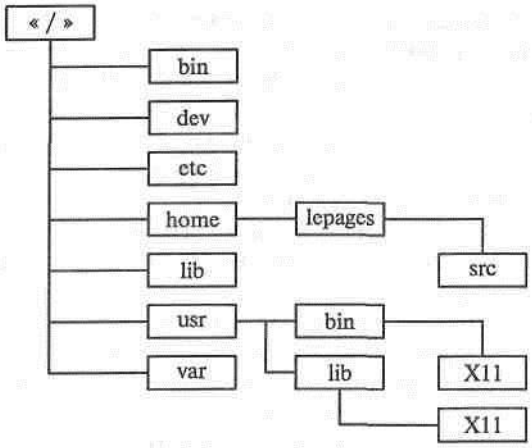


Рис. 3.5. Дерево каталогов системы Unix

шению к корневому каталогу (/). Дополнительные диски и разделы диска присоединяются к файловой системе в точке монтирования. Точка монтирования — это просто название каталога на основном диске, в котором находится корневой раздел (или, в некоторых случаях, в другой файловой системе вне корневого каталога). Например, у вас есть отдельный жесткий диск для учетной записи пользователей системы. Вам необходимо вызвать команду mount для монтирования этого диска в соответствующем месте в файловой иерархии системы Unix, такой как /home/users. Таким образом, путь /home/users/iarrera/-.profile фактически указывает на файл, находящийся на втором диске; файловая система этого диска смонтирована на /home/users, а подкаталоги /home/ users находятся на втором диске.

Можно расширить этот прием. Если каждый пользователь имеет собственный компьютер под управлением Unix, то можно поместить рабочий каталог пользователя, например /home/users/ iarrera, на собственном компьютере пользователя, а потом смонтировать этот каталог на всех других компьютерах. Таким образом, каждый пользователь может начинать работу на любом компьютере и пользоваться всегда одним и тем же рабочим каталогом. Для выполнения этого необходима NFS (Network File System — сетевая файловая система).

Система Unix поддерживает много различных типов файловых систем (в зависимости от используемой версии). Независимо от типа файловой системы, к которой есть доступ, все файловые системы смонтированы в корневом узле. Переход от файловой системы одного типа к файловой системе другого типа незаметен для пользователя и не требует, с точки зрения пользователя, ни-

каких семантических изменений. Имеете ли вы доступ к смонтированному диску с NFS или с DOS, разделы диска представляются вам в качестве одной единообразной файловой системы. Таким образом, несмотря на то, что файловые системы показаны пользователю в одной иерархической древовидной структуре, их внутреннее представление может быть различным. Собственная файловая система Unix состоит из нескольких различных компонентов.

Понимание этих компонентов и того, что они делают, необходимо при конфигурировании дисков. На рис. 3.6 схематично показаны компоненты файловой системы.

Первый компонент файловой системы известен как блок начальной загрузки. За этим блоком зарезервировано место в самом начале файловой системы. В корневом узле этот блок содержит фрагмент двоичного кода, загружающий ОС при запуске системы. В других файловых системах блок начальной загрузки, вероятно, будет незанятым. Независимо от того, используется этот блок или нет, он есть в каждой файловой системе.

Суперблок содержит информацию о максимальном количестве файлов, которые система может хранить на диске (перечень i-уз-лов, inode table), размер файловой системы, оставшееся количество свободных i-узлов и информацию о количестве и расположении свободного места. Этот сектор диска периодически обновляется при изменениях в файловой системе.

Для успешной работы с файловой системой Unix в стыковке с файловой системой MS DOS/ Windows необходимо учитывать следующие рекомендации и указания:

1) необходимо перемещаться по обеим файловым системам с помощью команды cd (от *англ.* change directory — сменить каталог);

2) в обеих файловых системах используются символы «.» и «..» для обозначения текущего и вышестоящего каталогов соответственно;

3) в системе Unix имя пути файла разделяется символом «/». В MS DOS для этой цели используется символ «\»;

4) каталоги в обеих системах создаются командой mkdir;

Рис. 3.6. Схема компонентов файловой

5) в системе Unix различаются прописные и строчные буквы в именах файлов. Например, имена fubar, Fubar и FUBAR указывают на три различных файла. В DOS все они относятся к одному файлу, поскольку DOS не различает регистры;

6) файловая система Unix не маркирует различные накопители информации. Дисководы и дополнительные жесткие диски «смонтированы» на подкаталоги корневого раздела основного жесткого диска;

7) по сравнению с DOS установки атрибутов файлов в системе Unix обширнее. DOS поддер-

живает атрибуты «только чтение», «архивный», «скрытый» и «системный», а система Unix иначе управляет правами доступа к файлам. Они устанавливаются отдельно для владельца файла, группы, к которой принадлежит владелец, и всех остальных пользователей, не относящихся к группе владельца файла;

8) в отличие от файловой системы MS DOS Unix поддерживает длинные имена файлов. Операционные системы Windows 95, 98, 2000, CE и NT поддерживают длинные имена файлов, а система Windows 3.1 (просто графическая оболочка для MS DOS) и собственно MS DOS — нет;

9) несмотря на то что система Windows поддерживает пробелы в длинных именах (большинство программ, например, расположены в каталоге \Program Files), при использовании системы Unix вы никогда не должны использовать пробел в имени файла (вы можете создать файл с пробелами в имени, но лучше этого избегать);

10) не существует никаких ограничений относительно символов, разрешенных в именах файлов системы Unix. Годен любой из символов ASCII, включая управляющие и групповые символы («*», «?», «.» и т.д.). Следовательно, не существует понятия расширения файла, за исключением выбранного вами для включения в имя файла.

Изменения в файловой системе не записываются на диск немедленно. Вместо этого они вносятся в копию суперблока в памяти, которая периодически записывается на диск. Именно данная стратегия обеспечивает высокое быстродействие. Административные расходы на поддержание данной информации на диске привели бы к значительному ухудшению производительности системы, вызванному большим количеством пользователей и процессов, постоянно обновляющих и манипулирующих с файлами.

Если же система выйдет из строя, когда суперблок не синхронизирован с копией, находящейся в памяти, то при следующем монтировании файловой системы он должен быть восстановлен, прежде чем файловой системой можно будет пользоваться. Система хранит на диске многочисленные копии суперблока для облегчения восстановления файловой системы в случае сбоя в системе и повреждения суперблока. На рис. 3.7 представлена функциональная схема суперблока Unix.

Перечень i-узлов создается и запоминается на диске в момент формирования файловой системы. Этот перечень содержит все i-узлы, существующие в файловой системе. Размер данного перечня постоянный и вычисляется или устанавливается системным администратором при форматировании раздела. При любом обращении к файловой системе i-узлы являются отправной точкой.

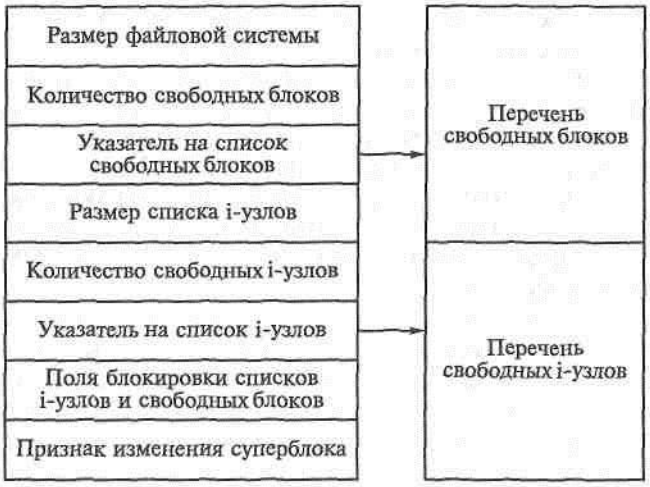


Рис. 3.7. Функциональная схема суперблока Unix

Каждому файлу на диске присвоен только один i-узел, который определяется уникальным номером. Это означает, что число файлов, которые могут храниться в файловой системе, ограничено количеством i-узлов в перечне.

Данные файлов запоминаются на диске в области данных. Эта область разбита на логические блоки, выделяющиеся файлам по мере необходимости. В процессе создания файловой системы, в зависимости от предполагаемого ее использования, при форматировании раздела можно выбрать размер логического блока.

Применяют несколько основных вариантов. Большие размеры блоков области данных направлены на уменьшение количества обращений к дискам при чтении файла. В то же время, если средний размер файлов вашей системы небольшой (например, вы поддерживаете файловую систему, хранящую статьи конференций), то будет растрачиваться большой объем дискового пространства, поскольку средний размер файлов меньше размерор блока.

Обычный размер блоков области данных — 4 или 8 Кбайт (эти стандартные значения приемлемы для большинства целей). Некоторые файловые системы, такие как Berkeley Fast File System, позволяют вам назначать размер фрагментов. В этом случае операционная система распределяет дисковое пространство между фрагментами, а не между блоками. Это уменьшает объем растрачиваемого дискового пространства, поскольку различные файлы могут хранить данные в одном блоке, но при этом сохраняются выгоды использования блоков большого размера.

Ранее мы рассматривали i-узлы и то, каким образом i-узлы служат средством для доступа к файлам в файловой системе, но не объясняли, что такое i-узлы. Каждый i-узел содержит информацию о владельцах файла, включая имя пользователя и группы, а также права доступа к файлу. Также в i-узле хранится тип файла; время создания, открытия и изменения файла; размер файла; количество связей; список указателей на местонахождение области данных файла. На рис. 3.8 показана структура i-узла Unix.

Хотя i-узел существует отдельно от файла, без него нельзя найти данные файла. Доступ к файлам получается с помощью их i-узлов, которые определяются своими номерами. На рис. 3.8 нет поля, определяющего имя файла. Только благодаря каталогам становится возможной связь имени файла с соответствующим i-узлом.

В каждой файловой системе существует один i-узел, называемый корневым (root) i-узлом (см. рис. 3.5). Этот i-узел является точкой монтирования, куда файловая система монтируется командой mount. После ее монтирования вся иерархия файловой системы становится доступной через каталог.

Каталог содержит пары соответствий «имя файла — i-узел» для всех элементов каталога. Процедуры ввода-вывода файла получают номер i-узла от каталога, когда определяется имя файла. Это соответствие имени файла и i-узла в каталоге, содержащем файл, называется *связью.* В результате такого способа запоминания имени становится возможной поддержка многочисленных связей файла путем создания различных элементов каталога или могут быть различные элементы в разных каталогах, указывающие на один и тот же i-узел. Посмотреть перечень i-узлов файла можно с помощью команды Is с ключом i. Схема процедуры нахождения данных файла представлена на рис. 3.9. При этом используются указатели блока данных.

Указатели блока данных являются оглавлением таблицы данных файлов. Количество позиций данного списка также свидетельствует о максимальном размере файла, поддерживаемом файловой системой, имеющей постоянный размер блока.

Существуют два основных типа блочных указателей: прямые и косвенные. Прямой блочный указатель описывает блок в системной области данных, который содержит данные файла, тогда как косвенный блочный указатель описывает блок данных, содержащий указатели на другие блоки данных в области данных, которые хранят данные файла.

Рис. 3.8. Структура i-узла Unix

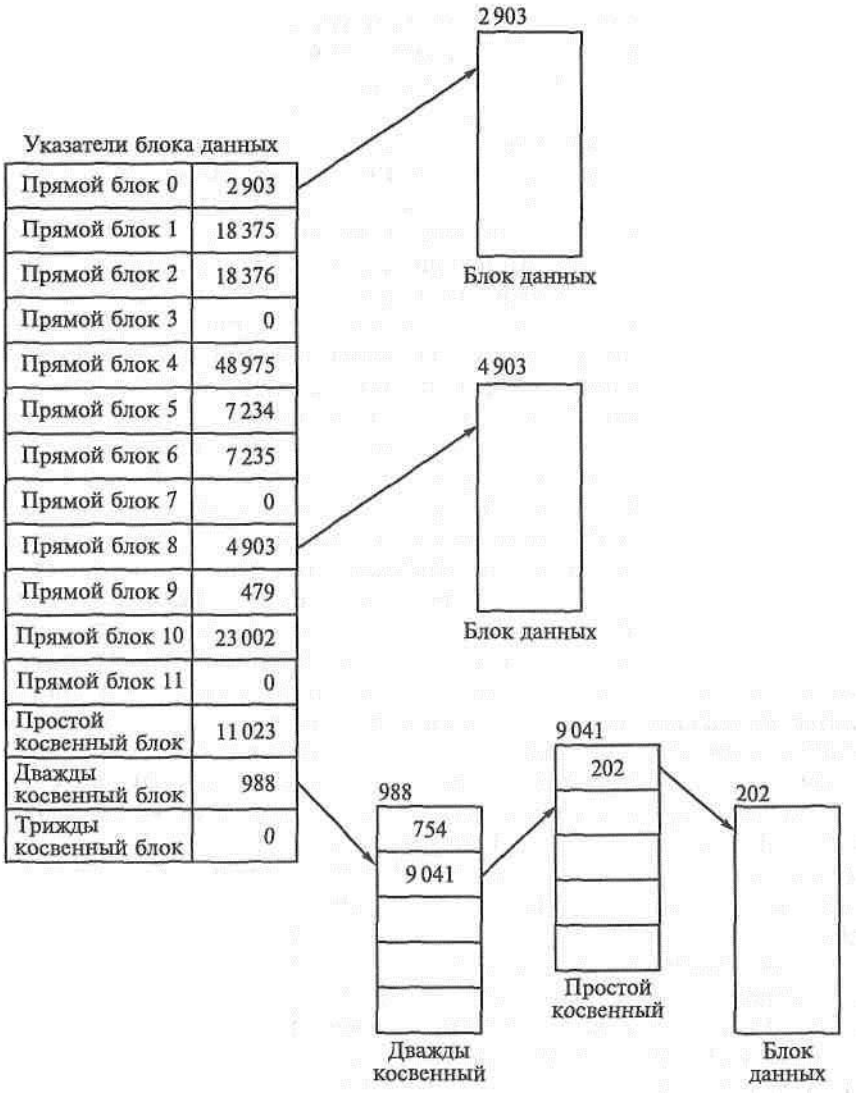


Рис. 3.9. Схема процедуры нахождения данных файла

Простой косвенный указатель адресует блок указателей на данные файла, дважды косвенный указатель адресует блок, содержащий простые косвенные указатели, а трижды косвенный указатель — блок с дважды косвенными указателями, как показано на рис. 3.9.

Эта схема адресации блоков может поддерживать файлы размером до терабайта.

3.3.2. Ядро системы Unix

Ядро — это сердце операционной системы Unix. Эта относительно небольшая часть кода обеспечивает все сервисы, требуемые для планирования работы процессов, доступа к оборудованию системы, управления памятью и обеспечения взаимодействия между процессами. Ядро состоит из нескольких подсистем, всегда присутствующих при работе системы Unix, и некоторого числа загружаемых модулей и драйверов устройств, управляющих периферийными устройствами, в зависимости от конфигурации системы.

Драйверы устройств являются частью подсистемы ввода-вывода ядра системы Unix. Они управляют взаимодействием между ОС Unix и оборудованием, таким как дисководы, принтеры, накопители на магнитных лентах и т.д. Интерфейс драйвера устройства защищает ядро от деталей аппаратной реализации и служит средством связи с широким набором внешних устройств типичной системы.

Драйвер обычно пишется на языке С и тщательно оптимизируется (и (или), из соображений лучшей производительности, на Ассемблере). Эти модули драйверов зависят от архитектуры машины, на которой они установлены, и их нельзя перенести с одной платформы на другую. Уровень абстракции модулей драйверов является одной из особенностей, которая позволяет этой ОС быть такой транспортабельной, — интерфейсы нового аппаратного оборудования просто связываются с остальными командами ядра во время сборки или динамически загружаются во время работы, когда в них возникает потребность.

В системе Unix существуют два типа интерфейсов драйверов внешних устройств: блочный и символьный (рис. 3.10). Часто одно и то же устройство поддерживает оба способа доступа. Как следует из названия, блочный интерфейс позволяет считывать и посылать на устройство буферизованные блоки данных рациональным способом.

Устройства, например дисковые накопители и накопители на магнитной ленте, обычно доступны через блочные интерфейсы внешних устройств и появляются в системе как устройства произвольного доступа. Символьный интерфейс обрабатывает данные посимвольно. Этот тип интерфейса также известен как необработанный интерфейс, поскольку с ним не связан никакой механизм буферизации. Терминалы, модемы и сетевые адаптеры — вот примеры периферийных устройств, работающих через интерфейсы устройств символьного ввода-вывода.

При работе драйвера устройства аппаратный интерфейс доступен через соответствующий специальный файл устройства, почти так же, как получают доступ к обычному файлу. Действия с

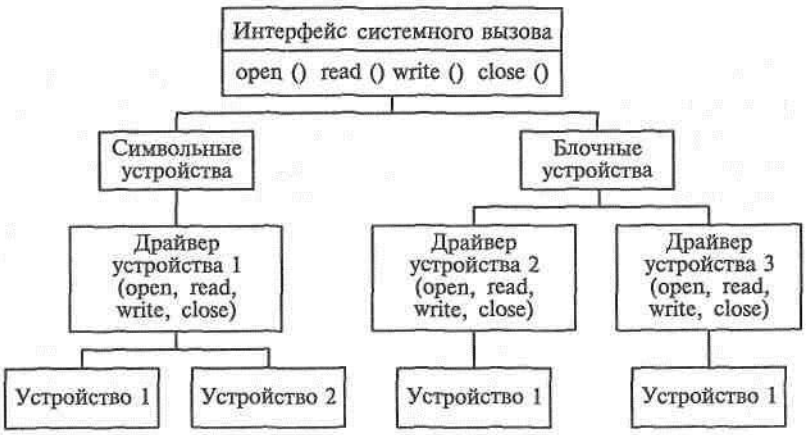


Рис. 3.10. Схема переключения устройств ядра

файлом (например, открытие, закрытие, чтение, запись) не обязательно поддерживаются каждым устройством, но, как правило, функционируют подобно обычным файлам. Чтобы это работало, ядро системы Unix поддерживает набор таблиц, которые перенаправляют эти запросы к соответствующим определенным подпрограммам, зависящим от конкретного устройства.

И тип интерфейса, и старшее число устройства являются частями переключающего механизма ядра. Они служат ключами в таблице соответствия устройств и требуются для того, чтобы ядро могло найти определенное устройство при перенаправлении обращения к специальному файлу. Например, процесс, который хочет выполнить операции ввода-вывода со вторым последовательным портом (в нашем примере /dev/cual), сначала должен открыть это устройство для чтения и записи.

Очевидно, вы встретитесь с целым набором отличий в требованиях при открытии последовательного порта для ввода-вывода и при открытии обычного текстового файла. В основном при системном вызове open() происходит следующее: ядро использует старшее число устройства как указатель в таблице соответствия символьных устройств, а затем вызывается подходящая процедура конкретного устройства, рассматривающая, какая семантика необходима для выполнения поставленной задачи. На рис. ЗЛО представлена схема переключения устройств ядра.

3.3.3. Процессы в ОС Unix

Процессы для системы Unix так же существенны, как дыхание для человека. Каждый процесс — обособленная единица, представляющая собой экземпляр выполняемой программы. В системе

Unix много процессов могут выполняться одновременно, а роль ядра заключается в координации и управлении их деятельностью.

Подсистема управления процессами обеспечивает фундамент для планирования процессов, управления памятью и взаимодействия между процессами. Управление многочисленными процессами и создание у пользователя иллюзии одновременности выполнения требует от ядра хранения информации о состоянии каждого процесса. Эта информация хранится в таблице процессов, которая содержит отдельную запись для каждого выполняемого процесса. Процесс может находиться в одном из нескольких состояний, и для системного администратора часто оказывается полезным понимание этих состояний и их отношения к задаче, над которой он в данный момент работает.

В операционной системе Unix все процессы порождаются системным вызовом fork(). Процесс, выполняющий вызов fork(), называется порождающим (родительским) процессом, а возникший в результате процесс называется порожденным (дочерним) процессом. Процесс может иметь много порожденных процессов, но только один порождающий процесс. Каждый процесс идентифицируется и отличается от других своим PID (process ID — идентификатор процесса). Далее приведен вывод команды ps, сообщающей о состоянии процессов:

```
orion_piarrera_13% ps -f
UID      PID  PPID C STIME    TTY    TIME CMD
piarrera 3612 3533 0 15:27:33 pts/2  0:00 /bin/tcsh -c tcsh
piarrera 3349 3347 0 15:23:09 pts/2  0:01 -tcsh
piarrera 3533 3349 0 15:26:34 pts/2  0:00 vi fubar
piarrera 3629 3612 0 15:27:37 pts/2  0:01 tcsh
```

Сравнивая столбцы с заглавиями PID и PPID, можно легко проследить связи между порождающими (PPID) и порожденными (PID) процессами. Процесс, соответствующий наивысшему идентификатору PID, является позднейшим, или самым младшим, процессом. Процесс, названный tcsh, имеет PID, равный 3349. Если вы проследите цепочку, то увидите, что процесс 3349 породил процесс 3533, который, в свою очередь, породил процесс 3612, который, в свою очередь, породил процесс 3629. Это изображает генеалогию.

Другим важным понятием является понятие владения. Система Unix не только многозадачная, но и многопользовательская, поэтому механизм управления правами доступа ориентирован на пользователя. Этот подход справедлив и для выполняемых процессов. UID (User ID — идентификатор пользователя) процесса и связанные с ним права доступа показывают, кто из пользователей является владельцем выполняемого процесса и каким процессам позволено посылать сигналы данному процессу. В системе

Unix каждый выполняемый процесс находится во владении того пользователя, который его запустил.

Ядро должно хранить информацию о состоянии каждого процесса при работе системы. Рассмотрим подробнее различные состояния процесса, возникающие во время его существования:

• *создание.* Состояние нового процесса непосредственно после того, как вызов fork() создал процесс. Это переходное состояние; хотя процесс и существует в этот момент, но он еще не готов выполняться;

• *пользовательский режим.* Как правило, процесс находится в этом состоянии большую часть времени своего выполнения. В пользовательском режиме могут выполняться стандартные действия процесса: присвоение значений переменным, выполнение вычислений и другие действия с обработкой данных;

• *режим ядра.* Процесс находится в режиме ядра, когда обрабатываются системные вызовы для выполнения задач вроде ввода-вывода. Когда процесс выполняется в режиме ядра, он находится под управлением ядра, при этом нельзя управлять его выходом из этого состояния. Фактически он даже может никогда не выйти, как в случае получения вызова exit();

• *готов к выполнению.* В этом состоянии процесс не исполняется в действительности в центральном процессоре, а готов к выполнению и ожидает, пока ядро не назначит его на исполнение;

• *спящий режим.* Это состояние обычно появляется, когда процесс ждет какого-нибудь события, например завершения запроса ввода-вывода к диску;

• *прерванный.* Это состояние похоже на состояние «готов к выполнению», за исключением того, что оно может появиться только тогда, когда процесс находится в переходном состоянии из режима ядра в пользовательский режим, но ядро решает, что подошло время для выполнения какой-то другой задачи;

• *готов в файле подкачки.* В случае нехватки физической памяти для выполнения текущих заданий ядро переносит образ процесса из оперативной памяти на диск для удовлетворения возросшего спроса. В этом состоянии процесс готов к выполнению, но, прежде чем его назначат на выполнение, его нужно перекачать обратно в оперативную память;

• *спящий в файле подкачки.* Процесс находится в спящем состоянии и перенесен из оперативной памяти в файл подкачки для удовлетворения возросшего спроса;

• *режим зомби.* Финальное состояние процесса. Выполнен системный вызов exit() и процесса не существует. В то же время, пока родитель этого процесса способен контролировать его состояние выхода, его данные остаются в таблице процессов.

Для просмотра состояния системы используется команда ps. Можно многое определить из того, что происходит в системе Unix,

основываясь на состоянии процесса или всех процессов. Команда ps должна стать постоянной частью административного арсенала.

Две основные разновидности системы Unix, которые сейчас используются: BSD-производные системы и System V. На машине с BSD-системой команда ps, используемая для перечня всех процессов, принадлежащих пользователю, имеет вид ps -ax, а в System V для той же цели используется команда ps -ef. Вывод данных в обеих системах также немного отличается. Вам необходимо использовать те аргументы команды ps, которые соответствуют вашей системе. Команда man ps подскажет вам, какие аргументы необходимо использовать.

Команда ps дает мгновенный снимок текущих выполняемых процессов. С помощью этого снимка и некоторых знаний о выполняемых программах вы можете использовать команду ps для определения, например, тех процессов, которые тормозят систему, или для выяснения того, что вообще делает система.

Иногда в системе Unix требуется больше памяти, чем фактически установлено. Когда возникает такая ситуация, вместо того чтобы остановиться, Unix освобождает память, сохраняя на диске образы процессов в памяти, которые в данный момент не выполняются или ждут какого-нибудь события. Они хранятся в специальной области диска, известной как устройство подкачки (swap device). Такое решение позволяет системе продолжать функционирование, хотя и с меньшей производительностью, в условиях нехватки памяти.

При настройке системы Unix производится выбор конфигурации подкачки памяти. Процесс, управляющий подкачкой, решает, какие процессы следует вытеснить на диск или вернуть в память, а также выполняет все необходимые действия.

Современные системы Unix также поддерживают процесс, называемый замещением страниц по требованию (demand paging), т. е. более гибкую схему для управления памятью. При замещении страниц обрабатывающееся адресное пространство управляется постранично и части образа процесса могут находиться на диске и считываться в оперативную память по мере необходимости. Управление с помощью страниц памяти может потребовать больших системных затрат, чем необходимо для простой подкачки. В то же время замещение страниц по требованию позволяет процессам иметь больший размер, чем оперативная память в системе, поскольку в этом случае для выполнения данного процесса ему уже не обязательно полностью храниться в оперативной памяти.

В ОС Unix используется методология извещения о каком-либо событии с помощью сигналов. Сигналы ОС Unix — это средство, с помощью которого ядро или другой внешний процесс извещают процесс о каком-то событии и приказывают ему выполнять в ответ некоторое действие. (Сигналы — это аналоги прерываний в

MS DOS.) Стандартными событиями, которые могут вызвать посылку сигнала, являются аппаратные прерывания, в частности ввод с клавиатуры или получение данных с последовательного порта; сбойные ситуации; тайм-ауты; отказ аппаратуры; недействительные инструкции и, кроме того, завершение порожденного процесса.

Определенные типы сигналов могут перехватываться выполняемыми процессами, при этом вместо выполнения стандартных действий они вызывают определяемые пользователем функции обработки сигналов. Возможен также вариант игнорирования процессом перехваченного сигнала и продолжение работы.

Другие сигналы не могут игнорироваться или перехватываться, и при получении такого сигнала выполняется стандартная процедура, обычно заканчивающаяся завершением процесса, получившего данный сигнал. Существует от 30 до 40 различных сигналов в зависимости от версии ОС Unix. В табл. 3.3 описано большинство из них.

Хотя в основном сигналы появляются в процессе работы программ, системный администратор должен ознакомиться с самыми важными из них: что они делают, когда появляются и как их использовать при администрировании Unix-системы. Далее подробно описаны некоторые сигналы из табл. 3.3:

• SIGHUP. По умолчанию при получении сигнала об отбое процесс завершается. Дочерний процесс, работающий в фоновом режиме, получает данный сигнал при выходе породившего его процесса, например при выходе из системы. Некоторые процессы-демоны перехватывают данный сигнал до помещения себя в фоновый режим с помощью системного вызова fork() и либо совершенно игнорируют данный сигнал, либо заменяют программу обработки сигнала на другую, выполняющую некоторые административные функции, такие как вывод содержимого памяти на диск или повторное чтение конфигурационных файлов. Примером такого процесса является демон init, который при получении сигнала об отбое перечитывает файл /etc/inittab для обновлении информации о конфигурации системы. Можно послать сигнал процессу командой kill. Например:

```
# kill -1 pid
```

где pid — идентификатор процесса, которому вы хотите послать сигнал;

• SIGTERM. Сигнал прекращения работы программы дает указание о корректном завершении процесса, активизируя встроенные в процесс функции освобождения ресурсов или прекращения работы. Этот сигнал посылается по умолчанию командой kill, если номер сигнала не задан в командной строке;

Таблица 3.3

Сигналы ОС Unix

Имя сигнала	Номер сигнала	Действие по умолчанию	Описание
SIGHUP	1	Выход	Сигнал об отбое
SIGINT	2	Выход	Сигнал прерывания (окончания)
SIGQUIT	3	Выгрузка	Сигнал выхода
SIGILLSIG	4	Выгрузка	Недействительная инструкция
TRAP	5	Выгрузка	Перехват трассировки или точки останова
SIGABRT	6	Выгрузка	Аварийное прекращение процесса
SIGFPE	8	Выгрузка	Исключительная ситуация с плавающей точкой
SIGKILL	9	Выход	Уничтожение процесса (нельзя прерывать или проигнорировать)
SIGBUS	10	Выгрузка	Ошибка системной шины
SIGSEGV	11	Выгрузка	Нарушение сегментации
SIGSYS	12	Выгрузка	Неправильный аргумент системного вызова
SIGPIPE	13	Выход	Разрушенный канал
SIGALRM	14	Выход	Сигнал тревоги
SIGTERM	15	Выход	Завершение программы
SIGUSR1	16	Выход	Пользовательский сигнал 1
SIGUSR2	17	Выход	Пользовательский сигнал 2
SIGCHLD	18	Игнорируется	Изменение статуса дочернего процесса
SIGPWR	19	Игнорируется	Сбой питания, перезапуск
SIGWINCH	20	Игнорируется	Изменение размера окна
SIGURG	21	Игнорируется	Экстренная ситуация сокета
SIGPOLL	22	Выход	Появление запроса
SIGSTOP	23	Остановка	Остановка (сигнал нельзя прерывать или проигно-рировать)
SIGTSTP	24	Остановка	Остановка пользователя, запрошенная с терминала
SIGCONT	25	Игнорируется	Возобновление остановленного процесса

• SIGKILL. Сигнал kill нельзя перехватить и он требует от процесса немедленного выхода. Используемые процессом функции завершения в этом случае не вызываются. Используйте этот сигнал как последнее средство для уничтожения процесса, не отвечающего на сигналы об отбое или прекращении работы. Если команда kill -9 pid не может завершить процесс, то поможет только перезагрузка системы;

• SIGSEGV. Сигнал о нарушении сегментации (сигнал 11) появляется, когда процесс пытается получить доступ к памяти, находящейся в несуществующей или недоступной для процесса области адресного пространства. При получении этого сигнала процесс записывает свой образ из памяти на диск (dumps core — разгрузка оперативной памяти) и выходит. Этот тип поведения указывает на ошибку программирования, наиболее вероятно появившуюся вследствие неправильного использования указателей;

• SIGBUS. Реакция выполняющегося процесса на сигнал об ошибке шины (bus error) очень похожа на реакцию на сигнал о нарушении сегментации (т. е. запись на диск образа памяти, разгрузка оперативной памяти, аварийный отказ). Хотя SIGBUS иногда вызван аппаратным отказом, чаще его причиной является разрушение программного стека из-за неправильного доступа к памяти;

• SIGPIPE.Запись данных в конвейер (pipe) не имеет никакого смысла, если никто не может их прочесть. Процесс записи данных в канал также подразумевает существование считывающего процесса. Этот сигнал посылается ядром процессу, проводящему вывод в конвейер, если тот пытается записать данные в конвейер после того, как считывающий процесс по каким-то причинам завершился.

Интерфейс системных вызовов Unix является средством доступа выполняемых процессов к функциям ядра. Эти функции выполняют такие действия как ввод-вывод, управление процессами и взаимодействие между процессами. Программисты осуществляют системные вызовы так же, как и вызов любой функции из библиотеки.

Когда процесс выполняет системный вызов, он находится в режиме ядра и по существу никто не контролирует, когда системный вызов возвращается и возвратится ли он вообще. Пример этого — процесс, требующий ввода пользователем данных и поэтому выполняющий вызов read() на терминал. Процесс не может вернуться из состояния чтения, пока не существует данных для считывания. На рис. 3.11 показано, как процесс использует системные вызовы для считывания данных с периферийного устройства.

IPC (Interprocess Communications — взаимодействие между процессами) — это связующее звено, позволяющее слабосвязанным процессам в системе синхронизировать их ресурсы и распределять

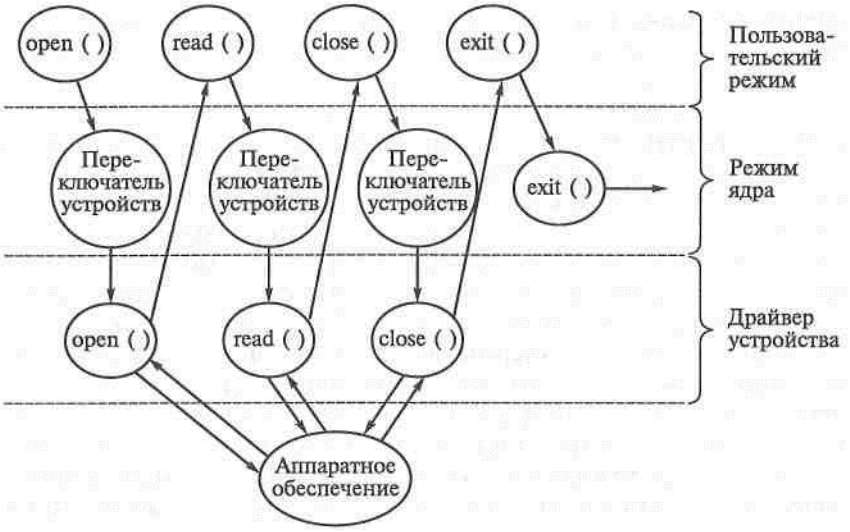


Рис. 3.11. Схемы считывания данных с периферийных устройств

данные, требуемые для выполнения заданий, для которых они запущены. Процессы могут выполняться независимо, но связаны каким-то образом (возможно, как часть подсистемы) и часто обращаются к общим данным и обмениваются сообщениями.

Unix обеспечивает богатый выбор инструментария, благодаря которому можно создавать большие системы и приложения, объединяющие неравноправные процессы, и при этом поддерживать в системе высокий уровень интеграции. Можно осуществлять взаимодействие между процессами различными методами, и системный администратор Unix должен ознакомиться с этими методами, чтобы знать, как они применяются в практических ситуациях.

Файлы, вероятно, проще и шире всего используются для связи между различными процессами в среде Unix. Создание файла блокировки, который сообщает другим процессам, что устройство в данный момент используется, — это пример относительно простого задания для Unix-программы, требующей монопольного доступа к устройству или ресурсу.

Также обычным делом для процесса является создание временных файлов, которые содержат данные, которые можно считывать и подвергать воздействию со стороны других процессов. Подсистема UUCP (Unix-to-Unix Copy Program) является основным примером такого типа использования. Процесс uucico создает файл блокировки для монопольного доступа к устройству доз-вона, например к модему, когда система соединена с удаленным узлом во время передачи файла. Программа uucp также создает

временные файлы, хранящие данные и команды, которые будут читаться и выполняться на удаленной системе после того, как они скопированы на удаленный узел.

Этот метод работает адекватно для ситуаций, в которых можно контролировать, как и когда процессы выполняются, или когда один процесс должен выбрать направление последующего выполнения в зависимости от результатов работы его предшественников. Но применение этого метода все больше и больше затрудняется при управлении событиями, происходящими асинхронно, когда многочисленные процессы должны передавать информацию в разных направлениях интерактивно. Пересылка данных от одного процесса к другому посредством обычных файлов не очень эффективна, поскольку считывающий процесс должен регулярно проверять наличие данных и необходимо также удостовериться в том, что данные считаны правильно и процесс записи завершен.

Ситуация усложняется, когда обмен данными идет в обоих направлениях; синхронизация — когда какой процесс должен иметь доступ к файлу — становится очень сложной. Трудность задачи растет экспоненциально в зависимости от числа процессов. Еще один источник проблем возникает, когда процесс, имеющий эксклюзивные права на некоторые ресурсы, внезапно прерывается и оставляет файл блокировки, который запрещает доступ других процессов к данному ресурсу.

Программы ОС Unix в основном осуществляют вывод данных таким образом, что эти данные передаются другим программам, которые сразу начнут с ними работу; при этом не приходится беспокоиться о запоминании промежуточных результатов во временных файлах. Конвейер — это тот механизм, который делает возможным такую передачу данных. Конвейер — это соединительное звено, используемое для перенаправления данных от одного процесса к другому по принципу FIFO («первым вошел, первым вышел»).

Например, можно направить выход одной команды в другую, использовав символ конвейера «|»:

```
ls /usr/bin | more
```

В этой команде длинный вывод команды Is (каталог /usr/bin содержит много файлов) посылается к команде more, которая отображает этот длинный вывод по страницам, помещающимся на экране. Оболочка ОС Unix распознает символ «|» как конвейер. Поскольку оболочки Unix являются просто программами, они используют основополагающие системные вызовы Unix для выполнения удобной команды «|».

Unix поддерживает два типа каналов. Первый, наиболее часто используемый, создается системным вызовом pipe().ЗТ0Т вызов создает двунаправленный конвейер и возвращает файловые деск-

рипторы чтения и записи, к которым затем можно получать доступ, используя ту же семантику, что и для обычного файла. Не существует имени файла, который следует открывать, только файловые дескрипторы, созданные системным вызовом pipe(); это означает, что только связанные процессы способны сообщаться через этот тип конвейера.

Именованный конвейер можно использовать подобно конвейеру, созданному системным вызовом pipe(), за исключением того, что он создается системным вызовом mknodQ и доступен через файловую систему Unix так же, как и обычный файл. Как и в случае с обычным конвейером, данные считываются и обрабатываются в порядке поступления, что согласуется с режимом работы конвейера. После того как данные считаны из именованного конвейера, они больше не доступны в файле. Кроме того, из соображений производительности, данные, записанные в именованный конвейер, хранятся только в прямых i-узлах, что устанавливает предельный размер этих файлов. (Обратитесь к разделу «Файловая система Unix» для более подробной информации об i-узлах.)

Именованный конвейер реализован как кольцевой буфер. Как показано на рис. 3.12, ядро системы Unix хранит два указателя, указывающих на текущие позиции считывания и записи. Эти ука-

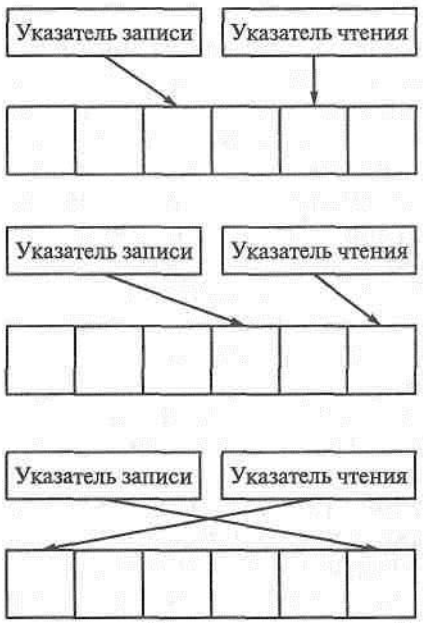


Рис. 3.12. Виды указаний считывания и записи в конвейерах

затели хранятся в файле вместе с данными. Многочисленные несвязанные процессы могут использовать этот механизм для обмена данными между собой.

Для взаимодействия процессов ОС Unix, синхронизации, обмена данными, совместного использования памяти применяют System V IPC.

В данное время пакет программ System V IPC широко реализуется различными производителями ОС Unix, и обычно он доступен даже в BSD-вариантах системы Unix. Система System V IPC предоставляет процессам методы обмена данными, совместного использования памяти и синхронизации выполняемых процессов. Доступ к этим функциям очень похож на управление доступом к обычным файлам, т. е. права доступа для владельца, группы и всех остальных пользователей поддерживаются и могут управляться владельцем процесса.

Механизм сообщений в ОС Unix позволяет многочисленным процессам посылать и получать форматированные данные с помощью очереди сообщений. Эта очередь хранится в ядре системы и создается или становится доступной через системный вызов msgget(). Получив соответствующие права доступа, этот вызов возвращает дескриптор очереди сообщений, вычисленный и назначенный на основании выбранного ключа. Любой процесс, получающий доступ к данной очереди сообщений, должен иметь соответствующий ключ, который служит идентификатором очереди.

Очередь сообщений поддерживает многочисленные типы сообщений. Взаимодействующие процессы могут настраивать общую очередь сообщений, обеспечивая отдельные каналы, основанные на типах сообщений, посылаемых и получаемых системными вызовами msgsnd() и msgrcvO соответственно. При использовании этого механизма взаимодействующие процессы достигают высокого уровня интеграции. Например, приложение, включающее в себя множество различных двоичных выполняемых файлов, может содержать программы мониторинга и формирования отчетов о состоянии различных подпроцессов и состоянии приложения в целом, основываясь на сообщениях, посылаемых соответствующими процессами.

Подход, управляемый событиями, более эффективный и менее ресурсоемкий, чем подход, в котором управляющая программа опрашивает различные программные модули для выяснения их состояния. Мгновенные сообщения, посылаемые через регулярные промежутки времени программе управления, могут использоваться для упругого реагирования на сбои. Другими словами, управляющее приложение может использовать эти сообщения для перезапуска поврежденного или прерванного процесса. Ресурсы очереди сообщений являются внешними для использую-

щего их процесса и не принадлежат виртуальному адресному пространству процесса, т.е. ими можно манипулировать извне при наличии соответствующих прав доступа.

Вызов msgget() выполняет функции, подобные системному вызову open(), используемому для операций ввода-вывода с файлом. В то же время, в отличие от операций ввода-вывода, где команду open() нужно было вызывать до того, как работать с данными, команду msgget() можно и не вызывать для того, чтобы воздействовать на данные очереди, если, конечно, приложение способно вычислить идентификатор очереди для существующей очереди сообщений. Вызов msgctl() используется для получения информации о состоянии процесса и изменения прав доступа в очереди, а также для удаления очереди из списка очередей ядра. Как показано далее, команда ipcs используется для получения информации, относящейся к различным очередям сообщений, поддерживаемым в данное время системой.

Изучение очереди сообщений:

```
bash$ ipcs -q
---- Message Queues ----
msquid    owner    perms    used-byted  messagaes
129       iarrera  7777     1944        486
```

Приложение может угадать правильный ключ и присоединиться к совместно используемому ресурсу, такому как очередь сообщений или область памяти; это есть ограничение пакета System V IPC. То, что программа может анонимно получить доступ к этим ресурсам, вносит потенциальный риск повреждения или перехвата данных. Конечно, данная ситуация подразумевает, что процесс имеет соответствующие права на выполнение этих действий.

Механизм совместного использования памяти обеспечивает процессу средство для присоединения в назначенный сегмент памяти, находящийся вне адресного пространства процесса. Этот внешний сегмент становится частью виртуального адресного пространства процесса и после настройки доступен таким же образом, каким процесс получал доступ к памяти в собственном сегменте данных. Из памяти можно считывать данные, в память можно записывать данные, и она имеет структуру, определяемую преобразованием типов.

Ядро кроме сообщений и семафоров поддерживает также таблицу, записи которой указывают на области памяти, выделенные для совместного использования. До того как процесс присоединится к области совместно используемой памяти с помощью команды shmat(), он должен получить дескриптор, возвращаемый системным вызовом shmget().

Вызов shmdt() выполняет отсоединение процесса от определенной области памяти. Как уже объяснялось ранее, после присо-

единения процесса к области совместно используемой памяти не требуется никаких специальных действий для получения к ней доступа. В то же время, в отличие от обычной памяти, занимающей часть адресного пространства процесса, область совместно используемой памяти не освобождается при выходе процесса. Для удаления этих сегментов необходимо специально вызывать команду shmctl().

Многие системы управления базами данных и многопользовательские приложения прибегают к совместному использованию памяти для повышения производительности системы. Это действительно полезно, когда много процессов должны получать доступ к часто используемым данным, поскольку это уменьшает количество доступов к диску и число файловых конфликтов между взаимодействующими процессами. Как показано далее, команда ipcs позволяет получить информацию, относящуюся к любому сегменту совместно используемой памяти в системе.

Изучение сегментов совместно используемой памяти:

```
bash$ ipcs -m
---- Shared Memory Segments ----
shmid  owner    perms    bytes     nattch   status
256    iarrera  777      131072    2
```

Механизм семафоров широко используется взаимодействующими процессами для синхронизации выполнения процессов и доступа к совместно используемым ресурсам. В многозадачной среде, такой как Unix, поддерживающей совместный доступ к системным ресурсам, такая синхронизация очень важна.

Различные события, находящиеся вне сферы воздействия и контроля выполняемых процессов, негативно влияют на рабочую среду процесса в критической ситуации. Это может вызвать внешние случайные ошибки, которые впоследствии невозможно отследить. Рассмотрим, например, случай присоединения двух процессов к одному совместному сегменту памяти, причем их поведение зависит от значений определенных переменных, хранящихся в этой области. Рассмотрим следующий фрагмент программы:

```
if (*i < MAX) {
*i +=1;
/* сделать что-то важное*/
}
```

Если величина переменной i из предыдущего примера хранится в совместно используемой памяти, другой параллельный процесс имеет потенциальную возможность получить к ней доступ и изменить ее значение. Если это произойдет после проверки *i < MAX, но до выполнения основного блока, то результаты могут оказаться непредсказуемыми. То, что величину переменной i мог изменить другой процесс, является условием, которое не

будет учитываться первым процессом, который продолжит выполнение программы с того места, на котором остановился. Использование семафоров для блокировки ресурсов, таких как совместная память, предотвращает появление подобной ситуации, сигнализируя другим процессам, что ресурс заблокирован и может находиться в нестабильном состоянии.

Семафоры выполняются в виде массивов, содержащих набор флагов, которые процесс может анализировать и изменять. Это позволяет процессу сообщать и получать сообщения о ситуациях, которые могут повлиять на работу одновременно выполняемых процессов. Действия семафоров либо выполняются все вместе, либо не выполняется ни одно путем программного увеличения или уменьшения величин, которыми оперируют семафоры.

Не стоит опасаться того, что массивы семафоров останутся в бессодержательном состоянии в результате прерывания процесса. Конечно, возможна борьба за ресурсы семафора. Рассмотрим случай, когда процесс *A* заблокировал семафор 1 и ждет разблокировки семафора 2. Тем временем процесс *B* заблокировал семафор 2 и ждет разблокировки семафора 1. Системный вызов semop() аннулирует подобные состязания, позволяя осуществлять операции над набором семафоров. Вместе с двумя описанными ранее механизмами пакета System V IPC доступны системные вызовы semget() и senmctlQ. Все они получают дескрипторы семафоров и обеспечивают операции управления над семафорами; в этом они подобны вызовам сообщений и совместно используемой памяти.

3.3.4. Технологии администрирования в Unix

Администратор Unix должен обеспечивать среду для функционирования рабочих станций, число которых может увеличиваться. Способ создания такой среды основывается на выбранной стратегии. В данном подразделе описаны стратегии, позволяющие предотвратить, обнаружить и решить возможные проблемы при создании и обслуживании такой среды.

Путь к решению всех задач администрирования — это планирование.

Прежде чем приступать к инсталляции новой системы, необходимо детально продумать, как нужно устанавливать, поддерживать эту систему и решать возникающие проблемы. Не запланировав все заранее, можно встать перед необходимостью решать возникающие вопросы в процессе работы.

Существует выражение: «Все, что может сломаться, обязательно сломается». Оно распространяется и на ОС Unix, и на сеть, и на приложения. Например, может закончиться лицензия на ПО и пользователи останутся без права доступа к нужным им данным.

Необходимо составить список потенциальных проблем и искать пути их разрешения, или, по крайней мере, предусмотреть такую возможность заранее. Необходимо заранее предусмотреть, что делать в случае аварии, а если она возникнет, то как можно быстро устранить последствия.

Изменения — одна из самых больших проблем при управлении. Один из способов контроля за изменениями — записывать все действия и постоянно обновлять эти записи. При этом необходимо записывать все изменения, которые проводятся, все специальные команды, которые при этом используются, и т.д. Все это поможет проследить, что происходит. Если возникнут проблемы юридического характера, то системный журнал также поможет в этом.

Можно использовать записи и для изменения плана. Предположим, что план предусматривает те или иные действия в случае выхода системы из строя. Если запланированные действия по какой-то причине не увенчались успехом, то придется для решения проблемы предпринять другие действия. Если описывается происходящее в системном журнале, то в следующий раз уже можно знать, что нужно делать, и быстро устранить неисправность.

Обнаружив неисправность, обязательно следует подробно записать причины неисправности, возможные способы ее устранения и способы, позволяющие не допустить возникновения этой проблемы.

Для того чтобы быть уверенным, что система работает нормально, нужно постоянно наблюдать за ней: следить за использованием ресурсов, наличием свободного места на диске, контролировать взаимодействие с сетью и проверять содержимое файлов журналов.

Отслеживая производительность системы, необходимо следить, чтобы нагрузка на систему не превышала допустимых пределов. Заметив, что сеть, диски, оперативная память или другие ресурсы используются очень интенсивно, можно заблаговременно принять меры и предотвратить нарушение работы системы. Может быть, будет найден способ распределить нагрузку между другими системами; если же это невозможно, то следует запланировать покупку нового оборудования.

Пользователи создают или разрушают систему. На первый взгляд кажется, что с компьютером взаимодействует система Unix, на самом деле с компьютером взаимодействует пользователь. По тому, как администратор работает с пользователями, другими системными администраторами и руководством, можно определить, как работают сами системы, или, по крайней мере, как воспринимается их работа.

Поскольку администратор обеспечивает поддержку системы, на время, пока все работает нормально, он становится невиди-

мым. О нем вспоминают только тогда, когда возникают какие-либо проблемы. Для того чтобы обратили на него внимание, пока все идет нормально, ему необходимо «повернуться лицом» к своим пользователям, разговаривать с ними, проверять, обеспечивает ли он необходимую поддержку.

Нужно доверять людям, но не настолько, чтобы попасть в ловушку. Некоторые пользователи могут «выстрелить ему в спину», например доложить руководству, выставив администратора в невыгодном свете. Чтобы «сохранить лицо», а также чтобы защититься в подобных ситуациях, требуется использовать способы, которые могут быть сформулированы следующим образом:

• администратор должен наблюдать за тем, что происходит в системе, а также следить, как пользователи воспринимают происходящее. Качество выполняемой работы во многом зависит от взаимодействия с «трудными» пользователями;

• необходимо составить договор об уровне обслуживания, чтобы убедиться, что обе стороны нашли общий язык;

• требуется немедленно откликаться на любой вопрос или просьбу о помощи. Это не означает, что нужно сразу же на месте решать все проблемы. Надо дать понять пользователю, что его просьба воспринята и она будет выполнена, как только администратор освободится. Необходимо разъяснить пользователю, сколько времени потребуется, чтобы решить данную задачу, объяснить ему, что в данный момент есть очень важная работа, которую необходимо выполнить в первую очередь. Нужно деликатно предложить пользователю подождать — это гораздо лучше, чем проигнорировать его запрос. В этом случае руководству придут жалобы на администратора и у него возникнут проблемы. Поэтому следует отвечать на любое почтовое сообщение, запись в журнале, chat-сообщение и т.д.;

• обязательно нужно записывать все запросы и ответы на них. В этом администратору может помочь журнал, о котором говорилось ранее. Если пользователь пожалуется, что на его запросы не реагируют, то можно в качестве контраргумента привести запись о том, через какое время откликнулись на запрос, что делали для решения проблемы и какие еще задачи стояли перед администратором в тот момент. Такая информация заставит замолчать многих любителей жаловаться. Если администратор общается с пользователем по электронной почте, то ему необходимо оставлять у себя копию приходящего письма и ответа на него.

Поддержка системы Unix включает в себя много разных задач. Необходимо быть уверенным, что система все время работала и продолжает работать нормально. Вы обязаны поддерживать работу системы, дисков, периферийного и сетевого оборудования, общаться с пользователями, работать с операционной системой и приложениями, обеспечивать безопасность, а главное — предос-

тавлять необходимые услуги, но при этом не нарушать правовые требования.

Работа, которую необходимо выполнять, различается в зависимости от типа среды. Так, условия работы университетской системы отличаются от условий работы системы, обслуживающей биржевых брокеров. Однако независимо от типа окружения следует придерживаться только хорошо продуманного плана и разработанной стратегии администрирования.

3.3.5. Средства администрирования

Как уже отмечалось ранее, каждый производитель программных средств Unix предлагает свой собственный набор инструментальных средств, предназначенных для выполнения задач системного администрирования. Будет ли это графический интерфейс X Window или же управляемая меню система, работающая в текстовом режиме, — почти все они создают интерфейс к сценариям оболочки Unix или программам, которые используют базовые утилиты работы в командной строке Unix.

Как уже отмечалось ранее, необходимо создавать учетные записи пользователей и управлять ими. Даже если администратор — единственный пользователь системы, рекомендуется не использовать учетную запись суперпользователя в повседневной работе. Основные задачи для выполнения каждой учетной записи в системе можно сформулировать следующим образом:

- добавление записи в файлы паролей системы;
- назначение пользователю оболочки;
- создание стандартной рабочей среды;
- добавление пользователя в группу или группы;
- создание рабочего каталога пользователя.

Все учетные записи включаются в отдельные группы, определяемые системным администратором. Группы обеспечивают легкий способ объединения пользователей и облегчают совместное использование файлов группой пользователей без предоставлений доступа к файлам каждому пользователю системы Unix в отдельности.

Настройка средств печати системы Unix оказывается достаточно рутинной процедурой, и установка принтеров в системе включает в себя много этапов (в зависимости от версии Unix). Основными задачами управления принтерами являются следующие:

- добавление принтера;
- удаление принтера;
- создание класса или группы принтеров. Классы принтеров являются частью средств печати Unix System V. Они позволяют приписывать ряд принтеров к конкретному классу. Это средство

наиболее полезно в рабочих средах с высокой загрузкой, в которых полезно распределять задания печати на нескольких принтерах;

- отключение принтера;
- включение принтера;
- снятие задания на печать.

Если система подключена к локальной сети или Интернету, то потенциально потребуется конфигурирование различных сервисов, в зависимости от того, для выполнения каких задач предназначена Unix-система. Далее представлены некоторые базовые сетевые сервисы, которыми необходимо управлять:

- NIS/NIS+. Сервис передачи сетевой информации работает на многих различных версиях Unix. Этот протокол, разработанный Sun Microsystems, дает возможность централизованно управлять несколькими различными сервисами на многочисленных узлах. Информация, которая чаще всего распространяется по локальной сети с помощью NIS, включает в себя пароли Unix, базу данных имен узлов, почтовые псевдонимы, информацию о группах и порты сетевых сервисов;
- DNS. Особенность заключается в том, что при управлении сервером доменных имен требуется содержать в порядке файлы базы данных имен узлов домена;
- /etc/services. Данный файл содержит номера портов TCP и UDP для сервисов, доступных через сеть. Для широко распространенных сервисов используется файл по умолчанию, однако в зависимости оттого, какие программные средства в системе, время от времени требуется модификация либо добавление записей о сервисах;
- HTTP. При работе с Web-сервером нужно выполнять системное обслуживание и управление файлами журналов HTTP-сервера;
- электронная почта. При предоставлении услуг электронной почты многочисленным пользователям нужно выполнять задачи системного обслуживания и конфигурирования для обеспечения максимальной эффективности и безопасности;
- брандмауэр. Если ваша сеть подключена к Интернету, то вы, вероятно, захотите установить брандмауэр для обеспечения безопасности системы. Брандмауэр имеет набор правил, которыми необходимо управлять с учетом того, какие сервисы нужно заблокировать при внешнем доступе к системе.

Unix поддерживает много различных типов файловых систем, и каждый из них имеет свои собственные характеристики и часто собственные средства обслуживания. В круг ваших обязанностей будет входить создание разделов на дисках для размещения файловых систем, создание файловых систем и обновление записей в таблице монтирования файловых систем по мере добавления или

удаления файловых систем. Некоторые типы файловых систем охватывают несколько физических дисков, состав которых динамически изменяется для повышения объема доступного дискового пространства либо обеспечения избыточности информации. Некоторые версии Unix используют файловые системы с ведением журнала (JFS), которые в типичном случае представляют набор утилит, упрощающих управление дисками и предоставляющих различные способы организации и монтирования дисков. В состав этих систем часто входит диспетчер логических томов (LVM), который используется для управления группами томов (группы дисков, которые по существу являются физическими носителями логических томов и файловых систем и делают возможным сегментацию дисков из общего доступного пула), логическими томами и файловыми системами.

Преимуществами систем, управляемых LVM/JFS, являются легкое управление дисками и файловыми системами и способность к расширению размера смонтированных файловых систем (без перерывов в обслуживании пользователей) в случае правильного их использования.

В многопользовательской среде, особенно при высоком объеме информационного обмена, необходимо выполнять мониторинг системы для выделения ее узких мест с точки зрения производительности, а также использовать конфигурации для планирования мощности оборудования системы.

Системный администратор отвечает за установку и поддержку различных программных компонентов и приложений, необходимых в системе. Большинство утилит системного администрирования (от smit фирмы IBM до SAM фирмы HP) используют собственный метод установки программных средств, в ходе применения которого программные средства регистрируются операционной системой и их легко идентифицировать. Такие утилиты значительно упрощают установку заплат и исправленных версий установленных программ.

Недорогие жесткие диски решают многие проблемы хранения информации, и в настоящее время можно обеспечить непрерывный доступ к огромным объемам информации. Платой за это удобство является то, что работа по резервированию ценной информации стала более сложной, прежде всего из-за больших объемов информации, с которыми приходится иметь дело.

Возможно, придется управлять сложным многотомным резервированием данных большого количества компьютеров; при этом проектирование и управление политикой резервирования данных в соответствии с имеющимися потребностями уже не сводится просто к установке магнитной ленты в накопитель и предоставлению возможности системному планировщику заданий копировать все на ленту в назначенный период времени.

Приведем описание некоторых инструментальных средств администрирования.

Фирма Sun предлагает *два различных инструментальных средства управления:* admintool (инструмент администрирования) и solstice (административный комплект solstice). При этом, хотя большинство из возможностей этих средств перекрываются, каждое из них может делать кое-что, что другое не может. Основная разница между двумя названными утилитами заключается в том, что admintool предназначена для локального использования на одной ЭВМ, в то время как solstice обеспечивает сетевую поддержку и средства управления удаленными системами. В табл. 3.4 приведен перечень основных функциональных возможностей инструментальных средств admintool и solstice.

Из названных двух утилит комплект средств администрирования solstice фирмы Sun более современен и масштабируем. Добавлением модулей, интегрируемых в среду solstice, в него вводятся новые функциональные возможности, такие как управление резервированием данных.

Утилита системного администрирования, предлагаемая Hewlett-Packard, называется диспетчером системного администрирования (SAM). SAM обеспечивает как текстовый, так и графический ин-

Таблица 3.4

Функциональные возможности утилит **admintool и solstice**

Функция	admintool	solstice	Описание
Управление пользователями	Да	Да	Создание учетных записей и управление ими
Управление группами	Да	Да	Создание групп пользователей и управление ими
Управление принтерами	Да	Да	Добавление/удаление/модифицирование принтеров
Управление узлами	Да	Да	Добавление узлов и их удаление из соответствующих баз данных
Управление NIS/NIS+	Нет	Да	Управление различными файлами баз данных NIS
Устройства последовательных портов	Да	Да	Управление:;МОдемами и другими терминальными устройствами' :^,
Управление программными средствами	Да	Нет	Управление и установка программных пакетов

терфейс. Это более сложное инструментальное средство, чем solstice фирмы Sun, поскольку данная утилита поддерживает более широкий диапазон функций администрирования. Например, управление дисками и конфигурирование RAID в среде Sun выполняются разными инструментальными средствами. В то же время панель управления дисками HP встроена непосредственно в инструментальное средство SAM для более полной интеграции. Преимущество данного подхода заключается в том, что практически все стандартные функции администрирования доступны в одном интерфейсе, поэтому вам не придется изучать новые средства для выполнения таких задач, как периодическое резервирование данных либо добавление и удаление дисковых накопителей. Кроме того, интерфейс SAM расширяется для добавления пользовательских команд и сценариев через добавление позиций пользовательских меню и групп меню.

Утилита системного управления (SMIT) представляет собой инструментальное средство администрирования, распространяемое IBM совместно с ее вариантом системы Unix. Как и в случае инструментальных средств Hewlett-Packard, SMIT обеспечивает и графический интерфейс пользователя, и текстовый интерфейс для работы в командной строке. SMIT работает, формируя файлы сценария по мере того, как вы перемещаетесь в системе меню, выбирая опции и выполняя различные задачи администрирования. Файл сценария содержит команды и опции, которые вам пришлось бы вставлять, выполняя соответствующие действия в командной строке. Это полезно при изучении деталей администрирования системы AIX, так как вы сможете изучать сценарий, наблюдая, как используются различные команды. Вместе с тем мы не любим использовать системы с управлением через меню при выполнении задач администрирования, потому что часто для выполнения простой операции приходится «пробираться» через целую серию подменю. SMIT решает эту проблему, обеспечивая быстрый путь, позволяющий обходить меню верхнего уровня и переходить непосредственно к детальному экрану для той задачи, которую нужно выполнить. Например, ввод команды smit mknfsexp делает возможным непосредственный переход к экрану, с которого можно указать файловую систему для экспорта через NFS-сервер.

Поставка Linux от фирмы Red Hat включает в себя отличное средство администрирования, названное linuxconf. Эта утилита конфигурирования Linux обеспечивает текстовый интерфейс для работы в командной строке, графический интерфейс пользователя, а также интерфейс Web-броузера. Интерфейс Web-броузера прост и понятен. Его дополнительное преимущество заключается в том, что не нужен http-сервер. С помощью этого легкого в использовании инструментального средства можно управлять мно-

гими аспектами работы системы Linux. Главный экран данной утилиты состоит из следующих панелей:

- панель состояния. Позволяет исследовать различные аспекты работы системы: перечень запущенных процессов, использование дисков и памяти, а также файлы системных журналов;
- панель конфигурирования. Обеспечивает возможность управления системой и конфигурирования большинства сервисов, которые выполняются в стандартной системе Unix, включая работу с сетью, почтовыми сервисами и учетными записями пользователей;
- панель управления. Обеспечивает возможность изменения состояния системы посредством останова и запуска сервисов по мере необходимости — все это без перезапуска системы или ручного редактирования файлов конфигурирования или сценариев запуска.

Одно из лучших свойств linuxconf, отсутствующее в других инструментальных средствах, — ее способность поддерживать многочисленные системные профили, которая весьма полезна в целом ряде ситуаций. Допустим, вы используете Linux для управления автономным компьютером дома и портативным компьютером, который подключаете к локальной сети в офисе. В этом случае нужно сконфигурировать два профиля и запускать только необходимые сервисы в зависимости от того, где вы находитесь.

Управление несколькими системными профилями — нелегкая задача в Unix, поскольку различные подсистемы управляются многочисленными файлами конфигурации. Без такого средства, как linuxconf, вам придется поддерживать набор подробных сценариев, которые будут конфигурировать систему в зависимости от запускаемого профиля. Linuxconf защищает вас от этого благодаря использованию интерфейса с использованием форм ввода данных, который позволяет конфигурировать и сохранять различные профили для их использования в будущем. Вы не только выберете, какой профиль устанавливать при запуске системы, linuxconf может сравнивать текущее состояние системы с конкретным профилем. Затем она динамически активизирует либо де-активизирует необходимые сервисы с тем, чтобы состояние системы соответствовало профилю, который вы хотите запустить. Это очень удобно при тестировании и конфигурировании различных сред для специфических приложений и сэкономит время, так как не надо перезапускать систему при тестировании различных компонентов.

Утилита linuxconf есть в составе дистрибутивов от большинства основных производителей программного обеспечения Unix, а не только от Red Hat. Подробности на Web-странице linuxconf по адресу: http://www.solucorp.qc.ca/linuxconf/.

В дистрибутив Linux от SuSE входит YaST (Yet Another Administration Tool — еще одно средство администрирования). Хотя

эта простая система для работы в текстовом режиме с управлением через меню менее полная, чем linuxconf, она все же позволяет выполнять большинство важных задач администрирования и настройки системы. Аналогично linuxconf YaST модифицирует стартовую последовательность системы и сохраняет всю информацию о конфигурировании в едином месте. Такой подход делает конфигурирование системы простым, однако и он имеет недостаток. Параметры системного профиля обычно сохраняются в форме переменных главного файла конфигурирования, и все другие сценарии запуска написаны на основе этого файла. В случае потери данного файла система не запустится правильно и потребуется значительное время для ее восстановления. Далее представлен фрагмент файла конфигурирования, создаваемого YaST, и настройка некоторых типичных параметров конфигурирования.

```
Фрагмент /etc/rc.config:

Должен ли запускаться httpd-сервер Apache при записке? (да/нет) S
TART_HT T P D=ye s
# Должна ли запускаться программа автоматического монтирова
ния autofs ? (да/нет)
START_AUTOFS=no
# Запускать программу управления принтерами Lpt ? (Если вы
используете pip, то вы также можете заблокировать ее здесь
или активизировать ее в /etc/inetd.conf) (да/нет)
START.LPD=yes
```

Все эти инструментальные средства очень легки в использовании, однако они большей частью сильно привязаны к соответствующим версиям дистрибутива Unix и требуют от администратора, управляющего несколькими системами от различных изготовителей, изучения средств администрирования от каждого изготовителя.

В зависимости от количества и разнообразия систем, которыми необходимо управлять, достижение эффективного уровня использования средств администрирования всех этих систем окажется задачей, которой придется уделять значительное время. Дело даже может закончиться тем, что придется терять гораздо больше времени, разбираясь с инструментальными средствами, чем фактически управлять системами. Хотя некоторые из поставляемых программных пакетов, например SMIT, и обеспечивают некоторую поддержку управления гетерогенными системами, диапазон их функциональности демонстрирует тенденцию к ограниченности.

В настоящее время есть значительное количество различных коммерческих программных пакетов от сторонних производителей, которые можно использовать при автоматизации решения задач системного администрирования, если работа с различными платформами вызывает затруднения. Системы управления этого

типа обычно дорогостоящие; при этом обычно поставляется только базовый пакет, к которому для обеспечения требуемой функциональности нужно подключать дополнительные модули расширения. Не следует удивляться, если дополнительные модули окажутся такими же дорогими, как и базовый пакет. Однако такие пакеты, как Unicenter TNG и Tivoli Enterprise Solutions от Computer Associates, предлагают всеобъемлющий набор программ для широкого диапазона задач управления — от системной безопасности и работы с сетями до управления данными и приложениями в системах, использующих разнородные платформы и различные операционные системы. Средства администрирования этого класса предлагают большое количество различных высокоспециализированных программных модулей, спроектированных для тесного интегрирования в стандартные интерфейсы. Конечно же, выйдя на этот уровень, потребитель далеко уходит от прихотей поставщиков и различий в их поставках; фактически, располагая названными инструментальными средствами, администратор уже будет управлять чем-то большим, чем просто система Unix.

Большинство современных утилит администрирования позволяют управлять системой из Web-броузера, например Netscape Navigator. В этом случае обычно запускается один либо больше серверных процессов и некоторое количество небольших вспомогательных приложений, которые выполняют конкретные задачи. Преимуществом инструментальных средств этого типа является то, что их мощность легко наращивать. Кроме того, они используются для администрирования различных систем из любой рабочей среды, которая обеспечивает функциональность Web-броузера. После установки вспомогательных приложений в конкретной системе не имеет значения, работаете ли вы с системой Sun под управлением Solaris или же с ПК, работающим под управлением Linux, поскольку каждая задача будет выполняться надлежащим образом и пользователь будет защищен от различных проявлений особенностей ОС.

Одно из таких инструментальных средств распространяется свободно — это пакет Webmin.

Webmin представляет собой достаточно мощную утилиту. Вследствие своей модульной структуры она легко наращивается для выполнения специфических для данной системы задач. Webmin поддерживает много различных вариантов поставок Unix и Linux. В табл. 3.5 приведен список поддерживаемых систем, взятый с начальной странички Webmin.

Титульная страница Webmin отображает главное меню, которое дает возможность перемещаться по разделам:

• системное меню Webmin. Используется для конфигурирования ряда различных рабочих параметров сервера Webmin, которые управляют, в частности, пользовательским интерфейсом,

Таблица 3.5

Варианты поставок ОС Unix и Linux, поддерживаемые Webmin

Операционная система	Поддерживаемая версия
BSDI	3.0, 3.1, 4.0
Caldera Open Linux	2.3, 2.4
Caldera Open Linux Server	2.3
Cobalt Linux	2.2, 5.0
Corel Linux	1.0, 1.1
Debian Linux	1.3, 2.0, 2.1, 2.2
DEC/Compaq OSF/1	4.0
Delix DLD Linux	5.2, 5.3, 6.0
Free BSD	2.1, 2.2, 3.0, 3.1, 3.2, 3.3, 3.4, 4.0, 5.0
HP/UX	10.01, 10.10, 10.20, 10.30, 11
IBM AIX	4.3
Linux	2.2
LinuxPL	1.0
MacOS Server X	1.0, 1.2
Mandrake Linux	5.3, 6.0, 6.1, 7.0
MkLinux	DR2.1, DR3
OpenBSD	2.5, 2.6, 2.7
Red Hat Linux	4.0, 4.1, 4.2, 5.0, 5.1, 5.2, 6.0, 6.1, 6.2
SCO OpenServer	5
SCO UnixWare	7.2
SGI Irix	6.0, 6.1, 6.2
Slackware Linux	3.2, 3.3, 3.4, 3.5, 3.6, 4.0, 7.0
Sun Solaris	2.5, 2.5.1, 2.6, 7, 8
SuSE Linux	5.1, 5.2, 5.3, 6.0, 6.1, 6.2, 6.3, 6.4
Turbo Linux	4.0
Xlinux	1.0

доступом к серверу и обслуживанием модулей. Не все модули Webmin обязательно поддерживаются во всех вариантах поставок Unix. В настоящее время наилучшими с точки зрения поддержки Webmin системами являются Solaris, Linux и FreeBSD;

• системное меню (System). Используется для выполнения многих наиболее распространенных задач администрирования, включая манипулирование процессами, управление файловой системой, составление расписаний запуска привязанных ко времени заданий, установка программных средств и управление учетными записями пользователей. Одним из выдающихся свойств Webmin является способ, которым он интегрируется в стартовую последовательность системы, в отличие от других инструментальных средств, например linuxconf и YaST, которые модифицируют системные стартовые файлы так, чтобы они им подходили. Хотя Webmin и не поддерживает многочисленные системные профили, можно легко модифицировать стартовую последовательность с помощью файла /etc/inittab, включив сценарии, которые должны выполняться, в процессе загрузки системы. Мы предпочитаем такой подход методу конфигурирования-активирования, используемому linuxconf и подобными ему инструментальными средствами, поскольку он не сопряжен с заметным изменением файлов конфигурации системы для поддержки конфигурационной утилиты. Это облегчает управление системой и ее конфигурирование без использования Webmin, если это необходимо или желательно;

• меню серверов (Servers). Используется для конфигурирования и управления распространенными сервисами, которые вы, вероятно, захотите использовать в системе. Webmin распознает многие из наиболее широко используемых серверов, таких как Web-сервер Apache и DNS-сервер BIND; он также может активировать и управлять сервисами и протоколами Интернета;

• меню аппаратных средств (Hardware). Используется для конфигурирования периферийных устройств системы, таких как разделы дисков и принтеры;

• прочее (Others). Предоставляет некоторые удобные функции, например быстрое создание и добавление в систему пользовательских команд, а также графический броузер файлов, написанный на языке Java. Особенно интересна функция, которая позволяет использовать telnet из интерфейса Web-броузера.

В настоящее время можно выполнять большинство задач администрирования, применяя простые в использовании графические или текстовые интерфейсы. Описанные в данной главе интерфейсы позволяют администратору системы быстро добиться результата при решении простых задач администрирования без изучения множества загадочных команд.

Контрольные вопросы

1. Перечислите основные компоненты обобщенной структуры ИС.
2. Сформулируйте основные задачи системного администрирования.

3. Опишите особенности администрирования в различных средах на примере системы Unix.

4. Опишите архитектуру средств администрирования Windows 2000.

5. Опишите архитектуру средств администрирования ОС Unix.

6. Приведите 10 рекомендаций и указаний при работе с файловой системой Unix в стыковке с файловой системой MS DOS / Windows.

7. Опишите ядро ОС Unix.

8. Перечислите сигналы прерываний ОС Unix. Опишите некоторые из них.

9. Что из себя представляет пакет программ System V IPC?

10. Опишите перечень базовых сетевых сервисов.

11. Сформулируйте основные функциональные возможности утилит admintool и solstice.

12. Раскройте назначение и виды поддерживаемых систем Webmin.

Глава 4 ОБЕСПЕЧЕНИЕ ИБ В АДМИНИСТРИРОВАНИИ ИС

4.1. Правовое и организационное обеспечение ИБ переработки информации в ИС

4.1.1. Правовое регулирование информационных процессов в деятельности общества

Процессы регулирования информационно-пропагандистского сопровождения любого вида деятельности общества и его структур на мировом и российском информационном пространстве являются обеспечивающей частью ИБ. Рассмотрение этой проблематики необходимо по следующим причинам.

Во-первых, средства массовой коммуникации в настоящее время трансформировались из сферы профессиональной деятельности журналистов в фактор эффективного влияния и стали политическим институтом. Однако область средств массовой коммуникации, информационного обмена и защиты процессов переработки информации является наименее кодифицированной в международном публичном праве и соответственно можно изучить предпосылки их направленного влияния для формирования позиций в интересах проводимой Российской Федерацией информационной политики.

Во-вторых, вопросы законодательной базы в области СМИ, допустимого уровня иностранного присутствия на внутрироссий-ском информационном пространстве являются в России в настоящее время наиболее злободневными, так как это предметы внимания постоянного мониторинга экспертов Совета Европы и ОБСЕ и уже интенсивно обсуждаются в компетентных ведомствах и парламенте Российской Федерации.

В-третьих, за последние три года в Российской Федерации принято несколько важных документов доктринального характера, которые влекут за собой существенные изменения и кодификацию правового поля в сфере средств массовой коммуникации, информационных отношений, информационно-пропагандистского обеспечения внешнеполитической деятельности нашего государства. Они могут существенно повлиять на постулируемую им позицию в данной области на международной арене.

В-четвертых, несмотря на то, что регулирование информационных отношений (информация, средства и методы ее доведения для потребителя) является наименее разработанной областью права, как внутреннего, так и международного, за последние 13 лет в сфере внутреннего права массовой информации Россия значительно продвинулась на пути ликвидации отрыва, отделяющего ее от наиболее развитых в этом отношении стран мира, а в области международного права внесла значительный вклад в формирование принципов и норм зарождающейся отрасли права.

Правовой фактор приобретает особую роль и в связи с ростом значения информационно-пропагандистской деятельности и так называемой публичной дипломатии в условиях продолжающегося «информационного взрыва». Реалией сегодняшнего дня стало использование информации в качестве оружия, в том числе оружия массового поражения. Угроза применения достижений в области ИТ в целях, не совместимых с задачами поддержания международного мира, например в качестве оружия терроризма, весьма реальна, что показали события, произошедшие 11 сентября 2001 г. в США. Это требует совместного принятия превентивных мер, в том числе и правового характера, для недопущения использования информационно-компьютерных технологий в целях ведения информационных войн, осуществления террористических ударов.

В качестве инструмента регулирования этих процессов может быть принято международное право массовой информации.

Международное право массовой информации — это совокупность специальных международных принципов и норм, регулирующих права и обязанности субъектов международного права в процессе использования (или санкционирования использования) средств массовой информации.

Нормы данной отрасли права регламентируют как технические аспекты распространения массовой информации, так и вопросы ее содержания.

В настоящее время сформулирован ряд главных принципов, регулирующих международное использование средств массовой информации:

1) каждое государство имеет право на распространение массовой информации за пределами своих границ;

2) все народы имеют право на свободный доступ к сведениям, распространяемым с помощью средств массовой информации;

3) все государства имеют право развивать свои средства массовой информации и использовать их в трансграничном масштабе;

4) государства обязаны воздерживаться от распространения и пресекать распространение ряда антидемократических, реакционных идей, таких как пропаганда войны, расовая дискриминация, апартеид, порнография и др.;

5) государства вправе противодействовать распространению через средства массовой информации идей, противоречащих основным принципам международного права;

6) государства обязаны воздерживаться от использования и пресекать использование национальных средств массовой информации для вмешательства во внутренние дела государств, а также от клеветнических кампаний, оскорбительной или враждебной пропаганды в отношении других государств;

7) государства обязаны поощрять распространение прогрессивных общедемократических идей;

8) государства обязаны осуществлять контроль за деятельностью национальных органов массовой информации, распространяющих идеи и сведения за границей.

В формировании правовой базы информационного права активное участие принимает ООН, в том числе ее Генеральная Ассамблея. Активную роль в этом процессе играют Комитет ООН по информации и ЮНЕСКО. Принципы и нормы, которые становятся ее основой, были зафиксированы во многих документах ООН. Однако ввиду того, что в настоящее время происходит обособление этой отрасли международного права, его нормы и принципы «рассыпаны» по документам, регламентирующим смежные отрасли.

В проблеме международной информационной безопасности обозначились два различных подхода. США и поддерживающие их ряд стран НАТО пытаются свести общую проблему к частным направлениям информационной преступности и информационного терроризма. Возможность создания информационного оружия и угроза возникновения информационных войн отодвигаются ими на задний план. Отрицается соответственно и разоруженческий аспект проблемы. Подобный подход позволяет сохранить свободу для дальнейших военных разработок в этой сфере, создания новых видов информационного оружия. В таком подходе США развивающиеся страны (КНР, Индия, ЮАР, Египет, Пакистан) видят угрозу их изоляции от активного участия в решении проблемы и, кроме того, попытку консервации их уязвимости от информационной агрессии (примеры Ирака и Югославии).

В соответствии с рекомендациями резолюции ГА ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» (2000 г.) в МИД России в качестве нового российского вклада в обсуждение этой темы в ООН был подготовлен проект документа «Общая оценка проблем информационной безопасности. Угрозы международной информационной безопасности». Данный документ передан в июне 2001 г. в Секретариат ООН и включен в доклад генерального секретаря по данной теме на 56-й сессии ГА ООН.

Таким образом, Россия играет одну из ключевых ролей в области разработки правовых механизмов регулирования проблемати-

ки информационного противоборства и, как следствие, международной информационной безопасности. Осознание российским политическим руководством насущной необходимости выработки общемировых правил игры на информационном поле, политическая воля и активные действия, предпринимаемые им в данном направлении, служат гарантией того, что России, возможно, удастся, улучшить свое нынешнее положение в данной сфере.

О незаконченности процесса выделения рассматриваемой отрасли международного права свидетельствует и тот факт, что еще не получило никакого международно-правового осмысления появление сетей Интернет. Проблема правовой характеристики Интернета нуждается в специальном исследовании и соответствующем документально-правовом оформлении, которое отразило бы всю многогранность его природы, так как данное образование не может рассматриваться только как средство массовой информации в силу своей многофункциональной структуры.

Россия входит в число стран—лидеров по объему информационного законодательства. Кроме положений Конституции РФ и инкорпорированных во внутреннее право норм международного права одной из особенностей российской правовой системы является наличие в ней Федеральных законов, содержащих право массовой информации в чистом виде, таких как «Об информации, информатизации и защите информации» от 25.01.95 № 24-ФЗ, «Об участии в международном информационном обмене» от 04.07.96 № 85-ФЗ. Существует также большое количество законов, регулирующих разные стороны (по сути) информационной деятельности применительно к конкретным явлениям: Закон РФ «О средствах массовой информации» от 27.12.91 № 2124-1, Федеральные законы «О государственной поддержке средств массовой информации и книгоиздания Российской Федерации» от 01.12.95 № 191-ФЗ, «О рекламе» от 18.07.95 № 108-ФЗ, Законы РФ «Об авторском праве и смежных правах» от 09.07.93 № 5352-1, «О правовой охране программ для электронно-вычислительных машин и баз данных» от 23.09.92 № 3523-1.

Имеется огромное количество указов Президента РФ и постановлений Правительства РФ, а также кроме них было принято значительное количество документов по вопросам телевидения и радиовещания, отдельным средствам массовой информации.

Концепция государственной информационной политики 1998 г., одобренная Государственной Думой и Постоянной палатой по государственной информационной политике Политического консультативного совета при Президенте РФ, в разд. 2.6 «Информационное право» предусматривает формирование правовой базы информационных отношений. Концепции развития законодательства, осуществляемые с 1995 г., активно влияют на законопроектный процесс в данной области. Активно формируется законода-

тельная основа регулирования отношений в области информатики, что подразумевает и активное участие страны в формировании и международных норм в этой сфере.

4.1.2. Международные и отечественные нормативные документы и технологии обеспечения безопасности процессов переработки информации

Законодательные меры по защите процессов переработки информации заключаются в исполнении существующих в стране или введении новых законов, положений, постановлений и инструкций, регулирующих юридическую ответственность должностных лиц — пользователей и обслуживающего технического персонала — за утечку, потерю или модификацию доверенной ему информации, подлежащей защите, в том числе за попытки выполнить аналогичные действия за пределами своих полномочий, а также в ответственности посторонних лиц за попытку преднамеренного несанкционированного доступа к аппаратуре и информации.

Цель законодательных мер — предупреждение и сдерживание потенциальных нарушителей.

Таким образом, государственная информационная политика (ГИП) должна опираться на следующие базовые принципы:

- открытость политики (все основные мероприятия информационной политики открыто обсуждаются обществом, и государство учитывает общественное мнение);
- равенство интересов участников (политика в равной степени учитывает интересы всех участников информационной деятельности независимо от их положения в обществе, формы собственности и государственной принадлежности);
- системность (реализация процессов обеспечения ИБ через государственную систему);
- приоритетность отечественного производителя (при равных условиях приоритет отдается конкурентоспособному отечественному производителю информационно-коммуникационных средств, продуктов и услуг);
- социальная ориентация (основные мероприятия ГИП должны быть направлены на обеспечение социальных интересов граждан России);
- государственная поддержка (мероприятия информационной политики, направленные на информационное развитие социальной сферы финансируются преимущественно государством);
- приоритетность права — законность (развитие и применение правовых и экономических методов имеет приоритет перед любыми формами административных решений проблем информационной сферы);

• сочетание централизованного управления силами и средствами обеспечения безопасности с передачей в соответствии с федеральным устройством России части полномочий в этой области органам государственной власти субъектов Российской Федерации и органам местного самоуправления);

• интеграция с международными системами обеспечения ИБ.

Международные нормативные акты обеспечения ИБ для администрирования. В международной практике для администрирования в компьютерных сетях можно выделить основные направления обеспечения ИБ:

• нормирование компьютерной безопасности по критериям оценки защищенности надежных систем и ИТ;

• стандартизация процессов создания безопасных информационных систем.

Так, уже в 1983 г. Агентство компьютерной безопасности Министерства обороны США опубликовало отчет, названный TCSEC («Критерии оценки защищенности надежных систем»), или «Оранжевая книга» (по цвету переплета), где были определены семь уровней безопасности *(A1* — гарантированная защита; *B], B2, B3* — полное удовлетворение доступом; *C1, C2* — избирательное управление доступом; *D* — минимальная безопасность) для оценки защиты грифованных данных в многопользовательских компьютерных системах. Для оценки компьютерных систем Министерства обороны США Национальный центр компьютерной безопасности МО США выпустил инструкции NCSC-TG-005 и NCSC-TG-011, известные как «Красная книга» (по цвету переплета). В свою очередь, Агентство информационной безопасности ФРГ подготовило GREEN BOOK («Зеленая книга»), где рассмотрены в комплексе требования к доступности, целостности и конфиденциальности информации как в государственном, так и в частном секторе.

В 1990 г. «Зеленая книга» была одобрена ФРГ, Великобританией, Францией и Голландией и направлена в ЕС, где на ее основе были подготовлены ITSEC («Критерии оценки защищенности информационных технологий»), или «Белая книга», как европейский стандарт, определяющий критерии, требования и процедуры для создания безопасных информационных систем и имеющий две схемы оценки: по эффективности (от *E1* до *E6)* и по функциональности (доступность, целостность системы, целостность данных, конфиденциальность информации и передачи данных).

В «Белой книге» названы основные компоненты безопасности по критериям ITSEC:

1) информационная безопасность;
2) безопасность системы;
3) безопасность продукта;
4) угроза безопасности;
5) набор функций безопасности;

6) гарантированность безопасности;
7) общая оценка безопасности;
8) классы безопасности.

Согласно европейским критериям ITSEC, ИБ включает в себя шесть основных элементов ее детализации:

1) цели безопасности и функции ИБ;
2) спецификация функций безопасности:

• идентификация и аутентификация (понимается не только традиционная проверка подлинности пользователя, но и функции для регистрации новых пользователей и удаления старых, а также функции для изменения и проверки аутентификационной информации, в том числе средств контроля целостности и функции для ограничения количества повторных попыток аутентификации);

• управление доступом (в том числе функции безопасности, которые обеспечивают временное ограничение доступа к совместно используемым объектам в целях поддержания целостности этих объектов; управление распространением прав доступа; контроль за получением информации путем логического вывода и агрегирования данных);

• подотчетность (протоколирование);

• аудит (независимый контроль);

• повторное использование объектов;

• точность информации (поддержка определенного соответствия между разными частями данных (точность связей) и обеспечение неизменности данных при передаче между процессами (точность коммуникации));

• надежность обслуживания (функции обеспечения, когда действия, критичные по времени, будут выполнены именно тогда, когда нужно; некритичные действия нельзя перенести в разряд критичных; авторизованные пользователи за оптимальное время получат запрашиваемые ресурсы; функции обнаружения и нейтрализации ошибок; функции планирования для обеспечения коммуникационной безопасности, т.е. безопасности данных, передаваемых по каналам связи);

• обмен данными;

3) конфиденциальность информации (защита от несанкционированного получения информации);
4) целостность информации (защита от несанкционированного изменения информации);
5) доступность информации (защита от несанкционированного или случайного удержания информации и ресурсов системы);
6) описание механизмов безопасности.

Для реализации функций идентификации и аутентификации могут использоваться такие механизмы, как специальный сервер KERBEROS, а для защиты компьютерных сетей — фильтрующие

маршрутизаторы, сетевые анализаторы протоколов (экраны) типа FireWall/Plas, Fire Wall-1, пакеты фильтрующих программ и т.д.

При проверке эффективности анализируется соответствие между задачами безопасности по конфиденциальности, целостности, доступности информации и реализованным набором функций безопасности — их функциональной полнотой и согласованностью, простотой использования, а также возможными последствиями использования злоумышленниками слабых мест защиты. Кроме того, в понятие «эффективность» включается и способность механизмов защиты противостоять прямым атакам, которая называется мощностью механизмов защиты. По ITSEC декларируется три степени мощности: базовая, средняя и высокая. При проверке корректности анализируется правильность и надежность реализации функций безопасности. По ITSEC декларируется семь уровней корректности: от *EO* до *E6.*

В «Европейских критериях» устанавливается 10 классов безопасности *(F-Cl, F-C2, F-Bl, F-B2, F-B3, F-1N, F-AV, F-DI, F-DC, F-DX).* Первые пять классов безопасности аналогичны классам *C1, C2, B1, B2, B3* американских критериев TCSEC. Класс *F-1N*предназначен для систем с высокими потребностями к обеспечению целостности, что типично для СУБД, и различает следующие виды доступа: чтение, запись, добавление, удаление, создание, переименование и выделение объектов. Класс /МКпредназначен для систем с высокими требованиями к обеспечению их работоспособности за счет противодействия угрозам отказа в обслуживании (существенно для систем управления технологическими процессами). Класс *F-DI* ориентирован на системы с повышенными требованиями к целостности данных, которые передаются по каналам связи. Класс *F-DC* характеризуется повышенными требованиями к конфиденциальности информации, а класс *F-DX* предназначен для систем с повышенными требованиями одновременно по классам *F-DIn F-DC.*

Канада разработала CTCPEC, США разработали новые «Федеральные критерии» (Federal Criteria). Так как эти критерии являются несовместимыми между собой, было принято решение попытаться гармонизировать (объединить) все эти критерии в новый набор критериев оценки защищенности, названный Common Criteria. Общие критерии дают набор критериев по оценке защищенности и устанавливают: требования к функциональным возможностям и требования к гарантиям; семь уровней доверия (уровни гарантий при оценке), которые может запросить пользователь (уровень EAL1 обеспечивает лишь небольшое доверие к корректности системы, а уровень EAL7 дает очень высокие гарантии); два понятия: «профиль защиты» и «цель безопасности».

Отечественное организационное и правовое обеспечение регулирования процессов безопасности в администрировании ИС. Основ-

ные задачи в сфере обеспечения и регулирования ИБ функционирования любой ИС можно сформулировать следующим образом:

- формирование и реализация единой государственной политики по обеспечению защиты национальных интересов от угроз в информационной сфере, реализации конституционных прав и свобод граждан на информационную деятельность;
- совершенствование законодательства Российской Федерации в сфере обеспечения ИБ;
- определение полномочий органов государственной власти Российской Федерации, субъектов Российской Федерации и органов местного самоуправления в сфере обеспечения ИБ;
- координация деятельности органов государственной власти по обеспечению ИБ в стране и ее структурах;
- создание условий для успешного развития негосударственной компоненты в сфере обеспечения ИБ, осуществления эффективного гражданского контроля за деятельностью органов государственной власти;
- совершенствование и защита отечественной информационной инфраструктуры, ускорение развития новых информационных технологий и их широкое распространение, унификация средств поиска, сбора, хранения, обработки и анализа информации с учетом вхождения России в глобальную информационную инфраструктуру;
- развитие стандартизации информационных систем на базе общепризнанных международных стандартов и их внедрение для всех видов информационных систем;
- развитие отечественной индустрии телекоммуникационных и информационных средств, их приоритетное по сравнению с зарубежными аналогами распространение на внутреннем рынке;
- защита государственных информационных ресурсов, прежде всего в федеральных органах государственной власти, на предприятиях оборонного комплекса;
- духовное возрождение России; обеспечение сохранности и защиты культурного и исторического наследия (в том числе музейных, архивных, библиотечных фондов, основных историко-культурных объектов);
- сохранение традиционных духовных ценностей при важнейшей роли Русской Православной церкви и церквей других конфессий;
- пропаганда средствами массовой информации элементов национальных культур народов России, духовно-нравственных, исторических традиций, норм общественной жизни и передового опыта подобной пропагандистской деятельности;
- повышение роли русского языка как государственного языка и языка межгосударственного общения народов России и государств — членов СНГ;

• создание оптимальных социально-экономических условий для осуществления важнейших видов творческой деятельности и функционирования учреждений культуры;

• противодействие угрозе развязывания противоборства в информационной сфере;

• организация международного сотрудничества по обеспечению ИБ при интеграции России в мировое информационное пространство.

• установление стандартов и нормативов в сфере обеспечения ИБ, которые являются наиболее важной регулирующей функцией. Девять государственных стандартов Российской Федерации (ГОСТ 28147-89, ГОСТ Р 34.10-94, ГОСТ Р 34.11-94, ГОСТ 29.339-92, ГОСТ Р 50752-95, ГОСТ РВ 50170-92, ГОСТ Р 50600-93, ГОСТ Р 50739-95, ГОСТ Р 50922-96) относятся к различным группам по классификатору стандартов и, к сожалению, не являются функционально полными ни по одному из направлений защиты процессов переработки информации. Кроме того, есть семейства родственных стандартов, имеющих отношение к области защиты процессов переработки информации:

• системы тревожной сигнализации, комплектуемые извещате-лями различного принципа действия — 12 ГОСТов;

• информационные технологии (сертификация систем телекоммуникации, программных и аппаратных средств, аттестационное тестирование взаимосвязи открытых систем, аттестация баз данных и т.д.) — около 200 ГОСТов;

• системы качества (в том числе стандарты серии 9000, введенные в действие на территории Российской Федерации) — больше 100 ГОСТов.

Значительная часть стандартов на методы контроля и испытаний (около 60 %) может быть признана не соответствующей требованию Закона РФ «Об обеспечении единства измерений» от 27.04.93 № 4871-1, как правило, в части погрешностей измерений. Отсутствуют стандарты в сфере информационно-психологической безопасности.

Одним из отечественных аналогов перечисленных стандартов является руководящий документ Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требований по защите информации».

Комплексный характер защиты процессов переработки информации достигается за счет использования унифицированного алгоритмического обеспечения для средств криптографической защиты в соответствии с российскими государственными стандартами:

• ГОСТ 28147 — 89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»;

• ГОСТ Р 34.10—94 «Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки

электронной цифровой подписи на базе асимметричного криптографического алгоритма»;

• ГОСТ Р 34.11 — 94 «Информационная технология. Криптографическая защита информации. Функция хэширования»;

• ГОСТ Р 50739 — 95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования».

Проблема обеспечения безопасности в администрировании ИС носит комплексный характер. Для ее решения необходимо сочетание как правовых мер, так и организационных (например, в компьютерных ИС на управленческом уровне руководство каждой организации должно выработать политику безопасности, определяющую общее направление работ, и выделить на эти цели соответствующие ресурсы), и программно-технических (идентификация и аутентификация, управление доступом, протоколирование и аудит, криптография, экранирование).

4.2. Угрозы безопасности обработки информации при администрировании

4.2.1. Комплексные и глобальные информационные угрозы функционирования ИС

При комплексном подходе классификации видов угроз ИБ (рис. 4.1) их можно разделить на угрозы общей направленности. По своей общей направленности угрозы ИБ Российской Федерации, как и других государств, подразделяются на следующие виды:

• угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;

• угрозы информационному обеспечению государственной политики Российской Федерации;

• угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;

• угрозы безопасности информационных и телекоммуникационных средств и систем как уже развернутых, так и создаваемых на территории России.

Затем их разделяют на случайные и преднамеренные, пассивные и активные, и по конкретным направлениям на организационные физико-технические, информационные и программно-математические.

Рис. 4.1. Классификация угроз ИБ

Наибольшую практическую опасность в настоящее время составляют угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России. Ими могут быть:

- противоправные сбор и использование информации;
- нарушения технологии обработки информации;
- внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;
- разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;
- уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникаций и связи;
- воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;
- компрометация ключей и средств криптографической защиты информации;
- утечка информации по техническим каналам;
- внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;
- уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;
- перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;
- использование сертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;
- несанкционированный доступ к информации, находящейся в банках и базах данных;
- нарушение законных ограничений на распространение информации.

4.2.2. Источники угроз ИБ ИС

Источники угроз ИБ ИС подразделяются на внешние и внутренние.

К *внешним источникам* угроз ИБ ИС относятся:

. деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов Российской Федерации и ее структурных образований в информационной сфере;

• стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;

• обострение международной конкуренции за обладание ИТ и ресурсами;

• деятельность международных террористических организаций;

• увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских ИТ;

• деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств;

• разработка рядом государств концепций информационных войн и соответствующего вооружения, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов (ИР), получение несанкционированного доступа к ним.

К *внутренним источникам* угроз ИБ ИС относятся:

• критическое состояние отечественных отраслей промышленности;

• неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями «сращивания» государственных и криминальных структур в информационной сфере, получения криминальными структурами доступа к конфиденциальной информации, усиления влияния организованной преступности на жизнь общества, снижения степени защищенности законных интересов граждан, общества и государства в информационной сфере;

• недостаточная координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации по формированию и реализации единой государственной политики в области обеспечения ИБ РФ;

• недостаточная разработанность нормативно-правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;

• неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;

• недостаточное финансирование мероприятий по обеспечению ИБРФ;

• недостаточная экономическая мощь государства;

• снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения ИБ;

• недостаточная активность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации в информировании общества о своей деятельности, разъяснении принимаемых решений, формировании открытых государственных ресурсов и развитии системы доступа к ним граждан;

• отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

В вооруженных силах НАТО, особенно США, значительное внимание уделяется роли «несмертельного оружия и технологий», прежде всего информационному оружию и психолого-пропагандистским операциям в войнах XXI в., которые существенно изменяют характер применения сухопутных, военно-воздушных и военно-морских сил и геополитического и цивилизационного противоборства основных центров формирующегося многополярного мира.

Практика показала, что наибольшие потери вооруженные силы несут при применении против них «несилового» информационного оружия, в первую очередь, от воздействия поражающих элементов, действующих на системы управления и психику человека. Информационное и консциентальное оружие воздействует на «идеальные» объекты (знаковые системы) или их материальные носители.

В настоящее время осуществляется глобальная информационно-культурная и информационно-идеологическая экспансия Запада, осуществляемая по мировым телекоммуникационным сетям (например, Интернет) и через средства массовой информации. Многие страны вынуждены принимать специальные меры для защиты своих сограждан, своей культуры, традиций и духовных ценностей от чуждого информационного влияния. Возникает необходимость защиты национальных информационных ресурсов и сохранения конфиденциальности информационного обмена по мировым открытым сетям, так как на этой почве могут возникать политическая и экономическая конфронтация государств, новые кризисы в международных отношениях. Поэтому ИБ, информационная война и информационное оружие в настоящее время оказались в центре всеобщего внимания.

Информационным оружием применительно к ИС являются средства:

• уничтожения, искажения или хищения информационных массивов, в первую очередь, ИС;

• преодоления систем защиты КС;

• ограничения допуска законных пользователей;

• дезорганизации работы технических средств, компьютерных систем.

Атакующим информационным оружием в настоящее время можно назвать:

• компьютерные вирусы, способные размножаться, внедряться в программы, передаваться по линиям связи, сетям передачи данных, выводить из строя информационные системы управления и т.д.;

• логические бомбы — программные закладные устройства, которые заранее внедряют в информационно-управляющие центры военной или гражданской инфраструктуры, чтобы по сигналу или в установленное время привести их в действие;

• средства подавления информационного обмена в телекоммуникационных сетях, фальсификация информации в каналах государственного и военного управления;

• средства нейтрализации тестовых программ в ИС;

• различного рода ошибки, сознательно вводимые противником в программное обеспечение ИС.

В докладе Объединенной комиссии по безопасности, созданной по распоряжению министра обороны и директора ЦРУ в США в июне 1993 г. и завершившей свою работу в феврале 1994 г., говорится: «...Уже признано, что сети передачи данных превращаются в поле битвы будущего. Информационное оружие, стратегию и тактику применения которого еще предстоит тщательно разработать, будет использоваться с «электронными скоростями» при обороне и нападении.

Информационные технологии позволят обеспечить разрешение геополитических кризисов, не производя ни одного выстрела. Наша политика обеспечения национальной безопасности и процедуры ее реализации должны быть направлены на защиту наших возможностей по ведению информационных войн и на создание всех необходимых условий для воспрещения противоборствующим США государствам вести такие войны...».

Уничтожение определенных типов сознания предполагает разрушение и переорганизацию общностей, которые конституируют данный тип сознания.

Можно выделить пять основных способов поражения и разрушения сознания в консциентальной войне:

1) поражение нейромозгового субстрата, снижающее уровень функционирования сознания, может происходить на основе действия химических веществ, длительного отравления воздуха, пищи, направленных радиационных воздействий;

2) понижение уровня организации информационно-коммуникативной среды на основе ее дезинтеграции и примитивизации, в которой функционирует и «живет» сознание;

3) оккультное воздействие на организацию сознания на основе направленной передачи мыслеформ субъекту поражения;

4) специальная организация и распространение по каналам коммуникации образов и текстов, которые разрушают работу сознания (условно может быть обозначено как психотропное оружие);

5) разрушение способов и форм идентификации личности по отношению к фиксированным общностям, приводящее к смене форм самоопределения и деперсонализации.

4.3. Методология обеспечения защиты процессов переработки информации в ИС

4.3.1. Администрирование сетевой безопасности

Информационная сфера является в настоящее время системообразующим фактором для всех реальных сфер общества и в значительной мере определяет состояние экономической, оборонной, социальной, политической и других составляющих национальной безопасности вообще, а также влияет на безопасность различных общественных структур и институтов в частности. ИБ представляет собой самостоятельную часть безопасности, роль и значение которой с каждым годом неуклонно возрастают, особенно в ИС управления организациями. Особая роль ИБ объясняется теми глобальными процессами, которые характерны в настоящее время для социально-экономического развития общества.

Администрирование сетевой безопасности, как и всякий процесс регулирования, начинается с планирования.

При планировании сети необходимо внедрить технологии безопасности, причем это следует сделать на стадии планирования установки операционной системы Windows 2000, Unix и т.д.). Таким образом можно обеспечить безопасную работу в сети.

По мере разработки плана сетевой безопасности следует:

- выявить ситуации, когда возможен риск снижения сетевой безопасности;
- определить размер сервера и требования размещения;
- подготовить персонал;
- создать и опубликовать политики и процедуры безопасности;
- использовать формальную методологию для создания плана безопасности;
- определить группы пользователей, их нужды и риски снижения безопасности.

Для эффективной реализации плана сетевой безопасности необходимо учесть риски ее снижения, которые значительно зависят от угроз снижения сетевой безопасности, представленных в табл. 4.1.

Для обеспечения доступа к ресурсам и данным только санкционированных пользователей необходимо тщательно спланировать

Угрозы снижения сетевой безопасности

Угрозы снижения безопасности	Содержание угрозы
Маскировка под пользователя	Нарушитель маскируется под действительного пользователя, например, присваивая IP-адрес надежной системы. С его помощью получает права доступа к соответствующему устройству или системе
Использование реквизитов пользователя	Нарушитель какими-то способами получает имя и пароль действительного пользователя и использует их при входе в систему. Нарушитель записывает сетевой обмен между пользователем и сервером и затем воспроизводит его, чтобы выдать себя за пользователя
Перехват данных	Если данные перемещаются по сети в виде открытого текста, то нарушители могут отследить и перехватить их
Манипулирование сетевыми данными	Незашифрованные сетевые финансовые транзакции доступны для манипулирования. Нарушитель с помощью, например, вирусов изменяет или повреждает сетевые данные
Угроза при неидентификации автора	Ориентированные на работу в сети деловые или финансовые транзакции подвергаются угрозе, если получатель транзакции не способен идентифицировать автора сообщения
Использование макровирусов	Вирусное заражение приложений с помощью макроязыков сложных документов
Отказ в обслуживании	Нарушитель бомбардирует сервер запросами, потребляющими системные ресурсы, и либо выводит сервер из строя, либо не позволяет выполнять нужную работу. Вывод сервера из строя иногда позволяет проникать в систему
Применение изменяющегося кода	Применяется злонамеренно изменяющийся код автоматически выполняемых ActiveX-элементов или Java-программ, которые загружаются из Интернета

Окончание табл. 4.1

Угрозы снижения безопасности	Содержание угрозы
Неправильное использование прав администратором сети	Системный администратор сознательно или ошибочно использует полные права работы с ОС для получения частных данных
Применение программы «Троянский конь»	Нанесение вреда с помощью программы, маскирующейся под полезную утилиту
Социально-административная атака	Получение доступа в сеть путем фальсификации административного положения, попросив новых работников подтвердить свои пароли

стратегию сетевой безопасности. Это также позволяет вести учет использования сетевых ресурсов. Основные этапы планирования стратегий сетевой безопасности могут быть представлены в следующем виде:

1) составление плана развертывания стратегии безопасности;
2) создание границ безопасности;
3) анализ стратегий сетевой безопасности;
4) внедрение стратегий безопасности для всех пользователей;
5) внедрение стратегий для пользователей корпоративных приложений;
6) внедрение стратегий для персонала организации;
7) внедрение стратегий для партнеров;
8) мониторинг реализации плана.

Решающим фактором успешной работы персонала отдела администрирования по обеспечению безопасности работы в сети является постоянное совершенствование сотрудниками их навыков и знаний. Персонал должен изучить базовую и другие ОС, особенно их технологии сетевой безопасности. При этом целесообразно сконцентрировать внимание на функциях безопасности ОС. Перечень функций безопасности ОС Windows 2000 приведен в табл. 4.2.

Качество технологий безопасности зависит от применяемых методов, и это должно быть отражено в плане сетевой безопасности.

Рекомендуемое типовое содержание плана сетевой безопасности ИС представлено в табл. 4.3.

Планирование распределенной сетевой безопасности предусматривает координирование многих функций безопасности в сети

Таблица 4.2

Функции безопасности ОС Windows 2000

Название функции безопасности	Назначение
Применение шаблонов безопасности	Позволяет администраторам настраивать глобальные и локальные параметры безопасности, включая важные для безопасности значения реестра, управление доступом к файлам и реестру и безопасность системных служб
Аутентификация Kerberos	Основной протокол безопасности для доступа внутри или через домены Windows 2000. Обеспечивает взаимную аутентификацию клиентов и серверов и поддерживает делегирование и авторизацию посредством проксимеханизмов
Использование инфраструктуры открытого ключа (PKI)	Инфраструктура PKI применяется для надежной зашиты служб Интернета и предприятий, включая основанные на экстрасетях коммуникации
Использование смарт-карты	Windows 2000 имеет встроенную стандартную модель подключения устройств чтения смарт-карт и самих карт к компьютеру, а также не зависящие от устройств интерфейсы программирования приложений, работающих со смарт-картами
Управление протоколом IPSec	Протокол IPSec поддерживает аутентификацию на уровне сети, целостность данных и шифрование для обеспечения надежности соединений интрасети, экстрасети и Интернета
Шифрование в файловой системе	Основанная на открытых ключах файловая система NTFS может быть активизирована на уровне файлов или подкаталогов

для создания полной политики безопасности. Распределенная безопасность позволяет пользователям регистрироваться в компьютерных системах, находить и применять нужную информацию. Большая часть информации в сетях доступна всем клиентам для чтения, но только небольшой группе людей позволено изменять ее. Если данные важные или частные, то только санкционированным пользователям или группам разрешено считывать файлы. Защита и обеспечение конфиденциальности информации, передаваемой по телефонным сетям, Интернету и даже участкам внутренних сетей компании, также очень сложны.

Иногда организации требуется более одного плана безопасности. Количество планов зависит от размера организации. Например, международной организации нужен отдельный план для каждого подразделения, а локальной организации — всего один план. Компаниям с разграниченными политиками для различных групп пользователей может потребоваться отдельный план для каждой группы.

Защита и обеспечение конфиденциальности информации должны обеспечивать установление параметров пользователя. Это делается с помощью политики аутентификации и стратегии регистрации в сети.

Аутентификация — это процесс определения пользователей, пытающихся подключиться к сети. Пользователи, аутентифици-рованные в сети, могут использовать сетевые ресурсы на основе

Таблица 4.3

Типовой план сетевой безопасности ИС

Раздел плана	Содержание разделов
Угрозы снижения безопасности	Виды угроз снижения безопасности предприятия
Стратегии безопасности	Основные стратегии безопасности, необходимые для защиты от угроз
Политика (PKI) безопасности	Планы развертывания сертификационных центров для внутренних и внешних функций безопасности
Описания групп безопасности	Описания групп безопасности и их отношения между собой. Этот раздел связывает политики групп и группы безопасности
Групповая политика	Описание параметров безопасности групповой политики, например политик сетевого пароля
Аутентификации и стратегии регистрации в сети	Политики аутентификации для регистрации в сети и для использования удаленного доступа и смарт-карты для входа
Стратегии обеспечения безопасности	Описание обеспечения безопасности информации, например безопасности электронной почты и Web-соединений
Политики администрирования	Политики делегирования административных заданий и отслеживание журналов аудита для определения подозрительных действий
Тестирование плана	Проверка плана безопасности путем имитации функционирования с применением пилотных программ совершенствования плана

своих прав доступа. Для проверки подлинности сетевых пользователей создаются учетные записи. Это важнейшая часть управления безопасностью. Без аутентификации ресурсы, например файлы, доступны любым пользователям. Особенно это имеет значение при работе в Интернете.

Для обеспечения безопасной работы ИС в Интернете целесообразно установить между системой и Интернетом брандмауэр (рис. 4.2). Он уменьшает риски при подключении к Интернету, а также препятствует получению доступа к вашему компьютеру из Интернета, за исключением компьютеров, имеющих право такого доступа.

Брандмауэр использует фильтрование пакетов для разрешения или запрещения потока определенных видов сетевого трафика. Фильтрование пакетов IP позволяет точно определить, какой IP-трафик может пересекать брандмауэр. Эта функция важна при подключении частных сетей к общедоступным сетям, например к Интернету. Многие брандмауэры способны распознавать и отражать сложные атаки.

Брандмауэры часто выступают в роли проксисерверов или маршрутизаторов, потому что они передают трафик между частной и общей сетями. Программное обеспечение брандмауэра или прок-сисервера проверяет все сетевые пакеты каждого интерфейса и определяет адрес их места назначения. Если они соответствуют определенному заданному критерию, то пакеты передаются получателю другого сетевого интерфейса. Брандмауэр может просто маршрутизировать пакеты или действовать как проксисервер и переводить IP-адреса частной сети.

Как и функции проксисервера, так и некоторые функции брандмауэра, обеспечивает Microsoft Proxy Server. Он выполняется на компьютерах с Windows 2000, и оба они должны быть настроены

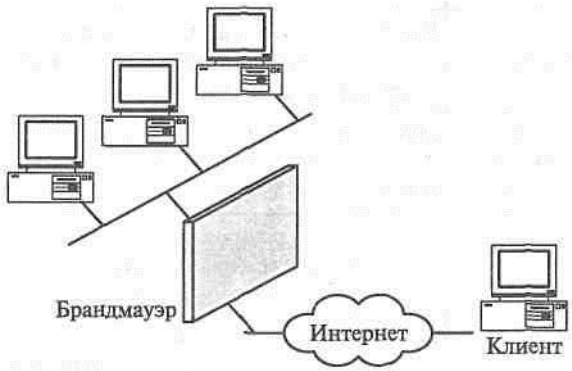


Рис. 4.2. Схема подключения брандмауэра

так, чтобы обеспечивать полную сетевую безопасность. Если и установлена более ранняя, чем 2.0, версия Proxy Server и Service Pack 1, то необходимо обновить ее для совместимости с Windows 2000 (это делается в момент обновления сервера до Windows 2000).

Часто один проксисервер не способен справиться с объемом трафика между сетью организации и Интернетом. В этих случаях применяются несколько проксисерверов. Трафик распределяется между ними автоматически.

За дополнительной информацией о Proxy Server и технологиях безопасности можно обратиться по адресу http://windows.microsoft.com/ windows2000/reskit/webresources.

После установки проксисервера, настройки параметров контроля и подготовки персонала сеть подключают к внешней сети. Для этого необходимо убедиться, что пользователям доступны только службы, которые вы санкционировали, и риск злоупотреблений практически отсутствует. Эта среда требует тщательного контроля и поддержки, но также надо быть готовым к предоставлению других служб сетевой безопасности.

4.3.2. Обеспечение безопасности сети при удаленном доступе

Удаленный доступ позволяет клиентам подключаться к сети с удаленного компьютера с помощью различных аппаратных устройств, включая карты сетевого интерфейса и модемы. Получив соединение удаленного доступа, клиенты могут использовать сетевые ресурсы, например файлы, так же, как они использовали бы клиентский компьютер, напрямую подключенный к ЛВС. Для обеспечения такого подключения в Windows 2000 используется система Routing and Remote Access (RRAS) — служба, позволяющая удаленным пользователям подключиться к локальной сети по телефону. Удаленный доступ позволяет несанкционированным пользователям проникнуть в сеть, поэтому Windows 2000 предлагает ряд мер безопасности для обеспечения защиты сети. При установке удаленного соединения с сервером клиент получает доступ к сети, если:

- запрос соответствует одной из политик удаленного доступа, заданных для сервера;
- учетная запись пользователя активизирована для удаленного доступа;
- аутентификация клиент-сервер завершена успешно.

Доступ клиента к сети может быть ограничен для определенных серверов, подсетей и типов протоколов в зависимости от клиентского профиля удаленного доступа. В противном случае все службы, обычно доступные для подключенного к ЛВС пользователя

(включая совместное использование файлов и принтеров, доступ к Web-серверу и доставке сообщений), активизированы посредством соединения удаленного доступа.

Так, при перехвате имени и пароля пользователя в момент подключения к серверу RRAS, используя технологии, аналогичные перехвату телефонных разговоров в RRAS, предусмотрены безопасные средства аутентификации пользователя:

• Challenge Handshake Authentication Protocol (CHAP). Протокол CHAP разработан для управления передачей паролей в открытом тексте. CHAP — это наиболее популярный протокол аутентификации. Поскольку алгоритм вычисления откликов протокола CHAP хорошо известен, необходимо тщательно подбирать и задавать достаточно длинные пароли. CHAP-пароли, являющиеся обычными словами или именами, легко вычисляются с помощью словаря путем сравнения откликов CHAP с каждым словом в словаре. Недостаточно длинные пароли выявляются сравнением CHAP-откликов с откликами пользователя (эта операция выполняется до тех пор, пока не будет найдено совпадение);

• Microsoft Challenge Handshake Authentication Protocol (MS-CHAP). Протокол MS-CHAP представляет собой разновидность протокола CHAP, которой не требуется пароль в виде открытого текста на сервере аутентификации. MS-CHAP-пароли хранятся на сервере в большей безопасности, но доступны вычислению так же, как и CHAP-пароли. В протоколе MS-CHAP ответ на запрос вычисляется с помощью Message Digest 4 (MD4) — хешируемой версии пароля и ответа сервера доступа к сети (Network access server — NAS). Это активизирует аутентификацию по Интернету на контроллер домена Windows 2000 (или на контроллер домена Windows NT 4.0, на котором не было выполнено обновление);

• Password Authentication Protocol (PAP). Протокол PAP передает пароль в виде строки от пользовательского компьютера устройству NAS. Когда NAS передает пароль, он шифрует его с применением секретного ключа протокола RADIUS в качестве ключа шифрования. PAP — это наиболее гибкий протокол, потому что передача пароля в виде открытого текста серверу аутентификации позволяет серверу сравнивать пароль практически с любым форматом хранения. Например, пароли ОС UNIX хранятся в виде зашифрованных строк, которые не могут быть расшифрованы. PAP-пароли можно сравнить с этими строками путем воспроизведения метода шифрования. Поскольку протокол PAP использует пароль в виде открытого текста, его безопасность уязвима. Хотя протокол RADIUS шифрует пароль, он передается через удаленное соединение в виде открытого текста;

• Shiva Password Authentication Protocol (SPAP). SPAP — это механизм двустороннего шифрования, применяемый серверами удаленного доступа Shiva. Клиент удаленного доступа может исполь-

зовать SPAP для собственной аутентификации на удаленном сервере Shiva. Клиент удаленного доступа с 32-разрядной ОС Windows 2000 может применять SPAP для собственной аутентификации на удаленном сервере Windows 2000. SPAP более надежен, чем PAP, но менее надежен, чем CHAP или MS-CHAP. SPAP не имеет защиты против констатации удаленного сервера. Как и PAP, SPAP — это простой обмен сообщениями. Сначала клиент удаленного доступа посылает сообщение «Authenticate-Request» («Запрос аутентификации») серверу удаленного доступа, содержащему клиентское имя пользователя и зашифрованный пароль. Затем сервер удаленного доступа расшифровывает пароль, проверяет имя пользователя и пароль и возвращает либо сообщение «Authenticate -Ack» («Аутентификация прошла»), когда информация пользователя верна, либо сообщение «Authenticate-Nak» («Аутентификация не прошла») с объяснением причины, почему информация пользователя неверна;

• Extensible Authentication Protocol (EAP). Это расширение протокола PPP, позволяющее применять произвольные механизмы аутентификации для подтверждения соединения PPP. При использовании таких протоколов аутентификации PPP, как MS-CHAP и SPAP, на этапе установки соединения выбирается определенный механизм аутентификации. Затем на этапе аутентификации соединения используется согласованный протокол аутентификации для подтверждения соединения. Протокол аутентификации — это фиксированные наборы сообщений, посылаемых в определенном порядке. EAP разработан для аутентификации подключаемых модулей как клиента, так и сервера. Путем установки библиотечного EAP-файла на клиенте удаленного доступа и сервере удаленного доступа может поддерживаться новый тип EAP. Это позволяет продавцам в любое время поставлять новую схему аутентификации. EAP обеспечивает наибольшую гибкость аутентификации уникальности и изменений.

Для эффективной реализации безопасности работы в режиме удаленного доступа службы RRAS и Internet Authentication Service (IAS) используют политики удаленного доступа с целью разрешения или запрещения подключения. В обоих случаях политики удаленного доступа хранятся локально и определяют правила на уровне отдельных подключений.

При использовании политик удаленного доступа можно предоставить или запретить авторизацию в зависимости от времени суток или дня недели, от группы, к которой принадлежит удаленный пользователь, и типа запрашиваемого соединения (удаленная сеть или VPN) и т.д. При этом выделяют локальное и централизованное управление политиками.

Поскольку политики удаленного доступа хранятся локально, на сервере удаленного доступа, или IAS-сервере, для централизо-

ванного управления одним набором политик для нескольких серверов удаленного доступа или VPN-серверов выполните следующую последовательность действий:

1) установите на компьютер IAS в качестве RADIUS-сервера;

2) сконфигурируйте IAS для RADIUS-клиентов для каждого сервера удаленного доступа или VPN-сервера;

3) на IAS-сервере создайте основной набор политик, используемых всеми серверами удаленного доступа;

4) сконфигурируйте каждый сервер удаленного доступа в качестве RADIUS-клиента для IAS-сервера.

После этого локальные политики удаленного доступа, хранящиеся на сервере удаленного доступа, не будут использоваться. Централизованное управление политиками удаленного доступа применяется также, когда серверы удаленного доступа работают под управлением Windows NT 4.0 и имеют службу RRAS. При этом можно сконфигурировать Windows NT 4.0 — сервер, имеющий службу RRAS, в качестве RADIUS-клиента для IAS-сервера.

Использование протоколов шифрования также применяется для защиты данных, пересылаемых между клиентом и сервером удаленного доступа. Шифрование данных важно для финансовых институтов, правительственных и других организаций, требующих безопасной передачи данных. Если требуется сохранение конфиденциальности данных, то сетевой администратор может настроить сервер удаленного доступа, чтобы он требовал зашифрованных соединений. Пользователям, подключающимся к такому серверу, придется шифровать их данные, иначе доступ будет запрещен.

Для VPN-соединений вы защищаете данные, шифруя их между конечными точками сети VPN. Для VPN-соединений всегда следует шифровать данные при передаче их по общедоступной сети, например по Интернету, так как присутствует риск несанкционированного доступа.

Для удаленных сетевых соединений можно защитить данные, шифруя их при передаче по линии связи между клиентом и сервером удаленного доступа. Шифрование следует использовать, если существует риск перехвата данных. Для удаленных соединений используют два вида шифрования:

• MPPE. Все PPP-соединения, включая PPTP, кроме L2TP, могут использовать MPPE. MPPE применяет шифр потока RSA RC4 и действует только совместно с методами аутентификации TLS или MS-CHAP (версии 1 или 2). MPPE может использовать 40-, 56-или 128-разрядные ключи шифрования (40-разрядный ключ предназначен для обратной совместимости и международного использования; 56-разрядный ключ — для международного использования (он подчиняется американским законам экспорта шифрования); 128-разрядный ключ действует в Северной Америке). По

умолчанию в процессе установки соединения выбирается наибольшая длина ключа, поддерживаемая вызывающим и отвечающим маршрутизаторами. Если отвечающий маршрутизатор требует ключ большей длины, чем поддерживаемый вызывающим маршрутизатором, то доступ запрещается;

• IPSec. Для соединений по требованию, применяющих L2TP поверх IPSec, шифрование определяется путем генерации сопоставления безопасности (security association — SA). Доступные алгоритмы шифрования включают DES с 56-разрядным ключом и 3DES, использующий 56-разрядный ключ и предназначенный для высоконадежных сред. Начальные ключи шифрования поступают от процесса аутентификации IPSec.

Для VPN-соединений Windows 2000 применяет MPPE с протоколом PPTP и шифрование IPSec с протоколом L2TP.

Настройку шифрования для удаленного подключения нужно выполнять в следующей последовательности:

1) раскройте меню Start\Programs\Administrative Tools *(Пуск\ Программы\ Администрирование)* и щелкните по кнопке *Routing and Remote Access (Маршрутизация и удаленный доступ);*

2) в списке имен сервера щелкните по кнопке *Remote Access Policies (Политики удаленного доступа);*

3) на правой панели щелкните правой кнопкой мыши по кнопке *Политика удаленного доступа,* которую хотите конфигурировать, и выберите в контекстном меню команду Properties *(Свойства);*

4) щелкните по кнопке *Edit Profile (Изменить профиль);*

5) на вкладке Encryption *(Шифрование)* задайте нужные параметры и щелкните по кнопке *ОК;*

6) щелкните по кнопке *ОК,* чтобы закрыть диалоговое окно свойств.

4.4. Технологии администрирования по обеспечению безопасности ИС функционирования сети

4.4.1. Общие положения по организации администрирования защиты в ИС

При организации защиты любой ИС от вторжения рекомендуется пользоваться определенным набором правил, который может носить типовой характер:

1) постоянно следить за тем, не появились ли отклонения от нормального хода работы системы. Нужно обращать внимание на все необычное, например на непонятные журнальные сообщения или изменение характера использования какой-либо учетной записи (резкое усиление активности, работа в необычное время, работа во время отпуска владельца учетной записи);

2) необходимо учиться защищать ОС своими силами, иначе не избавиться от различного рода высокооплачиваемых консультантов по вопросам безопасности, которые будут пугать ваших руководителей рассказами о том, насколько беззащитны ваши системы. Такие специалисты обучены грамотно доказывать, почему вам нужно вложить «всего» 50 тыс. долл. в обеспечение полной безопасности системы;

3) нужно устанавливать ловушки для обнаружения попыток вторжения. Необходимо следить за отчетами, которые генерируются программами (для Unix-систем — это tripwire, tcpd и crack). Незначительная проблема, проигнорированная в отчете, к моменту получения следующего отчета может перерасти в катастрофу;

4) нельзя оставлять без присмотра файлы, которые могут представлять интерес для хакеров и не в меру любопытных сослуживцев. Коммерческие тайны, персональные досье, бухгалтерские ведомости, результаты выборов — за всем этим «нужен глаз да глаз». Надежнее зашифровать данные, чем просто пытаться предотвратить к ним несанкционированный доступ. В организаций должен существовать порядок работы с секретной информацией;

5) следует «затыкать дырки», через которые хакеры могут получить доступ к системе. Нужно знакомиться с бюллетенями фирм-производителей и списками рассылки по вопросам защиты, чтобы своевременно узнавать о выходе «заплат». Следует отключить ненужные сервисы;

6) необходимо сделать так, чтобы в системе не было мест, где хакеры могли бы закрепиться. Хакеры часто вламываются в одну систему, а затем используют ее как базу для операций по взлому других систем. Анонимные FTP-каталоги с возможностью записи, групповые учетные записи, учетные записи с плохо подобранными паролями — вот основные уязвимые места.

Кроме того, необходимо рассмотреть основные источники нарушений. *Первый источник* нарушений — это уровень безопасности системы. Многие компоненты программного обеспечения можно сконфигурировать в режиме полной или не очень полной безопасности (открытой и полуоткрытой). К сожалению, по умолчанию чаще всего принимается второй вариант. Хакеры вламываются в системы, иезуитски эксплуатируя функциональные возможности, с миссионерской щедростью предоставленные разработчиками в надежде сделать работу пользователей удобнее и гуманнее: учетные записи без паролей, глобальный совместный доступ к жестким дискам и т.д. Одна из самых важных задач, связанных с обеспечением безопасности системы, — убедиться в том, что, заботясь о благополучии пользователей, в системе сохранились действенные инструменты защиты.

Проще всего устранить эти проблемы, хотя их может быть очень много и не всегда очевидно, что именно следует проверять. Ббль-

шая часть усилий, затраченных за несколько последних лет на разработку программных средств защиты, была связана с анализом причин, по которым система может непреднамеренно оказаться открытой для вторжений.

Второй источник нарушений — воздействие человеческого фактора на функционирование системы. Пользователи (и администраторы) системы часто являются ее слабейшим звеном. Например, компания America Online печально прославилась тем, что ее многократно атаковали хакеры, притворявшиеся служащими компании. Они посылали письма потенциальным жертвам с просьбой выслать пароли для системного теста или плановой проверки учетной записи. Наивные пользователи часто выполняли такие просьбы (некоторые до сих пор так делают). Есть масса разновидностей подобного шарлатанства. Одна из задач системного администратора заключается в обучении пользователей правилам техники безопасности. Многие пользователи, начиная работать в Интернете, часто не подозревают, сколько там хакеров. Надо научить их выбирать качественные пароли и хранить их, а главное — никогда не общаться с незнакомыми людьми. Администратор должен не забыть в своих наставлениях упомянуть об неэлектронных средствах коммуникации (в умелых руках телефон тоже может оказаться опасным оружием).

Третий источник нарушений — это ошибки в программах. За много лет в программном обеспечении (включая сторонние программы, как коммерческие, так и бесплатные) было выявлено несметное количество ошибок, связанных с безопасностью. Используя незаметные программистские просчеты или архитектурные зависимости, хакерам удавалось манипулировать системой по своему усмотрению. Что может сделать в этом случае администратор? Немногое, по крайней мере, до тех пор, пока ошибка не будет выявлена, а разработчик не исправит ее или не выпустит «заплату». Быть в курсе последних событий — обязанность администратора.

4.4.2. Процедурные технологии администрирования по обеспечению безопасности ИС

Организация борьбы и предупреждения несанкционированного доступа (НСД) в систему требует, как уже отмечалось ранее, комплексного подхода к администрированию процессов защиты ИС от вторжения. При этом сами технологии администрирования основаны на процедурах организационно-программной реализации отдельных операций по защите. Это дает возможность создать на базе типовых процедур комплексы процедурных технологий администрирования, которые могут быть скомпонованы в разных

последовательностях, обеспечивая в любой системе многоуровневую защиту. Рассмотрим также процедурные технологии администрирования, применяемые в ОС Unix-системах.

В первую очередь, интересны технологии файловой и парольной защиты. В Unix-системах в качестве файла передовой линии защиты системы от захватчиков используется файл /etc/passwd.

В файле /etc/passwd (в некоторых системах также в файле /etc/shadow) содержатся сведения о том, кто может входить в систему и что он при этом имеет право в ней делать. Такой файл нужно поддерживать с особой тщательностью, стараясь не допускать ошибок и не загромождать его устаревшими данными. Так, во FreeBSD файл /etc/passwd генерируется на основании файла /etc/master.passwd и не должен редактироваться напрямую. Тем не менее не помешает в одинаковой мере защищать оба файла.

Другой инструмент безопасности — это регулярные (желательно каждый день) проверки: все ли учетные записи имеют пароль. В элементах файла /etc/passwd, содержащих описания псевдопользователей наподобие daemon (такие псевдопользователи являются владельцами некоторых системных файлов, но они никогда не регистрируются в системе), в поле пароля должна стоять звездочка (*). Она не соответствует ни одному паролю и, таким образом, предотвращает использование учетной записи, но для ее выполнения требуется наличие интерпретатора Perl версии 5 или выше.

Существует несколько специализированных программных пакетов, которые обеспечивают проверку файла /etc/passwd на предмет наличия проблем, связанных с безопасностью, хотя для поиска пустых паролей вполне достаточно и такой команды:

```
perl -F: -ane 'print if not $F[1];' /etc/passwd
```

Сценарий, выполняющий эту проверку и направляющий по электронной почте результаты администратору, можно запускать посредством демона cron. Дополнительно можно обезопасить себя с помощью сценария, который будет ежедневно сверять файл /etc/passwd с его версией за предыдущий день (это позволяет делать команда diff) и сообщать о выявленных различиях. Таким образом, дополнительно появляется возможность проверки правомерности внесенных изменений.

Доступ к файлам /etc/passwd и /etc/group следует организовать так, чтобы их могли читать все пользователи, но право на запись имел только пользователь root. Если в системе присутствует файл /etc/shadow, то он должен быть недоступен пользователям. Файл /etc/master.passwd во FreeBSD должен быть доступен лишь суперпользователю.

В Unix пользователи могут задавать собственные пароли. Это, конечно, очень удобно, но влечет за собой массу проблем, связанных с безопасностью. Выделяя пользователям регистрацион-

ные имена, следует обязательно давать им указания о том, как правильно выбрать пароль. Необходимо предупредить пользователей о недопустимости задавать в качестве пароля фамилии, инициалы, имена детей и супругов, а также слова, которые можно найти в словаре. Пароли, сконструированные на основе таких личных данных, как номера телефонов и адреса, тоже легко поддаются расшифровке.

Рекомендуется выбирать пароль, состоящий не менее чем из восьми знаков; при этом допускается использование цифр, знаков препинания, а также прописных и строчных букв. Бессмысленные сочетания знаков, слогов, первые буквы слов легко запоминаемой фразы — вот самые лучшие пароли. При этом легко запоминаемая фраза не должна быть одной из широко распространенных. Лучше придумать собственную.

Во многих системах значащими являются лишь первые восемь символов пароля. Остальные просто игнорируются.

Пароли обычно меняются с помощью команды passwd. Существует множество ее эквивалентов, призванных заставить пользователей выбирать более удачные пароли. Рекомендуется применять для этой цели известный многим пакет npasswd, поддерживаемый Клайдом Хувером (Clyde Hoover) из университета штата Техас (США). Пакет можно найти по адресу http://www.utexas.edu/cc/unix/software/npasswd.

В Solaris входит версия программы passwd, заставляющая пользователей придерживаться определенных правил, например не выбирать в качестве паролей свои регистрационные имена. Правила построения паролей задаются в файле /etc/default/passwd.

Модель аутентификации в Red Hat основана на подключаемых модулях аутентификации (Pluggable Authentication Modules — PAM). В связи с этим команда passwd подчиняется набору правил имеющегося модуля, описанных в файле /etc/pam.d/passwd. Получить более подробную информацию о модулях PAM можно по адресу http://parc.power.net/morgan/Linux-PAM/index.html.

Каждый элемент файла /etc/passwd состоит из семи полей; второе поле содержит строку, которая представляет собой зашифрованный пароль пользователя. Для того чтобы могли работать такие команды, как Is и ей подобные, к файлу /etc/passwd должны иметь доступ для чтения все пользователи. Таким образом, зашифрованная строка пароля доступна каждому пользователю системы. Злоумышленнику ничего не стоит представить в зашифрованном виде целый словарь или отдельные слова и провести сравнение с указанным полем во всех элементах файла /etc/passwd. При совпадении сравниваемых объектов злоумышленник получает в свои руки пароль.

Насколько это опасно? В 80-е гг. XX в. существовал, по крайней мере, один способ очень быстрой расшифровки паролей, но ря-

довому хакеру приходилось довольствоваться библиотечной функцией crypt(), Для того чтобы шифровать слова из словаря для их последующего сравнения. Но в то время быстродействующий компьютер мог выполнять лишь порядка нескольких сотен операций шифрования в секунду. Последние исследования показывают, что с помощью специализированного компьютера стоимостью 1 млн долл. можно взломать любой 56-разрядный ключ DES за считанные часы.

Из этого следует настоятельная необходимость в ограничении доступа пользователей к зашифрованным строкам паролей. Самый распространенный способ — поместить пароли в отдельный файл, который может читать только суперпользователь, а остальную часть файла /etc/passwd оставить без изменений. Файл, содержащий информацию о паролях, называется файлом теневых паролей (часто он имеет имя /etc/shadow). Большинство производителей Unix-систем, в том числе наших тестовых, реализует механизм теневых паролей.

В HP-UX для работы механизма теневых паролей требуется установить вспомогательный программный пакет. Он содержит множество дополнительных средств защиты, но в то же время на порядок усложняет задачу администрирования.

Трудности также создаются тогда, когда учетная запись используется более чем одним человеком. Регистрационные имена групп (например, guest или demo) — удобная лазейка для хакеров, поэтому применять их не следует.

Нельзя допускать, чтобы пользователи делили учетные записи с членами семьи или друзьями.

Во многих организациях учетная запись root является групповой. Это опасно! Рекомендуется контролировать предоставление прав суперпользователя с помощью программы sudo.

Но пароль пользователя root следует модифицировать регулярно. При вводе он должен легко «скатываться» с пальцев, чтобы его нельзя было угадать, следя за движением пальцев по клавиатуре. Многие работают с программой sudo, но к выбору пароля суперпользователя все равно надо относиться с особой ответственностью.

Многие системы, поддерживающие теневые пароли, позволяют реализовать механизм так называемого устаревания паролей, при котором пользователей принуждают периодически менять таковые. На первый взгляд, это хорошая идея, однако на практике ее реализация влечет за собой определенные проблемы. Не всякому пользователю по душе замена пароля, поскольку она требует определенных усилий по его поиску и запоминанию. Обычно для пароля выбирается простое слово, которое легко вводится и запоминается, и когда подходит время замены, многие пользователи, не желая себя утруждать, опять берут предыдущий пароль. Таким образом, дискредитируется сама идея.

Особенностью использования root является то, что его идентификатор равен нулю. Поскольку в файле /etc/passwd может быть несколько элементов, для которых установлен этот идентификатор, существует и несколько способов входа в систему в качестве суперпользователя.

Один из способов, который хакеры, получив доступ к интерпретатору команд суперпользователя, широко применяют для открытия «черного хода», заключается в редактировании файла /etc/passwd посредством ввода в него новых регистрационных имен с идентификатором пользователя, равным нулю. Поскольку такие программы, как who и w, работают с регистрационным именем, записанным в файле /etc/utmp, а не с идентификатором владельца регистрационного интерпретатора, они не в состоянии разоблачить хакера, который выглядит как рядовой пользователь, а на самом деле зарегистрирован в системе в качестве суперпользователя.

Спасение от такого вероломства — применение интерпретатора Perl версии 5 и выше, подобно тому, как он использовался для поиска учетных записей без паролей:

```
perl -F: -ane 'print if not $F[2];' /etc/passwd
```

Этот сценарий отображает любые элементы файла passwd, в которых идентификатор пользователя не указан или равен нулю. Сценарий можно адаптировать для поиска в файле элементов с подозрительными идентификаторами групп или идентификаторами пользователей, совпадающими с идентификаторами руководящих сотрудников организации. Пристального внимания заслуживают, кроме того, элементы файла passwd, в которых нет имени пользователя либо вместо имени стоят знаки препинания. Эти элементы могут показаться не имеющими смысла, но очень часто они позволяют свободно входить в систему.

Программы, которые запускаются с измененным идентификатором пользователя, особенно те, для которых установлен идентификатор пользователя root, являются источником проблем, связанных с безопасностью системы. Теоретически команды с установленным битом SUID (Set User ID — смена идентификатора пользователя), поставляемые вместе с операционной системой, являются безопасными. Тем не менее огрехи в защите обнаруживались в прошлом и, несомненно, будут обнаруживаться в будущем.

Самый надежный способ уменьшения количества проблем, вызванных сменой идентификатора, — это сведение к минимуму числа программ с установленным битом SUID.

Сценарии интерпретатора команд автоматически ставят систему под угрозу. Они допускают множество способов настройки, поэтому их легко обмануть. Интерпретатор, запускаемый для выполнения сценария, не всегда читает пользовательские файлы конфигурации, но есть и другие способы воздействия на него:

посредством пользовательских переменных среды, содержимого текущего каталога, способа вызова сценария и т.д.

Не существуют правила, гласящего, что программы с установленным битом SUID должны запускаться от имени суперпользователя. Если нужно всего лишь ограничить доступ к файлу или базе данных, достаточно добавить в файл /etc/passwd псевдопользователя, единственное назначение которого будет заключаться во владении требуемыми ресурсами. Следуйте обычным соглашениям о добавлении псевдопользователей: используйте низкое значение SUID, поставьте в поле пароля звездочку и сделайте начальным каталогом псевдопользователя каталог /dev/null.

Большинство систем позволяет отключать выполнение программ с установленными битами SUID и SGID (Set Group ID — смена идентификатора группы) в отдельных файловых системах с помощью опции -o nosuid команды mount. Чаще всего это файловые системы, содержащие начальные каталоги пользователей или смонтированные из ненадежных доменов.

Полезно периодически сканировать диски на предмет выявления новых программ с установленным битом SUID. Хакер, взломавший систему, без особых усилий может создать собственный командный SUID-интерпретатор и утилиту, которая облегчит ему последующий вход в систему.

В Unix-системах есть много файлов, для которых должны быть установлены специальные права доступа, позволяющие предупреждать возникновение проблем, связанных с безопасностью. Некоторые поставщики выпускают дистрибутивы, в которых права доступа заданы в расчете на собственную «дружественную» среду разработки. ИС такие установки могут оказать «медвежью услугу».

В некоторых системах специальный файл /dev/kmem позволяет получить доступ к виртуальному адресному пространству ядра. Его используют те программы (например, ps), которые работают со структурами данных ядра. Право чтения указанного файла должно предоставляться только его владельцу и членам соответствующей группы. Если необходимо получить доступ к файлу из определенной программы, то для нее должен быть установлен идентификатор группы, владеющей этим файлом (обычно это kmem), и бит SGID.

В прошлом некоторые поставщики выпускали дистрибутивы, в которых файл /dev/kmem был доступен для чтения всем пользователям. Это создавало серьезную угрозу для безопасности системы, потому что опытный программист, получив доступ к данным и буферам ядра, мог найти там незашифрованные пароли. Если в системе файл /dev/kmem могут читать все пользователи, то необходимо исправить это положение несмотря на то, что после внесения изменений некоторые программы перестали работать. Для них следует установить бит SUID и идентификатор той группы, которой принадлежит файл /dev/kmem.

Также необходимо проверить права доступа к файлам /dev/drum и /dev/mem, если они присутствуют в системе. Эти файлы позволяют получить свободный доступ к системной области подкачки и физической памяти и потенциально так же опасны, как и файл /dev/kmem.

Файлы /etc/passwd и /etc/group должны быть доступны для записи только владельцу (пользователю root) и его группе. Режим доступа в данном случае будет 644. Группа должна быть какой-нибудь системной группой (обычно это daemon). Чтобы пользователи, не имея права записи в файл /etc/passwd, могли изменять свои пароли, команда passwd (владельцем которой является пользователь root) выполняется с установленным битом SUID.

Пользователи, относящиеся к категории «прочие», не должны иметь права записи в каталоги, доступные по анонимному протоколу FTP. Такие каталоги позволяют хакерам незаконно копировать программное обеспечение и другие важные файлы. При управлении FTP-архивом, допускающим добавление в него файлов, нельзя забывать регулярно просматривать каталог добавлений.

При настройке анонимного FTP-сервера в каталог -ftp/etc/ passwd обычно копируется усеченный файл паролей (с сохранением его структуры), что позволяет правильно работать программе Is. Но необходимо удалить зашифрованные строки паролей.

Еще один потенциальный источник проблем — файлы устройств для разделов жесткого диска. Наличие права чтения и записи такого файла равнозначно наличию аналогичных прав для любого элемента файловой системы этого раздела. Право чтения-записи может иметь только суперпользователь. Члены группы иногда могут получать право чтения, что позволит им выполнять резервное копирование. Для категории «прочие» права доступа не устанавливаются.

Контрольные вопросы

1. Сформулируйте главные принципы, регулирующие международное использование средств массовой информации.
2. Приведите основные международные и отечественные нормативные акты обеспечения ИБ при администрировании.
3. Дайте классификацию информационных угроз функционирования ИС.
4. Перечислите угрозы снижения сетевой безопасности.
5. Перечислите функции безопасности Windows 2000.
6. Что такое политика безопасности?
7. Составьте план сетевой безопасности ИС.
8. Как организуется и реализуется безопасная работа сети при удаленном доступе?
9. Перечислите правила администрирования при защите ИС.
10. Опишите технологии файловой и парольной защиты ИС на примере ОС Unix.

Глава 5
УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ И РЕСУРСАМИ ИС

5.1. Администрирование ИС на базе сетевых команд

5.1.1. Описание сетевых команд администрирования

Администрирование сетей строится в основном по методологии сценариев, которые представляют собой упорядоченный на-

Таблица 5.1

Файловые утилиты Unix

Команда	Фукнции	DOS-эквивалент
chgrp	Изменяет группу владельца файла	—
chown	Изменяет владельца файла	—
chmod	Изменяет права доступа к файлу	attrib
cp	Копирует файлы	copy, xcopy
dd	Проводит преобразование при копировании	—
df (disk free)	Выводит статистику файловой системы	ckdsk
du	Сообщает об использовании диска	—
find	Ищет файлы	—
In	Создает связи файлов	—
Is	Дает список содержимого каталога	dir
mkdir	Создает каталог	mkdir
mv	Перемещает файлы	ren
rm	Удаляет файлы	del
rmdir	Удаляет каталоги	rmdir
touch	Изменяет время последнего доступа к файлу	—

Таблица 5.2

Команды Unix для работы с данными

Команда	Функции	DOS-эквивалент
cat	Объединяет файлы	copy filel + Ше2
cut	Извлекает выделенную область	—
cmp	Сравнивает файлы	—
diff	Отображает различия между файлами	—
fold	Форматирует длинные строки по длине	—
grep	Ищет текст по образцу	—
head	Выводит начало файла	type filename
join	Объединяет строки различных файлов по общему полю	—
od	Выводит файл в восьмеричном формате	—
paste	Объединяет строки файлов	—
pr	Разбивает файл на страницы для печати	—
sed	Редактор потоков	—
sort	Сортирует текстовые файлы	sort
split	Разбивает файл на части	—
strings	Извлекает строки из файла	—
sum	Считает контрольную сумму файла	—
tail	Отображает конец файла	type filename
tr	Обеспечивает посимвольную перекодировку	—
uniq	Отображает вывод из отсортированных файлов без повторений	—
wc	Считает байты, слова и строки	—

бор команд сети ИС. Здесь важно осуществить описание оболочки сценария, по которому будет производиться набор команд. Для системы Unix в сценариях оболочек используются сотни различных команд.

Наиболее полезной командой является команда man, которая выводит на экран руководство пользователя. Ее можно использовать для получения информации о каждой из команд, указанных в табл. 5.1... 5.3. Здесь представлен сокращенный набор команд.

Можно выполнять различные задачи без понимания принципов работы каждого сценария, но будет тяжело работать без базо-

Таблица 5.3

Системные команды Unix

Команда	Описание	DOS -эквивалент
basename	Извлекает из имени маршрута часть, относящуюся к имени файла	—
date	Отображает или устанавливает системное время и дату	date, time
dirname	Извлекает из имени маршрута часть, относящуюся к имени каталога	—
echo	Отображает строку текста	echo
env	Устанавливает среду вызова команды	—
expr	Вычисляет выражение	—
false	Не делает ничего, но возвращает состояние ошибки	—
groups	Отображает принадлежность пользователя к группам	—
hostname	Отображает или устанавливает имя системы	—
id	Отображает действительные и текущие идентификаторы (ID) пользователя и группы	
logname	Отображает текущее имя пользователя	—
nice	Изменяет приоритет процесса	—
pathchk	Проверяет маршрут	—
printenv	Отображает переменные среды	echo %variable%
pwd	Отображает рабочий каталог	cd
sleep	Переходит в спящий режим на определенный период времени	—
stty	Отображает или изменяет параметры терминала	—
su	Изменяет идентификаторы пользователя и группы	—
tee	Перенаправляет вывод в несколько файлов	—
test	Проводит проверку состояний файлов и строк	—
true	Не делает ничего, но возвращает состояние успешного завершения	—
tty	Отображает имя терминала	—

Окончание табл. 5.3

Команда	Описание	DOS -эквивалент
uname	Отображает системную информацию	—
users	Выводит на экран имена пользователей, находящихся в системе	—
who	Отображает, кто находится в системе	—
whoami	Отображает текущий идентификатор пользователя	—

вых знаний об основной группе команд. Приведенный набор команд рассматривают как дополнительные компоновочные блоки, которые помогут освоить поставленную систему Unix.

5.1.2. Сетевые команды администрирования в Unix

Практически все оболочки поддерживают специальный синтаксис, позволяющий сценариям выглядеть как команды. Если первая строка сценария начинается с символов «#!» и следующего за ними пути к программе обработки сценария, то оболочка способна выполнить сценарий вызовом соответствующей программы обработки данного сценария.

Например, следующая строка указывает, что далее следует сценарий оболочки Bourne shell:

```
#!/bin/sh
```

Если запустить сценарий как команду Unix, то система проверит первые два байта на наличие последовательности символов «#!». Если такая последовательность обнаружена, то оболочка попытается запустить команду, следующую за символами «#!».

Это важно, потому что каждая оболочка поддерживает различные встроенные команды и поэтому необходимо точно определить, для какой оболочки написан сценарий. Если для работы выбирается оболочка C-shell, то все равно можно выполнять сценарии оболочки Bourne shell.

Это довольно общий подход. Оболочка Bourne shell используется для большинства сценариев. Специалисты рекомендуют писать сценарии именно для Bourne shell, конечно, если нет других оболочек.

После того как указана оболочка символами «#!», следующим шагом будет превращение сценария в выполняемую команду. Система Unix не нуждается в файловых расширениях, таких как команда .exe, предназначенная для выявления выполняемых фай-

лов. Вместо этого Unix использует права доступа для указания, является ли рассматриваемый файл выполняемым. Если для файла установлены права доступа на выполнение, то можно запускать его как команду.

Большинство файлов, помеченных подобным образом, — это программы, скомпилированные под формат архитектуры применяемой машины (например, Spare — исполняемый файл в среде системы Sun Spare под управлением Unix). Некоторые операционные системы включают в себя способность запуска с командной строки программ, написанных на языке Java (файлы с расширением .class). Все версии ОС Unix поддерживают способность запуска сценариев.

Для обозначения сценария как исполняемого потребуется установить право на исполнение файла с помощью команды chmod. Для того чтобы разрешить выполнение файла всеми пользователями, используют следующую команду:

```
chmod a+x scriptl
```

После того как выполнена подобным образом команда chmod, для выполнения сценария можно просто набрать его имя (в нашем случае — scriptl):

```
$   scriptl
```

Это простой сценарий оболочки, который иллюстрирует понятие написания сценариев.

Каждая оболочка обеспечивает набор возможностей, некоторые из которых приведены ранее. Из наиболее важных свойств оболочки, которые можно использовать, можно выделить следующие:

- перенаправление данных при вводе-выводе. Это свойство часто используется, так как управление входным и выходным потоками данных является основной характеристикой большей части сценариев. Вместе с использованием каналов эта функция станет одним из основных строительных модулей, позволяющих создавать сложные системы из маленьких программ типа «черный ящик»;
- конвейеризация команд. Это одна из часто используемых в оболочке конструкций. Конвейеризация команд позволяет выполнять операции над потоком данных, когда вывод предыдущей команды направляется на вход другой команды, которая, в свою очередь, может направить свой вывод дальше новым командам, и т.д.

Многие функции оболочки доступны через использование специальных символов, которые оболочка интерпретирует и на которые она реагирует соответствующим образом. Далее приведен набор нескольких специальных символов, понимаемых почти всеми оболочками.

Групповые символы. Символ «*» заменяет любую строку символов. Так, набор «*ain» соответствует именам again, ain, remain и прочим подобным.

Символ «?» представляет любой одиночный символ, т.е. fubar.? соответствует именам fubar.c, fubar.o и т.д.

Символы «[]» позволяют заменять набор или интервал выражений. Например, выражение [0-9] соответствует любому символу от 0 до 9. Также вы можете определить набор выражений, разделив их запятыми (например [1,3,5,a-c] соответствует символам 1, 3, 5, a, **Ь,** c).

Символ перенаправления. Для перенаправления выхода файла используется символ «>». Например, выполнение команды date>datefile приведет к записи в файл datefile вывода команды date. Выполнение команды date>>datefile присоединит вывод команды в конец файла.

Символы формирования конвейеров. Для передачи вывода одной команды на вход другой используется символ «|»: cat unsorted.dat | sort. В этом примере посылается вывод программы cat (действующей на файл unsorted.dat) на вход программы sort, которая выведет на экран упорядоченные данные.

Символ выполнения команд. Для выполнения команды в фоновом режиме в конец командной строки добавляется символ «&». Например, следующий пример создаст в файле dirs.dat перечень каталогов системы:

```
find / -type d -print > dirs.dat &
```

При этом команда find будет запущена в фоновом режиме и позволит продолжить работу. В одну и ту же командную строку можно вводить несколько команд, разделенных символом «;»:

```
ls * > file.dat; cat file.dat; cp file.dat file.old
```

В этом примере оболочка должна выполнить подряд три команды. Первая команда Is создает файл file.dat, команда cat выводит его на экран, а команда cp копирует его в файл file.old.

Использование специальных символов позволяет осуществить следующие функции:

• *замена символов.* Эта функция позволяет отмечать имена файлов с помощью специальных групповых символов. Интерпретатор команд системы DOS ограниченно поддерживает эту возможность, в то время как в оболочках системы Unix обычно предлагаются значительно более широкие возможности;

• *управление потоком.* Эта функция позволяет условно выполнять команду, что важно не только при написании сценариев для выполнения административных задач, но и при выполнении операций с несколькими файлами с командной строки. Все оболочки, рассмотренные в данном подразделе, имеют полный набор

конструкций передачи управления, включающий в себя циклы, циклы с условием while, блоки с условием if/else и операторы выбора;

•*подстановка команд.* Эта функция позволяет вычислять выражения, динамически помещая вывод командной строки в переменную среды. Например, можно пожелать сохранить текущий каталог в качестве переменной среды для дальнейшего использования. Можно этого добиться без непосредственного указания путей на формирование каталогов в программе. Механизм подстановки команд позволяет использовать выход команды pwd (от *англ.* print working directory — печать текущего каталога) в качестве переменной среды;

о *псевдонимы.* Эта функция позволяет создавать новые составные команды или переопределять уже существующие команды для включения часто используемых ключей в их выполнение по умолчанию. Например, можно так переопределить команду cd (от *англ.* change directory — сменить каталог), что приглашение командной строки будет содержать текущий каталог при каждой смене каталога;

•*описание функции.* Эта функция обеспечивает средство для расширения функциональности оболочки. Описав функции, можно не только улучшить читабельность программ, но и увеличить их надежность и производительность, создав команды общего использования, выполняющие многократно используемую последовательность действий;

•*передача параметров.* Эта функция нужна для написания общих сценариев и функций, способных выполнять операции с использованием параметров, переданных им при вызове;

x • *включение файлов.* Все новые процессы системы Unix порождаются системным вызовом fork(). Поэтому нельзя изменить родительскую среду дочерним процессом. При программировании сценариев такая ситуация не всегда желательна. В отличие от компилируемых бинарных файлов сценарии являются интерпретируемыми программами, которые нельзя связать с библиотеками функций. Чтобы пользоваться всеми выгодами использования библиотек, необходимо включать внешние файлы в сценарий оболочки в той же среде, что и выполняемый сценарий;

•*перехват сигналов.* Можно потребовать от сценария выполнения некоторых действий при получении определенного сигнала. Возможность управления сигналами облегчает написание утонченных программ, предназначенных для работы в фоновом режиме;

•*работа в фоновом режиме.* Как обеспечить мощную многозадачную операционную систему, если все команды выполняются последовательно? При этом требуется средство для сообщения

оболочке о выполнении процесса в фоновом режиме (нельзя путать с управлением заданиями);

• *управление заданиями*. Эта функция, хотя и не обязательная, может оказаться удобной, поскольку она обеспечивает больший контроль над процессами, выполняемыми в системе. Управление заданиями позволяет помещать процесс в фоновый режим, вре менно приостанавливать процесс и перемещать процессы из фо нового режима в приоритетный.

5.2. Организационно-правовое обеспечение администрирования

5.2.1. Общие рекомендации по формированию политики администрирования

Несмотря на то, что при обслуживании системы диктуются определенные требования, обязательно надо иметь набор правил, определяющих порядок выполнения основных задач администрирования (например, создания резервных копий, восстановления данных и т.д.). Для небольших систем действия «по ситуации» оправданы, поскольку администратор не связан жесткими правилами и обладает достаточной свободой. Однако по мере роста размера системы все больше проявляется необходимость в системной политике.

Организации формулируют специальные правила, регламентирующие взаимоотношения между сотрудниками. Например, это может быть перечень действий, которые разрешается и которые запрещается выполнять в ИС.

В среде предприятия автором системной политики часто выступает отдел кадров и работы с сотрудниками. Часто такие вопросы, как защита компьютеров, неправильное использование и правила доступа, объясняются человеческим фактором, а не проблемами работы компьютеров.

Почти любая политика основывается на определенных правилах. Политика системы является руководством о том, что можно, а что нельзя делать при использовании подсистем. Эти правила могут быть сформулированы вами или руководством организации и определяют действия пользователей.

При создании или изменении политики желательно учитывать следующие рекомендации:

• объяснить цели вашей политики. Многие пользователи очень негативно относятся к введению новых правил, которые им при дется выполнять. Они считают, что эти правила ограничивают их свободу действий. Приходится подробно объяснять, зачем нужны эти правила, что за счет этих правил обеспечиваются целостность

данных, защита информации и высокий уровень обслуживания, что выполнение этих правил позволяет удовлетворить требования всех пользователей;

• не разрабатывать политику в одиночку. Необходимо обсуждать ее со своими пользователями, прислушиваться к их мнению. Они могут предложить вариант, который не учтен. Участие пользователей в этом процессе облегчит задачу последующих изменений политики, они не будут пугаться этих изменений. Это позволит избежать противопоставления администратора пользователям. Можно даже заставить пользователей выработать политику. В этом случае все правила будут выполняться гораздо строже, чем можно было бы надеяться;

• доводить политику до сведения пользователей. Необходимо напоминать пользователям о том, что разрешено, а что запрещено; проверять, знают ли новые пользователи правила, которые необходимо соблюдать. Простого разговора иногда бывает недостаточно. Необходимо заставить пользователей подписать договор об обслуживании и о выполнении всех правил, которые перечислены в договоре. Этот договор защитит администратора и даст ему средства для наказания виновных;

• использовать правила, разработанные другими администраторами. Если в данный момент у администратора нет сформированной политики, то необходимо получить разрешение у администратора другой подобной организации скопировать его правила;

• остерегаться создания слишком общих правил, которые в результате будут бессмысленны или будут мешать работе. Политика, запрещающая уничтожение коммерческих данных, автоматически запрещает пользователям стирать файлы и освобождать дисковое пространство. Если пользователи не смогут удалять ненужную информацию, то дисковое пространство вскоре будет исчерпано. Кроме того, запись нового файла поверх старого — это также стирание старой версии, поэтому обновление версий также становится невозможным. Необходимо отличать допустимое использование системы от намеренного вредительства.

Часто политика, разработанная отделом кадров и работы с сотрудниками, запрещает нецелевое использование и манипуляции с компьютерами и оборудованием, предназначенным для обработки данных. Выключение компьютера также является манипуляцией. При выполнении реальной работы пользователи постоянно манипулируют оборудованием, поэтому такая политика бессмысленна.

Политика связана с правовыми вопросами. Иногда невозможно решить, кто имеет право использовать компьютеры, а кто — нет. Вопросы дисциплины, как правило, также находятся в ведении другого подразделения.

5.2.2. Правовое обоснование администрирования сети

Поскольку компьютеры содержат большой объем информации и постоянно обмениваются ею с другими компьютерами, стало довольно просто накапливать и распространять данные о пользователях. Каждый год вокруг вопроса о распространении информации, в частности сведений о пользователях, возникают споры. Предоставление доступа к информации о пользователях и мониторинг электронной почты часто становятся объектом судебного разбирательства.

Наилучшая защита — удостовериться в том, что пользователи знают, какой уровень конфиденциальности можно им предоставить. Необходимо объяснить пользователям, могут ли посторонние отслеживать их действия, раскрыть им, можно ли передавать по электронной почте секретные данные, в каких случаях информация, которую они хранят на сервере, может стать известной посторонним.

Необходимо быть осторожным с заявлениями о том, что администратор никогда ни при каких условиях не будет разглашать информацию. Судебное постановление заставит это сделать. Но если не согласиться предоставить имеющуюся информацию, могут возникнуть проблемы с правовыми органами. Учитывая возможность подобной ситуации, надо включить в политику соответствующие правила и удостовериться, что пользователи знают о них.

Торгующие компании должны учитывать, какие данные о покупателях не подлежат огласке. Чем больше данных хранится в компьютере, тем большее значение имеет защита компьютера.

Если безопасность компьютера очень важна, то нужно рассмотреть вопрос использования идентификационных карточек. Для входа в систему удаленный пользователь должен иметь такую карточку, называемую digital token card, а также знать пароль. Эти карточки, устройство для их чтения и соответствующее программное обеспечение вызовут дополнительные расходы, однако существенно повысят безопасность системы.

Политика администрирования должна защищать его. Единственный способ убедиться в этом — проконсультироваться с юристом. Запуск любой ОС требует вмешательства юридических органов.

К правовым вопросам, касающимся распространения информации о пользователях, наше общество обязательно создает новые правовые проблемы, как будто специально предназначенные для того, чтобы усложнить жизнь системному администратору. Поскольку он отвечает за происходящее в системе, то к нему всегда можно предъявить претензии через суд. С другой стороны, в его распоряжении есть политика, которая защитит в случае противоправных действий пользователей и даст возможность организации отреагировать на нарушения.

В среде финансов и бизнеса манипулирование данными является преступлением (конечно, учитывается, какое именно манипулирование было проведено). Поскольку здесь компьютеры содержат финансовую информацию, сохранение целостности данных, создание резервных копий и восстановление информации является правовым вопросом.

Шифрование поможет решить некоторые проблемы с защитой, по крайней мере, усложнит несанкционированное копирование информации. Однако оно само по себе может вызвать юридические проблемы.

Возможно, системному администратору придется отвечать за восстановление данных, закодированных служащими, которые были уволены. Ему необходимо также следить за правильным использованием кодирующего программного обеспечения. Он совместно с администрацией организации отвечает за содержимое личных Web-страниц, которые размещены на сервере фирмы. В этих страницах не должно быть клеветы. Также не должны нарушаться авторские права и торговые марки (включая изображения и логотипы) и не должно быть случаев распространения конфиденциальных данных.

Политика системного администрирования определяет поведение в различных ситуациях. Она определяет ограничения на использование вычислительной техники. С другой стороны, договор об уровне обслуживания содержит список тех услуг, которые он должен предоставить пользователям.

5.2.3. Документационное сопровождение администрирования

Для администрирования сети системы с пользователями составляется договор об уровне обслуживания, в котором описаны все виды услуг, которые система обещает оказывать, а также обязательства обеих сторон.

Основной проблемой при выполнении соглашения о предоставлении услуг становятся ситуации, развитие которых трудно контролировать. Например, нельзя полностью предотвратить возможность поломки оборудования. Нельзя предугадать, в какой момент времени все телефонные линии будут полностью загружены из-за какого-либо спортивного состязания, «имеющего историческое значение». Также нельзя быть уверенным в том, что не случится сбоя в электросети и ЭВМ не будут обесточены. Конечно, можно установить резервные генераторы, однако они очень дороги и не каждая организация может их себе позволить. Как правило, решение подобных проблем представляет собой компромисс между использованием дорогого высоконадежного обору-

дования и установлением приемлемой цены за предоставляемые услуги.

В некоторых случаях можно снизить уровень услуг и указать, что обеспечиваются максимально возможные услуги. Так поступают, когда пользователи имеют полный доступ к системе.

В договоре об уровне обслуживания должны быть описаны возможные ситуации. Должны быть упомянуты: возможность выхода из строя оборудования, перебои в электроснабжении, меры по созданию резервных копий и обеспечению целостности данных. В результате надо быть уверенным, что пользователи будут предъявлять только разумные требования, т.е. в договоре необходимо указать, какие виды услуг обеспечиваются, а какие услуги обеспечить невозможно. Это также поможет достигнуть взаимопонимания обеих сторон.

Договор об уровне обслуживания относится к внешней документации. Но при администрировании имеется большое количество внутренней документации, к оформлению и содержанию которой также предъявляются строгие требования.

Некоторые упоминавшиеся в данной главе процедурные документы можно получить по адресу www.admin.com. Часть из них описана в табл. 5.4.

Некоторые документы лучше оформлять на бумаге, в виде брошюр, а некоторые — в виде табличек, приклеиваемых к устрой-

Таблица 5.4

Перечень некоторых документов для администраторов сетей, находящихся на www.admin.com

Документ	Содержание
ugrad. policy	Соглашение о правилах пользования компьютерной лабораторией для студентов-новичков
grad. policy	Соглашение о правилах пользования компьютерной лабораторией для выпускников и преподавательского состава
sysadmin. policy	Правила для системных администраторов
services	Сервисы CSOPS, политики и приоритеты
hiring, quizl	Тесты для определения опыта работы
hiring. quiz2	Тесты на знание вопросов администрирования
localization	Контрольный список для локализации
amanda	Контрольный список для резервного копирования с помощью Amanda
tcp-wrappers	Контрольный список для установки TCP-оболочек

ствам. Внутреннюю документацию необходимо держать в определенном месте, например в каталоге /usr/local/doc.

На всех системных консолях должны быть прикреплены отпечатанные инструкции с указанием имени компьютера, последовательности его загрузки, архитектуры и специальных комбинаций клавиш, используемых для перезагрузки (например, [L1] + + [A], [Ctrl] + [Alt] + [Del]). Имя компьютера должно быть видно с другого конца комнаты. Поиск клавиши [L1] на терминале VT100 может оказаться сложной задачей.

Таблички с именем компьютера нужно наклеить и на другие связанные с ним устройства: дисководы, модемы, принтеры, ленточные накопители и т. д. Если компьютер — очень важный объект (например, сервер или центральный маршрутизатор), то нужно указать, где находится его выключатель. Если для начальной загрузки необходим гибкий диск или специальная карточка, то указывается, где они находятся. На файловый сервер необходимо наклеить перечень имен дисковых устройств, имен разделов, точек монтирования, адреса резервных суперблоков.

Для накопителей на лентах требуется указывать сведения о файлах устройств и командах, необходимых для доступа к ним. Лучшее место для этой информации — сам накопитель. Рекомендуется указывать тип лент, с которыми работает накопитель, ближайшее место, где их можно найти, и цену.

На принтерах нужно указывать их имена, краткие инструкции по печати и имена компьютеров, с которыми они работают (если таковые имеются). Сейчас принтеры уже начали поставляться с сетевыми интерфейсами и скоро станут «полноправными гражданами» сети.

Наиболее тщательно необходимо документировать схему сети. Следует пометить все кабели, обозначить коммутационные панели и розетки, промаркировать сетевые устройства. Не следует мешать электромонтерам вносить коррективы в документацию. В монтажном шкафу вешаются карандаш и бланки, чтобы техник смог сразу же зафиксировать, например, что кабель перекинут с одного устройства на другое. Зарегистрированные таким образом изменения можно перенести в память компьютера позже.

Центральный пункт, где собраны сведения о состоянии компьютера, — файл diary, в котором документируются основные события его «жизни» (расширения, ремонт аппаратной части, инсталляция основных программ и т.д.). Можно создать псевдоним электронной почты, указывающий на этот файл; тогда его копии будут рассылаться всем администраторам (это наиболее безболезненный и наименее организованный способ ведения записей).

Рекомендуется оставить печатный документ, который можно выдавать новым пользователям. В нем следует изложить местные

правила, порядок уведомления о неисправностях, имена и адреса принтеров, график резервного копирования и отключения и т.д. Такой документ позволит администратору сэкономить время. Эту информацию можно распространять и через Web-сервер.

Помимо этого своеобразного введения в локальную среду важную роль играют инструкции с наиболее распространенными пользовательскими командами, поскольку в таких средах пользо-иатели часто меняются и не обладают достаточными знаниями, например по Unix-системам (см. табл. 5.1...5.3). Применяются од-постраничные информационные листки о редакторе vi, системе mail, телеконференциях, входе и выходе из системы, X-среде и порядке использования man-страниц.

Во многих организациях команда системных администраторов и снабженцы полностью разделены и нет их интеграции.

Администраторам нужно знать, какая техника заказывается, иначе они не смогут решить, впишется ли она в имеющуюся инфраструктуру. Администраторы должны иметь возможность участвовать в составлении спецификаций, прилагаемых к заказам, потому что они могут сообщить полезные сведения о надежности оборудования и его поставщиках.

Участие системного администратора в решении таких вопросов особенно важно в организациях, которые должны покупать технику по минимальным ценам (это, например, правительственные учреждения и государственные университеты). В большинстве случаев при закупке можно предварительно указывать критерии соответствия предлагаемых изделий предъявляемым требованиям.

Эффект при подключении дополнительной рабочей станции зависит от многих факторов: какая она по архитектуре, какая по счету в инфраструктуре системы, достаточно ли места на ее диске для системных файлов, имеется ли свободный сетевой порт, будет ли она размещена в той части здания, где ее можно будет легко подключить к сети, насколько отличается ее ОС от уже используемых в организации и т.д.

Желательно участие в торговле с поставщиками (официально или по другим каналам). Системный администратор может добиться более выгодных условий, чем отдел снабжения.

Списание компьютера — болезненная процедура. Упрямые пользователи не желают расставаться со своими «любимцами», зная, что им придется изучать новую систему и переходить на новые прикладные программы. Руководители некоторых фирм убеждают себя, что новая система им не по карману, и принуждают сотрудников работать на старой. Обычно это заканчивается тем, что понапрасну тратится такая сумма денег, которой хватило бы не на одну новую систему. Старый компьютер VAX ежемесячно потребляет электроэнергии на сумму, превышающую его лик-

видационную стоимость, но попробуйте заставить пользователей смириться с его отключением!

Стоит только производительности аппаратуры возрасти, как программное обеспечение начинает тянуть ее вниз — увеличиваются его объем и сложность. После инсталляции новых программных средств старая техника работает медленно, иногда очень медленно.

Поскольку пользователи и руководители с неохотой соглашаются сдавать устаревшее оборудование в утиль, иногда системному администратору приходится самому проявлять инициативу. Самое убедительное доказательство — финансовая информация. Если можно продемонстрировать на бумаге, что затраты на эксплуатацию старого оборудования превышают затраты на его замену, многие возражения будут сняты.

Переход с одной системы на другую можно упростить, если держать оба компьютера в рабочем состоянии. Так можно оставить питание старой системы включенным, но уменьшить объем административного сопровождения. Можно прекратить обслуживание ее аппаратной части — пусть «хромает», пока не «умрет» сама собой. Пользователей можно соблазнить разными «приманками»: повышенной производительностью, программным обеспечением нового поколения и т.д.

Даже очень старому компьютеру можно найти применение, например в качестве сервера печати или гостевой станции. Если ваша организация коммерческая, то рассмотрите вопрос о передаче старой техники университету или школе.

С некоторых пор началось вторжение в компьютерную промышленность патентов на программное обеспечение. Этот вопрос имеет непосредственное отношение к системному администрированию.

В России в соответствии с патентным законом РФ от 07.02.2003 № 22-ФЗ предусматривается патентование алгоритмов и программ. Но, к сожалению, законодательная база в настоящее время плохо разработана.

Большое значение имеет организация конференций, выставок, которые очень важны для обмена технологиями и апробации систем. Также существуют группы поддержки ИС, например ОС Unix; их несколько (как общего плана, так и по различным версиям). Задача этих групп — помочь вам в контактах с людьми, которые пользуются тем же программным обеспечением. Перечень организаций, использующих ОС Unix, приведен в табл. 5.5. Существует также множество национальных и региональных групп.

Каждая организация издает свои информационные материалы и ежегодно проводит одну-две конференции. USENIX устраивает одну общую конференцию и несколько специализированных. UniForum, SUG и AUUG проводят крупные коммерческие выставки с конференциями.

Таблица 5.5

Организации, использующие ОС Unix

Название	URL	Комментарии
USENIX	www.usenix.org	Группа пользователей UNIX; занимается техническими вопросами
SAGE	www.sage.org	Гильдия системных администраторов, связанная с USENIX; проводит ежегодные конференции LISA
SANS	www.sans.org	Проводит конференции системных администраторов и администраторов защиты. Это менее техническая организация, чем SAGE, с акцентом на учебные пособия
EUROPEN	www.europen.org	Объединяет национальные группы, но практически прекращает функционирование. В настоящий момент действуют только NLUUG, DUUG, UKUUG и некоторые другие национальные группы
AUUG	www.auug.org.au	Австралийские пользователи UNIX, занимающиеся техническими аспектами и менеджментом
SAGE-AU	www.sage-au.org.au	Австралийское подразделение SAGE
JUS	www.jus.org	Японские пользователи UNIX, занимающиеся техническими аспектами и менеджментом

Проводятся также такие мероприятия, как Interop и UNIX Expo, — коммерческие выставки с небольшими техническими семинарами. Выставка Interop — значительное событие, а консультативные курсы Interop отличаются высоким качеством; упор делается на сети, а не конкретно на ОС UNIX. Выставка Interop раньше проводилась ежегодно, и ее с нетерпением ждали как технические специалисты, так и производители. Сейчас она проводится пять раз в год, а зарплата консультантов сокращена вдвое.

Структурно и технологически поддерживающей администраторов общественной организацией является гильдия системных администраторов SAGE. SAGE — гильдия системных администраторов USENIX — первая международная организация системных администраторов. Она развивает и рекламирует профессию системных администраторов, оказывая спонсорскую помощь в про-

ведении конференций и информационных программ. Подробную информацию о ее деятельности можно найти по адресу www.sage.org.

В настоящее время SAGE прорабатывает вопросы сертификации. Она планирует выработать процедуру сертификации системных администраторов, включающую в себя письменный экзамен и практикум. Это будет больше похоже на сертификацию Cisco CCIE (очень основательную как по части теории, так и по части практики), чем на сертификацию Microsoft MSCE (менее тщательную, включающую в себя только экзамены с выбором одного из нескольких вариантов ответа).

Поскольку профессия системных администраторов охватывает разные технические области и системы разных производителей, SAGE планирует организовать несколько сертификации. Они собираются выдавать базовый сертификат об общих знаниях и навыках, а также специализированные сертификаты по разным темам и системам различных производителей. Детали программы SAGE пока не проработаны. Последнюю информацию об этом можно найти на узле www.usenix.org/sage.

Еще одна важная задача, над которой работает SAGE, — программа помощи начинающим системным администраторам, которую могут оказывать их более опытные коллеги. Преподаватели работают один на один с учащимися раз или два в неделю. Проводится и более формальное обучение — члены сообщества SAGE преподают в университетских классах. Эта группа обменивается опытом и идеями через список почтовой рассылки sysadm-education. Для того чтобы на него подписаться, нужно отправить сообщение по адресу majordomo@maillist.peak.org и включить в него текст «subscribe sysadm-education».

Гильдия готовит один из разделов «;login:» бюллетеня USENIX. Раздел содержит новости, интересующие администраторов систем Unix, советы, обзоры и объявления. Гильдия SAGE выпустила уже серию кратких тематических буклетов. Список начала 2000 г. содержит:

- Job Description for System Administrators, редактор Tina Darmohray;
- A Guide to Developing Computing Policy Documents, редактор Barbara Dijker;
- System Security: A management perspective, David Oppenheimer;
- . Educating and Training System Administrators: A Survey, David Kuncicky и Bruce Wynn;
- Hiring System Administrators, Gretchen Philips;
- A System Administrator's Guide to Site Audits, Geoff Halprin;
- System and Network Administration for Higher Reliability, John Sellens;
- Effective Customer Support;

• Monitoring Techniques and Practices;
• The Role of Web Master.

Последние три брошюры вышли в 2000 г.

Вместе с USENIX, своей родительской организацией, SAGE каждую осень устраивает конференцию LISA. Проводимая USENIX/SAGE конференция LISA — самое масштабное и самое «техническое» из всех подобных мероприятий. Ее программа, как правило, включает в себя трехдневный семинар и трехдневные технические совещания, переговоры и консультации. Параллельно работают однодневные семинары по разным специализированным вопросам. Получить информацию об этой конференции можно по электронной почте (conference@usenix. org) или на узле www.usenix.org.

Помимо общенациональной группы SAGE сформированы несколько региональных групп, задача которых — оказывать администраторам помощь в регулярных контактах со своими коллегами. В настоящее время существует группа SAGE-AU в Австралии, SAGE-WISE в Уэльсе, Ирландии, Шотландии и Великобритании и SAGE-PT в Португалии. Контактную информацию этих региональных групп можно найти по адресу www.usenix.org/sage/locals.

5.2.4. Управление ресурсами администрирования в Unix

Существуют многочисленные списки рассылки для администраторов различных систем.

Для подписки на Sun Managers необходимо отправить письмо по адресу majordomo@sunmanagers.ececs.uc.edu, включив в него текст «subscribe sun-managers». Архивы здесь ведутся с 1991 г., они доступны по адресу www.latech.edu/sunman.html. Соответствующие группы новостей Usenet называются сотр.sys.sun.admin и comp.unix.solaris.

Одно время существовал список hpux-admin, вместо него выпускается другой по адресу www.egorups.com.

За информацией о списках рассылки, связанных с Linux, нужно обратиться по адресу www.redhat.com/mailing-lists. Можно подписаться прямо через Web. Списки называются Linux-xxx. К сожалению, ни один из них не адресован непосредственно системным администраторам.

Информацию о списках рассылки, связанных с FreeBSD, можно найти по адресу www.freebsd.org/handbook/eresources.html. Для подписки на любой из них нужно отправить сообщение «subscribe xxx» по адресу majordomo@freebsd.org. К сожалению, ни один из них не адресован непосредственно системным администраторам, но в списках freebsd-questions, freebsd.stable и freebsd-security можно найти много полезного.

Для системных администраторов имеется много ресурсов. Полезные ссылки можно найти на Web-страницах SAGE. Несколько адресов приведены в табл. 5.6.

Лучшими печатными ресурсами для администраторов Unix являются книги издательства O'Reilly. Серия начинается с книги «UNIX in a Nutshell», вышедшей более 20 лет назад. Сейчас серия включает в себя книги практически по всем важнейшим подсистемам и командам Unix. Кроме того, в этом издательстве выходят книги, посвященные Internet, Windows NT и другим темам, не связанным с Unix. Тим О'Рейли проводит ежегодные конференции, посвященные открытому программному коду, а также конференции на тему Perl, Java и TCL/Tk. За дополнительной информацией обращайтесь по адресу www.oreilly.com.

Стандартизация в одних случаях администраторам помогает (модемы разных производителей могут общаться друг с другом), а в других — вредит (протоколы OSI).

Задача стандартов заключается в том, чтобы предоставить пользователям возможность покупать совместимые продукты, созданные конкурирующими производителями. Некоторые организации, вовлеченные в процесс стандартизации, просто систематизируют и документируют существующую практику. Другие преследуют политические цели — стремятся к победе над конкурентами или сокращению объемов работ по приведению собственной продукции в соответствие с нормами.

Таблица 5.6

Некоторые Web-ресурсы для администраторов

Сайт	Содержимое
freshmeat.com	Большое собрание программного обеспечения для Linux
www.ugu.com	UnixGuru Universe, все для системных администраторов
www.stokely.com	Хорошее собрание ссылок на все, что необходимо системным администраторам
www.tucoes.com	Программное обеспечение для Windows и Mae, отобрано наиболее качественное
Slashdot.org securityfocus. com	Новости для любознательных. Информация, касающаяся безопасности; большая, но уязвимая база данных
google.com	Быстрый интеллектуальный поиск, особенно полезен для технического персонала
www.oreilly.com	Книги, немного коммерции и кое-что полезное

Часто крупнейшими заказчиками стандартизированных систем и приложений являются правительственные организации. Наличие стандартов позволяет им не привязываться к конкретным производителям. Однако крупные компании могут по собственной воле замедлять процесс стандартизации в ожидании, пока их продукты не закрепятся на рынке.

В США существует несколько органов по стандартизации (как официальных, так и неофициальных). В каждой из этих структур действуют свои правила приема новых членов, голосования и работы. С точки зрения администратора системы или сети самыми важными органами являются POSIX (Portable Operating System Environment — Организация по переносимым операционным системам) и IETF (Internet Engineering Task Force — Инженерная комиссия Интернет). Рефераты новых стандартов публикуются в материалах телеконференций comp.std.unix и comp.org.usenix, а также в «;login:», бюллетене USENIX.

Организация POSIX, являющаяся ответвлением IEEE, последние несколько лет занимается выработкой единого стандарта на ОС Unix. Open Group, лицензировавшая торговую марку Unix, основывает свою спецификацию Unix на стандарте POSIX. Каждая система, вызывающая Unix, теперь поддерживает интерфейсы POSIX. Альтернативные интерфейсы используются всего в нескольких доменах. К сожалению, POSIX ничего не говорит о том, что происходит на тех уровнях ОС, которые отданы на откуп системным администраторам.

Документы POSIX доступны только в печатном виде. Их издает IEEE Computer Society. В стандартах POSIX. 1 и P0SIX.2 (теперь это стандарты ISO 9945-1 и 9945-2) описываются POSIX-версии системных вызовов и команд Unix. В настоящее время эти стандарты совместно пересматриваются ISO, IEEE и Open Group. После этого все три организации будут пользоваться одним стандартом. Его законченная версия должна быть бесплатно доступна через Web.

Консорциум Open Group, ранее называвшийся X/Open, выработал подмножество стандартов POSIX, названное Single Unix Specification (SUS). Этот процесс начался с анализа всех систем и приложений, которые захотели контролировать члены консорциума. В результате было идентифицировано 1 170 различных широко используемых интерфейсов (команд, утилит, системных вызовов и т.д.). Проект получил рабочее название «Spec 1170».

Торговая марка Unix первоначально принадлежала AT&T Bell Labs. Затем она перешла к Unix Systems Laboratories (дочерней компании AT&T), затем к Novell и после этого к SCO. SCO предоставила безгонорарные лицензионные права консорциуму Open Group. Если ваш продукт соответствует спецификации Single UNIX Specification и у вас достаточно денег, то можете назвать свое

изделие «Unix». Специализированные лаборатории проведут сертификацию. Документ, определяющий спецификацию Single Unix Specification, можно приобрести или загрузить по адресу www. opengroup. org/publications.

Консорциум Austin Group (Austin — город в штате Техас, где впервые собрались его представители) состоит из организаций-участников IEEE, ISO и Open Group. Он поддерживает Web-узел с рабочими документами разных стандартов. Заинтересованных пользователей приглашают посещать узел, загружать черновики и принимать участие в процессе стандартизации. На этом узле нужно зарегистрироваться, но он не будет присылать спам или счета за загруженные документы. Его адрес: www.opengroup.org/austin.

Группа пользователей USENIX финансирует участие одного своего представителя в нескольких группах стандартизации. Его задача заключается не в том, чтобы определять направление будущего стандарта, а в том,чтобы информировать пользователей Unix о состоянии дел в области стандартизации и препятствовать появлению лжестандартов. Представитель USENIX собирает информацию, поступающую из многих источников, из которых наиболее заметными являются так называемые осведомители (snitches).

Осведомитель — это технический специалист, который посещает некоторое мероприятие и составляет о нем отчет. Такие отчеты ложатся в основу материалов, публикуемых в журнале «;login:». Кроме того, эти отчеты помогают понять, что предлагает стандарт и что в нем неправильно (или что в нем хорошо).

5.2.5. Взаимодействие Unix с Windows при управлении ресурсами ИС

Наиболее высокий уровень интеграции персональных компьютеров и платформы Unix достигается благодаря совместному использованию каталогов, размещенных на Unix-компьютере (или в специализированном файловом сервере Unix), настольными компьютерами, работающими под управлением Windows. Совместно используемые каталоги могут быть настроены таким образом, чтобы представляться частью среды Windows: либо в качестве логических дисков, либо в качестве дополнения дерева сетевых файловых систем Windows. Для выполнения этой функции можно использовать файловую систему NFS или CIFS.

Файловая система NFS (Network File System) предназначена для обеспечения возможности совместного использования файлов в сети Unix-компьютеров, где механизмы блокировки файлов и безопасности системы существенно отличаются от таковых в среде Windows. И хотя имеется множество программ, позволяющих монтировать NFS-каталоги в Windows, следует избегать это-

го, во-первых, из-за различия архитектур, а во-вторых, по причине того, что файловая система CIFS работает гораздо лучше.

CIFS (Common Internet File System — общая файловая система для Интернета) основана на протоколе SMB (Server Message Block — блок серверных сообщений). SMB стал дополнением к DOS, давно разработанным компанией Microsoft для того, чтобы операции дискового ввода-вывода переадресовывались в NetBIOS (Network Basic Input/Output System — сетевая базовая система ввода-вывода). Созданная компаниями IBM и Sytec система NetBIOS представляла собой примитивный интерфейс между сетью и приложениями.

В настоящее время пакеты SMB передаются через протокол NBT (NetBIOS over TCP), являющийся расширением NetBIOS. Упомянутые протоколы получили широкое распространение и стали доступными на многих платформах — от MVS и VMS до Unix и Windows.

Файловую систему CIFS на Unix-станциях реализует очень популярный пакет Samba. Он распространяется на условиях открытой GNU-лицензии.

Пакет Samba постоянно дорабатывается и расширяется. Он обеспечивает стабильный, проверенный механизм интеграции в сеть Unix компьютеров, работающих под управлением Windows. Преимущество Samba заключается в том, что достаточно инсталлировать только один пакет на Unix-компьютер и никакого дополнительного программного обеспечения на Windows-компьютер устанавливать не надо.

Файловая система CIFS предоставляет пять основных услуг:

- совместное использование файлов;
- сетевую печать;
- аутентификацию и авторизацию;
- преобразование имен;
- объявление о наличии сервисов (обзор файловых серверов и принтеров).

Большая часть функций пакета Samba реализована в двух демонах: smbd и nmbd. Первый предоставляет сервисы печати и доступа к файлам, а также сервисы аутентификации и авторизации, а второй управляет другими важными функциями CIFS: подсистемой преобразования имен и сервисными объявлениями.

. В отличие от NFS, которая жестко связана с ядром, пакет Samba не требует модификации ядра и запускается только как пользовательский процесс. Он связывается с сокетами, через которые посылаются NBT-запросы, и ждет запроса от клиента на доступ к ресурсу. Как только запрос поступает и аутентифицируется, демон smbd создает свой дубликат и запускает его от имени пользователя, сделавшего запрос. В результате все разрешения на доступ к Unix-файлам (включая групповые разрешения) остаются нена-

рушенными. Имеется только одна специальная функциональная возможность, которую демон smbd реализует сверх этого, — сервис блокировки файлов, позволяющий клиентским персональным компьютерам придерживаться привычной для них семантики блокирования.

Рассмотрим инсталляцию и конфигурирование пакета Samba. В настоящее время пакет Samba входит в комплект поставки систем Red Hat и FreeBSD (его местоположение — каталог /usr/ports), а в Solaris и HP-UX его нужно загрузить и инсталлировать самостоятельно. Пакет доступен по адресу www.samba.org.

Важно от используемой системы следует отредактировать файл smb.conf, указав в нем параметры конфигурации пакета Samba. В этом файле задаются каталоги и принтеры, предназначенные для совместного использования, а также права доступа к ним. Все опции задокументированы на man-странице, посвященной файлу smb.conf. Ознакомиться с документацией придется каждому, кто попытается интегрировать пакет Samba в сеть, в которой уже настроен совместный доступ к файлам Microsoft.

Необходимо понимать, какие угрозы безопасности возникают вследствие совместного использования файлов или ресурсов в сети. В пакете Samba имеются средства контроля безопасности, но они работают только тогда, когда кто-то их применяет. Чтобы обеспечить базовый уровень безопасности, нужно выполнить две процедуры:

- расположенная в файле smb.conf строка «hosts allow» задает адреса клиентов, которым разрешен доступ к ресурсам Samba. Необходимо удостовериться, что список содержит только проверенные IP-адреса (или диапазоны адресов);
- требуется блокировать доступ из Интернета к TCP-портам CIFS, соответствующим образом настроив фильтрующий брандмауэр.

Обычно пакет Samba работает нормально, не требуя вмешательства со стороны администратора. Но если при запуске возникли проблемы, можно обратиться к двум основным источникам отладочной информации: журнальным файлам, разным для каждого клиента, и команде smbstatus.

Местоположение журнальных файлов указано в файле smb.conf. В журнальном каталоге содержится файл для каждого клиента, обращавшегося к пакету. Демон smbd хранит эти файлы так, чтобы их размер не превышал заданной максимальной величины.

Следующие журнальные записи отражают успешные попытки соединений:

```
01/19/2000 17:38:01 pan (192.225.55.154) connect to service
trent
     as user trent (uid=8164, gid=10) (pid 16625) 01/19/2000
17:40:30 pan (192.225.55.154) connect to service
     silver-iw as user trent (uid-8164, gid=10) (pid 16625)
```

```
01/19/2000 17:43:51 pan (192.225.55.154) closed connection
     to service silver-lw 01/19/2000 17:43:51 pan
(192.225.55.154) closed connection
     to service trent
```

Команда smbstatus позволяет проверить текущие активные соединения и открытые файлы. Эта информация особенно полезна, когда приходится отслеживать проблемы блокировки (например, кто из пользователей открыл файл xyz для чтения-записи в монопольном режиме).

В первой части выходных данных перечислены ресурсы, к которым подключены пользователи, во второй части представлена информация об активных блокировках файлов, а в третьей части отображена статистика использования ресурсов, собранная демоном smbd. В выводе команды smbstatus содержится несколько длинных строк.

```
Samba version 2.0.5
Service    uid     gid    pid     machine

info       trent   staff  22545   pan
trent      trent   staff  22545   pan
Locked files: Pid  DenyMode  R/W  Oplock
Name

22545 DENY_NONE RDWR EXCLUSIVE+BATCH /home/trent/res alloc
2.xls
Share mode memory usage (bytes):
1048336 (99%) free + 168 (0%) used + 72 (0%) overhead =
1048576
(100%) total
```

Во многих версиях Unix можно запускать приложения Windows, но не все. Это делается разными методами, но все они обычно сводятся к созданию виртуальной машины, благодаря которой приложению «кажется», будто оно работает в Windows. Обычно эти виртуальные среды немного нестабильны, и далеко не все приложения хорошо функционируют в них.

Есть два пакета, которые позволяют запускать приложения Windows непосредственно в среде Red Hat Linux. Коммерческий продукт VMware (www.vmware.com) сделает весь компьютер единой виртуальной машиной, где сможет функционировать несколько операционных систем одновременно. Пакет Wine (www.winehq.com) реализует библиотеку Windows API в среде Linux, позволяя запускать приложения, которые не имеют доступа ни к одному драйверу.

Заслуживают внимания три пакета для Solaris. Наиболее интересным является SunPC — коммерческий продукт компании Sun, включающий в себя плату SBus с Intel-совместимым процессо-

ром, предназначенным для интерпретации инструкций ПК. Среди других приложений следует отметить SoftWindows компании FWB Software (www.fwb.com), полноценный эмулятор Windows, и NTRIGUE компании Citrix (www.citrix.com), которому для работы требуется отдельная Intel-система с Windows NT (эта программа позволяет пользователям запускать приложения Windows на рабочих станциях Solaris).

Sun бесплатно распространяет пакет StarOffice — аналог Microsoft Office для Solaris и Linux. В пакет входят основные офисные утилиты, такие как редактор электронных таблиц, текстовый редактор и простая СУБД. Эти программы могут читать и записывать файлы в форматах Microsoft Word и Microsoft Excel. Более подробную информацию о них можно найти по адресу http:// www. sun. com/products/staroffice.

Одним из достоинств оборудования для персональных компьютеров принято считать его невысокую стоимость. Поэтому даже при покупке высококлассного устройства следует учитывать целый ряд факторов.

Во-первых, если вы хотите оснастить свой компьютер не Windows, а какой-либо другой операционной системой, выясните, какие устройства в ней поддерживаются. Производители оборудования обычно снабжают все свои новые разработки Windows-драйверами, но в Unix они бесполезны. Некоторые поставщики стали предлагать драйверы для Linux.

Во-вторых, производительность компьютера зависит от многих факторов. В настоящее время тактовая частота процессора не является «узким местом». Недостаточная производительность подсистемы ввода-вывода приводит к снижению быстродействия всей системы. Выбирая устройство, необходимо ориентироваться на самую высокую скорость передачи данных и самую быструю шину. Надо быть особенно внимательными при покупке таких устройств, как дисковые контроллеры. Требуется убедиться в том, что они разработаны для действительно многопользовательской операционной системы и способны обрабатывать несколько запросов одновременно.

Еще один источник проблем составляют недорогие модемы, которые требуют наличия на компьютере программного обеспечения, выполняющего обработку сигналов. Маловероятно, что это программное обеспечение когда-нибудь будет перенесено в Unix, поэтому нужно выбирать модемы, имеющие собственный сигнальный процессор.

Первое, что хотят сделать пользователи, включив свой компьютер, — это проверить электронную почту. Обеспечение устойчивой электронной связи важно для большинства организаций. Причем это именно та область, где и персональные компьютеры, и Unix-серверы блестяще проявляют себя.

Персональные почтовые клиенты, такие как Microsoft Outlook, Netscape Messenger и Eudora компании Qualcomm, обладают широкими возможностями и намного превосходят старые программы чтения почты в Unix. Они позволяют пользователям обмениваться обычными и зашифрованными почтовыми сообщениями, посылать вложения и письма со специально отформатированным или даже цветным текстом. Все это — важные инструменты мира Интернет; давно ушли в прошлое программа /usr/ucb/mail и другие текстовые почтовые утилиты.

Организациям требуется предоставлять надежную почтовую связь сотням, а то и тысячам пользователей. Это возможно только там, где в качестве платформы выбрана Unix. Данная операционная система обеспечивает расширяемую, защищенную и конфигурируемую среду для приема и передачи почтовых сообщений через Интернет.

Сообщения могут храниться на Unix-сервере и быть доступными персональным почтовым клиентам с помощью протоколов IMAP и POP. Эта система является лучшей в мире. К тому же Unix не восприимчива к вирусам Windows.

Другое преимущество данного подхода, особенно в случае применения протокола ШАР, заключается в том, что почта хранится на сервере. Если какой-нибудь персональный компьютер сломался или вообще сгорел, это не значит, что папки с почтой пользователя безвозвратно пропали. Кроме того, IMAP позволяет пользователю получить доступ к своей почте откуда угодно: из дома, из интернет-кафе и т.д.

Резервное копирование данных на персональных компьютерах может стать серьезной проблемой, особенно сейчас, когда емкость обычного жесткого диска превышает 20 Гбайт. Имеется ряд подходов к решению этой проблемы, включая использование мощных сетевых средств резервного копирования, предлагаемых такими компаниями, как IBM и Seagate. Конечно, всегда можно воспользоваться локальным накопителем на магнитной ленте. Именно это — область, где коммерческие продукты оказываются наиболее эффективными.

Для экономии средств можно скопировать содержимое жесткого диска (всего или его части) на Unix-сервер, воспользовавшись для этой цели утилитой smbtar, включенной в пакет Samba. Правда, данный подход очень трудоемок.

В подобной ситуации наилучшее решение — вообще не создавать резервную копию содержимого компьютера. В организациях, где применяется такой подход, пользователей учат хранить все важные файлы на совместно используемом сетевом диске. Это позволяет конфигурировать все персональные компьютеры в пределах организации одинаково (имеются в виду инсталлированные приложения, конфигурация рабочего стола и т.д.). Если какой-

нибудь компьютер выходит из строя, то другой взамен него может быть загружен за несколько минут.

Также многим хотелось добиться максимальной отдачи от своего компьютера, установив на нем несколько операционных систем. Это стало возможным благодаря появлению средств мульти-системной загрузки. Данный термин означает, что в процессе начальной загрузки пользователь выбирает одну из нескольких операционных систем. Популярной стала комбинация Linux с Windows, особенно среди программистов, которым нужно быстро переключаться из одной среды в другую. В некоторых случаях можно даже совместно использовать одни и те же файловые системы во всех инсталлированных операционных системах.

Контрольные вопросы

1. Приведите основные группы команд Unix.
2. Опишите функции основных команд администрирования в Unix.
3. Перечислите основные правила администрирования при реализации политики сети.
4. Приведите перечень документов, необходимых для администрирования сетей.
5. Что такое SAGE?
6. Приведите перечень Web-ресурсов для администраторов.
7. Опишите стандарты POSIX.
8. Как производится интеграция ПК системы Unix с Windows?

Гл а в а 6 СЕТЕВЫЕ СЛУЖБЫ И ИХ МОНИТОРИНГ

6.1. Описание сетевых служб и протоколов

6.1.1. Адресация в сети Windows 2000

Большинство сетевых служб и технологий базируется на маршрутизируемом протоколе TCP/IP, являющимся стандартным стеком протоколов, обеспечивающих связь в среде от ЛВС масштаба предприятия до глобальных вычислительных сетей, включая Интернет.

Протоколом называют язык, на котором компьютеры передают информацию друг другу. Они представляют собой 32-разрядные двоичные числа, уникально идентифицирующие узлы сети. IP-адрес протокола IP состоит из двух частей: идентификатора сети и идентификатора узла. Поиск и подключение к узлам сети осуществляются через них. Обычно IP-адреса записываются в десятичном формате в виде четырех чисел по одному на восемь двоичных разрядов (октет), разделенных точками (например: 160.23.15.155). Адреса Интернета назначаются специальной организацией — группой Inter NIC (http://www.internic.net) и подразделяются на классы *A, B и C* (другие классы *D* и добычно не используются). Для определения кода сети и соответственно ее класса используется маска подсети (subnet mask) — это 32-разрядное число, состоящее из группы единичных битов для выделения кода сети и группы нулевых битов для выделения кода узла в сети.

Адреса класса *A* имеют маску 255.0.0.0 и первый октет адреса в диапазоне от 0 до 126. Они имеют очень большое число узлов (16 777 214). Адреса класса *B* присваиваются средним и большим сетям, а первый октет их адреса находится в диапазоне от 128 до 191; маска по умолчанию — 255.255.0.0, а число узлов может достигать 65 534. Сети класса *C* — небольшие (число узлов — не более 254), первый октет адреса таких сетей находится в диапазоне от 192 до 232, а маска по умолчанию будет представлена в виде 255.255.255.0. Идентификатор сети со значением 127 зарегистрирован для возвратной петли и диагностических функций.

Маршрутизируемый протокол TCP/IP обеспечивает коммутацию (перенаправление) пакетов данных на основе адреса назначения пакета. Одна из важных особенностей Windows 2000 — возможность подключения к Интернету и разнородным системам. Кроме того, в Windows 2000 реализованы усовершенствованные возможности защиты, которые разрешается использовать при подключении к системе по сети. Для поддержки этих возможностей в версию TCP/IP для Windows добавлены следующие протоколы и технологии:

• протокол PPTP (Point-to-Point Tunneling Protocol), позволяющий создавать защищенные виртуальные частные сети;

• протокол L2TP (Layer Two Tunneling Protocol), представляющий собой комбинацию протоколов PPTP и Layer 2 Forwarding (L2F). Последний является транспортным протоколом, позволяющим серверам удаленного доступа разделять удаленный трафик на пакеты протокола PPP (Point-to-Point Protocol) и передавать их по ГВС-соединениям серверу L2F (маршрутизатору);

• технология IP Sec (IP Security), используемая для шифрования сетевого трафика TCP/IP в целях обеспечения безопасного обмена данными.

В Windows 2000 также реализована поддержка устаревших систем и протоколов, созданных как фирмой Microsoft, так и другими фирмами. В их числе Apple Talk, IPX/SPX (Internetwork Packet Exchange/Sequenced Packet Exchange), NetBEUI.

Стек протоколов TCP/IP имеет четыре уровня: прикладной и транспортный уровни, уровень Интернета и сетевой уровень.

Прикладной уровень предоставляет приложениям доступ к сети. Он соответствует сеансовому, прикладному и представительному уровням модели OSI. На прикладном уровне применяют следующие стандартные утилиты и службы TCP/IP:

• протокол HTTP (HyperText Transmission Protocol) — используется для большинства WWW-коммуникаций. Windows 2000 включает клиента (Internet Explorer) и сервер HTTP — IIS (Internet Information Services);

• протокол FTP (File Transfer Protocol) — обеспечивает передачу файлов между компьютерами Интернета. В Windows 2000 имеются клиенты FTP — Internet Explorer и утилита командной строки FTP, а также сервер FTP, входящий в ITS;

• протокол SMTP (Simple Mail Transfer Protocol) — применяется почтовыми серверами для передачи электронной почты;

• протокол Telnet — используется для подключения к удаленным узлам сети методом эмуляции терминала. Это позволяет клиентам удаленно запускать приложения. В Windows 2000 включены клиент и сервер Telnet;

• DNS (Domain Name Service) — набор протоколов и служб TCP/IP-сети — позволяет использовать дружественные имена узлов сети вместо IP-адресов. В Windows 2000 включен DNS-сервер;

• протокол SNMP — позволяет централизованно управлять узлами сети.

Для взаимодействия со службами стека протоколов TCP/IP сетевым приложениям предоставляются два интерфейса: Winsock (версия API-интерфейса Sockets, реализованная в Windows 2000) и NetBIOS (стандартный API-интерфейс, используемый в среде Windows для межпроцессорной коммуникации) поверх TCP/IP (NetBT).

Протоколы *транспортного уровня* позволяют организовать связь между компьютерами. Здесь используются два протокола: TCP и UDP (User Datagram Protocol). Первый протокол обеспечивает приложениям надежную связь по логическому соединению, а протокол UDP обеспечивает связь без установления логического соединения и не гарантирует доставку пакетов. Этот протокол используется в том случае, когда приложения обмениваются небольшими объемами данных и за надежность их доставки отвечают сами приложения.

Протоколы *уровня Интернета* инкапсулируют пакеты в дата-граммы Интернета и управляют необходимыми алгоритмами маршрутизации.

Уровень Интернета в четырехуровневой модели соответствует сетевому уровню модели OSI и включает в себя пять протоколов, выполняющих совокупность функций, характерных для сетевого уровня.

Сетевой уровень стека протоколов TCP/IP (является основным и соответствует канальному и физическому режимам модели OSI) обеспечивает прием и передачу кадров — пакетов информации, пересылаемых по сети различных ЛВС и ГВС.

Все IP-адреса подразделяются на два типа: открытые и частные. *Открытые адреса* назначаются поставщиком услуг Интернета (Internet Service Provider — ISP) для подключения к Интернету. Для внутреннего использования узлов ЛВС, не нуждающихся в прямом доступе к Интернету, требуются IP-адреса без дублирования выделенных открытых адресов. В Интернете зарезервирована часть IP-адресов, которая названа частным адресным пространством. Адреса внутри частного адресного пространства называются *частными адресами,* и их использование помогает защитить сеть от взлома.

Так как частные адреса из Интернета недоступны, в ЛВС организации должен быть специальный сервер (прокси) для преобразования IP-адресов из частного адресного пространства локальной сети в открытые IP-адреса (или один IP-адрес), допускающие маршрутизацию. Другим вариантом может быть использование протокола трансляции NAT (Network Address Translation) частных IP-адресов перед их представлением в Интернете. Такое преобразование позволяет скрыть во внешних сетях IP-адреса внут-

ренней сети организации, что снижает риск несанкционированного доступа извне.

Протокол TCP/IP можно использовать в сетях разного масштаба — от небольших ЛВС до ГВС и Интернета. Если Windows Setup при установке системы обнаружит сетевой адаптер, то протокол TCP/IP будет установлен по умолчанию. Таким образом, протокол TCP/IP необходимо устанавливать, если по умолчанию применяется другой сетевой протокол. Инсталляцию протокола TCP/ IP нужно выполнять в следующей последовательности:

1) войти в меню *Пуск/Настройка* и щелкнуть по строке «Сеть и удаленный доступ к сети» («Network And Dial-Up Connection»);

2) в открывшемся окне щелкнуть правой кнопкой мыши по значку *Подключение по локальной сети* (Local Area Connection) и выбрать в меню команду *Свойства.* При этом откроется окно свойств локального подключения;

3) щелкнуть по кнопке *Установить {Install).* Откроется окно *Выбор типа сетевого компонента* (Select Network Component Type);

4) щелкнуть по кнопке *Протокол,* а затем — по кнопке *Добавить {Add).* При этом откроется окно *Выбор сетевого протокола {Select Network Protocol);*

5) выбрать «Протокол Интернета» («Internet Protocol, TCP/ IP») и щелкнуть по кнопке *ОК,* а затем — по кнопке *Закрыть.*

По умолчанию компьютеры с Windows 2000 пытаются получить конфигурационные параметры TPC/IP от сервера DHCP сети. Однако некоторым серверам (DHCP, DNS, WINS) необходимо назначать вручную статический IP-адрес. Для этого нужно выполнить следующие действия:

1) открыть окно свойств протокола;

2) указать IP-адрес, маску подсети и адрес шлюза по умолчанию. При наличии DNS-сервера настроить систему для использования DNS;

3) в полях «Предпочитаемый DNS-сервер» («Preferred DNS Server») и «Альтернативный DNS-сервер» («Alternate DNS Server») указать адреса основного и дополнительного серверов;

4) используя кнопку *Дополнительно {Advanced),* можно настроить дополнительные IP-адреса и шлюзы по умолчанию.

Для проверки и тестирования конфигурации протокола TCP/ IP можно использовать утилиты Ping и Ipconfig. Обе утилиты запускаются из командной строки. С помощью первой утилиты можно тестировать конфигурацию TCP/IP и выявлять ошибки соединений.

6.1.2. Описание некоторых сетевых служб

DNS (Domain Name Service) представляет собой иерархическую систему доменных имен, которая транслирует доменные име-

на в IP-адреса. Например, дружественное для пользователя доменное имя www.microsoft.com, которое легко запомнить, транслируется в адрес 207.46.130.149. В операционных системах Windows NT Server 4.0 и Windows 2000 Server служба DNS реализуется в форме сервера DNS. Клиенты Windows 2000 применяют DNS для расширения имен и поиска служб, включая поиск контроллеров домена, обслуживающего вход в систему. Служба DNS использует три основных компонента: распознаватели (клиенты), серверы имен и пространство имен домена. В простейшем случае распознаватель посылает запросы серверу DNS, который либо возвращает требуемую информацию или указывает на другой сервер имен, либо формирует отказ, если запрос не может быть выполнен.

Серверы имен иерархически группируются в домены, и, таким образом, может быть организована распределенная база данных. Она обеспечивает иерархическую структуру имен, распределенное администрирование и расширяемые типы данных, обладает высоким быстродействием и поддерживает практически неограниченный объем данных. Сервер имен содержит информацию об адресах компьютеров в сети, которая передается клиентам в ответ на их запросы.

Пространство имен домена представляет собой иерархическую группировку имен, а сами домены определяют различные уровни полномочий в иерархической структуре. Вершина иерархии называется *корневым доменом.* Ссылка на корневой домен обозначается точкой. В настоящее время можно выделить следующие *домены верхнего уровня:*

- .com — коммерческие организации;
- .edu — образовательные учреждения;
- .org — некоммерческие организации;
- .net — организации, предоставляющие услуги на базе Интернета;
- .gov — государственные учреждения;
- .mil — военные учреждения;
- .num — телефонные справочники;
- .arpa — используется для обратного сопоставления IP-адресов для компьютеров, использующих адреса, назначенные организацией IANA (Internet Assignet Number Authority);
- .xx — двухбуквенный код страны (например: ru — Россия).

Домены второго уровня могут содержать как узлы, так и другие домены, называемые поддоменами. Имя домена вместе с именем узла образует полное доменное имя. Таким образом, полное доменное имя компьютера состоит из последовательности имен компьютера и иерархии имен доменов (поддоменов).

Часть пространства имен домена, за которую отвечает один сервер имен, называется *зоной полномочий данного сервера* DNS. Процесс сопоставления (трансляции) имен, удобных для работы

пользователей, с числовыми IP-адресами, необходимыми для работы протокола TCP/IP, называется *разрешением имен.* Для разрешения имени узла или IP-адреса клиент (распознаватель) использует запросы трех типов: рекурсивные, итеративные и обратные. При рекурсивном запросе сервер имен возвращает требуемые данные или, если не существуют требуемые данные, сообщение об ошибке. Более типичен итеративный запрос, при котором сервер возвращает требуемую информацию либо отсылает к другому серверу DNS. Третий тип запроса, обратный, предназначен для поиска узла по его IP-адресу.

На формирование службы DNS влияют различные факторы: размер организации, размещение подразделений, требования по отказоустойчивости и др. Хотя Windows 2000 требует для разрешения имен сервер DNS, он не обязательно должен находиться на сервере Windows 2000 или даже в той же локальной сети. Для разрешения имени достаточно, чтобы Windows 2000 была настроена для обращения к действующему серверу DNS, например к серверу поставщика услуг Интернета. Внутри организации можно установить дополнительные DNS-серверы, независимые от Интернета.

Служба DNS в Windows 2000 Server дополнена новыми функциями, улучшающими совместимость компонентов сети и расширяющими диапазон применения DNS. Служба DNS тесно связана со службой каталогов Active Directory.

Для управления серверами DNS в Windows 2000 применяют консоль DNS.

Так как сервер DNS первоначально не имеет информации о пользовательской сети, он устанавливается как сервер кэширования Интернета, но содержит информацию только о корневых серверах Интернета. Первым шагом в настройке сервера DNS является определение иерархии доменов и зон, а затем добавляются основные и дополнительные зоны из консоли DNS. После этого следует редакция ее свойств. Также во время запуска DNS-серверу необходим список корневых ссылок (root hints). Они представляют собой записи серверов имен и адресов для корневых серверов. Сами же корневые ссылки можно настроить на вкладке *Корневые ссылки* окна свойств сервера DNS в консоли DNS. В этом окне можно увидеть имена серверов и их IP-адреса.

Служба DHCP предназначена для упрощения управления IP-адресами в сети. Для этого используются TCP/IP протокол и служба DHCP (Dynamic Host Configuration Protocol). В ЛВС на базе протокола TCP/IP любой компьютер должен иметь уникальный IP-адрес, который надо настраивать. Без использования DHCP настройку IP-адресов для вновь подключаемых компьютеров, а также перемещенных из одной подсети в другую или удаленных компьютеров приходится выполнять вручную администратору сети, а при применении DHCP эти процессы выполняются автоматически.

Windows 2000 Server включает в себя службу DHCP Server, позволяющую автоматически присваивать IP-адреса компьютерам — клиентам DHCP.

Каждый раз, когда DHCP-клиент загружается, он запрашивает у DHCP-сервера информацию: IP-адрес, маску подсети, адрес шлюза по умолчанию, адрес серверов DNS и WINS. Получив запрос на выполнение IP-адреса, сервер DHCP выбирает информацию об IP-адресе своей базы данных и предоставляет ее клиенту DHCP на определенное время. Если доступных адресов в пуле нет, то клиент DHCP не может инициализировать протокол TCP/ IP. Использование службы DHCP позволяет автоматически настраивать TCP/IP в ЛВС, что позволяет решить множество проблем, которые трудно выявить при статическом выделении IP-адресов администратором сети.

Настройка DHCP-клиента выполняется в четыре перехода. На *первом переходе* («поиск сервера DHCP») компьютер-клиент инициализирует ограниченную версию и посылает широковещательный запрос всем DHCP-серверам. Так как у клиента нет IP-адреса и ему неизвестен IP-адрес DHCP-сервера, он использует 0.0.0.0 как адрес источника и 255.255.255.255 как адрес назначения. Запрос посылается в виде сообщения DHCP DISCOVER, которое содержит аппаратный адрес клиента (MAC-адрес сетевого адаптера) и имя компьютера.

Во *втором переходе* клиенты, получившие запрос об аренде IP-адреса, посылают широковещательное сообщение DHCPOFFER. В нем содержатся аппаратный адрес клиента, предлагаемый IP-адрес, маска подсети, длительность аренды и IP-адрес сервера.

На *третьем переходе* («запрос аренды») клиент берет информацию об IP-адресе из первого полученного предложения и отправляет широковещательное сообщение DHCPPREQUEST с запросом о выделении ему IP-адреса из предложения, которое он получил. Все другие DHCP-серверы отменяют свои предложения и оставляют IP-адреса для следующих запросов аренды.

Во время *четвертого перехода* («подтверждение аренды») DHCP-сервер, отправивший предложение, которое было принято, посылает широковещательное подтверждение клиенту в форме сообщения DHCP/PACK, содержащее арендованный IP-адрес. Этот адрес резервируется сервером DHCP, чтобы он не был предложен другому клиенту.

Послав запрос на поиск сервера DHCP, клиент ожидает предложения в течение 1 с. Если в сети нет работающего сервера, то он должен послать запрос еще три раза: через 9, 13 и 16 с плюс интервал времени (до 1 000 мс), после чего попытки необходимо повторять каждые 5 мин.

В отличие от Windows NT 4.0 клиенты Windows 2000, используя средство APIPA (Automatic Private IP Addressing), могут автомата -

чески настроить IP-адрес и маску подсети, если DHCP-сервер недоступен при загрузке. В этой ситуации служба DHCP клиента Windows 2000 автоматически настраивает свой IP-адрес и маску подсети, используя адрес, выбранный из сети класса *B* 169.254.0.0, зарезервированный за Microsoft, с маской подсети 255.255.0.0. Затем проверяется, не используется ли этот адрес в сети. При обнаружении конфликта клиент выбирает другой адрес. Такая попытка автоконфигурации может повторяться перебором 10 IP-адресов. В случае успеха клиент использует выбранный IP-адрес, проверяя наличие DHCP-сервера каждые 5 мин. Если такой сервер будет обнаружен, то клиент запросит у него IP-адрес обычным образом.

Установка сервера DHCP проводится аналогично установке сервера DNS. Рекомендуется вручную сконфигурировать компьютер DHCP-сервера для использования статического IP-адреса, так как DHCP-сервер не может быть DHCP-клиентом. Он должен иметь статический IP-адрес, маску подсети и шлюз по умолчанию. Для управления DHCP-службой используется консоль DHCP, а также утилита командной строки Ipconfig. Она может выдать отчет о параметрах TCP/IP, сконфигурированных в DHCP.

Для надежной работы сети серверы DHCP должны быть авторизованными. Это предотвращает случайные повреждения, вызываемые работой DHCP-серверов. Для авторизации DHCP-сервера нужно запустить консоль управления DHCP, а затем щелкнуть правой клавишей мыши по узлу DHCP. В открывшемся окне будут перечислены авторизованные серверы DHCP, а кнопка *Авторизовать (Authorize)* позволит провести авторизацию, если это необходимо.

Прежде чем сервер DHCP сможет предоставить клиентам IP-адреса, нужно определить область DHCP — пул действительных адресов, которые могут быть выделены клиентам DHCP.

Для формирования новой области нужно в дереве консоли выбрать DHCP-сервер, затем войти в меню *Действие* (Action) и выбрать команду *Создать область* (New Scope). После этого ее можно сконфигурировать. Для этого нужно использовать окна *Свойства области* и *Параметры области* DHCP.

Служба WINS предназначена для поддержки и предоставления устаревшим приложениям базовых служб доступа к файлам и служб печати в ЛВС. Эта система разрешения имен, используемая в Windows NT Server 4.0 и более ранних ОС, представляет собой распределенную базу данных для регистрации имен компьютеров (имен NetBIOS) и сопоставления этих имен с IP-адресами в маршрутизируемой сетевой среде, использующей NetBIOS поверх TCP/IP.

WINS — это усовершенствованный сервер NetBIOS (NBNS), разработанный фирмой Microsoft в целях снижения широковещательного трафика в ЛВС. Важнейшее преимущество WINS заклю-

чается в пересылке клиентских запросов на разрешение имен непосредственно WINS-серверу. Если сервер WINS может разрешить имя, то он отсылает соответствующий IP-адрес непосредственно клиенту. Таким образом, отпадает потребность в широковещании и снижается объем сетевого трафика. Еще одно преимущество заключается в динамическом обновлении БД WINS. Это устраняет надобность в файле LMHOSTS. Кроме того, WINS предоставляет возможность просмотра ресурсов сети и других доменов.

Имя NetBIOS — это 16-разрядный адрес, идентифицирующий ресурс NetBIOS в сети. Имена NetBIOS могут быть уникальными (монопольными) и групповыми (общими). Уникальные имена обычно применяются для взаимодействия со специфическим процессом системы, групповые — для одновременной рассылки информации нескольким компьютерам.

Разрешение имени NetBIOS — это процесс преобразования имени компьютера NetBIOS в его IP-адрес, после чего IP-адрес можно преобразовать в аппаратный адрес (MAC-адрес сетевого адаптера). Версия пакета протоколов TCP/IP, реализованная Microsoft, использует несколько способов разрешения имени NetBIOS в зависимости от типа узла. Различают широковещательные (5-узлы), одноранговые (Р-узлы), смешанные (Af-узлы) и гибридные (*Я*-узлы). Компьютеры Windows 2000 по умолчанию функционируют как *В-узпы*. После того как для них определен WINS-сервер, они начинают функционировать в качестве //-узлов. Для разрешения удаленных NetBIOS-имен Windows 2000 может использоваться файл локальной базы данных адресов под названием LMHOSTS (хранится в папке *%systemroot %\System32\Drivers\Etc).* Он представляет собой статический ASCII-файл, используемый для преобразования имен NetBIOS в IP-адреса удаленных компьютеров с Windows NT, а также других NetBIOS-компьютеров.

WINS, представляющая собой динамическую БД, содержащую привязки имен компьютеров к IP-адресам, устраняет необходимость изменения широковещания для разрешения имен NetBIOS.

Технология использования WINS реализуется следующим образом. Для каждого клиента WINS задается IP-адрес основного и, при желании, дополнительного сервера WINS. При запуске клиент регистрирует имя NetBIOS и IP-адрес своего компьютера на определенном для него сервере WINS.

Если WINS-сервер доступен и требуемое имя не зарегистрировано другим клиентом, то клиенту возвращается сообщение об успешной регистрации имени на определенный период времени. До истечения этого времени клиент WINS должен послать серверу WINS запрос на продление аренды имени (обновление имени). Сервер WINS в ответ посылает подтверждение, содержащее новый интервал времени, в течение которого требуется продлить регистрацию имени.

Если сервер WINS недоступен, то клиент WINS трижды пытается обнаружить основной сервер, после чего запрос на регистрацию имени передается дополнительному серверу WINS (если он определен). При недоступности обоих серверов клиент может попытаться зарегистрировать свое NetBIOS-имя посредством широковещания.

Если имя больше использоваться не будет (например, при выключении компьютера), то клиент WINS отправляет серверу WINS запрос на высвобождение имени.

При попытке клиента зарегистрировать имя, идентичное имеющемуся в БД WINS, сервер WINS посылает вызов компьютеру, владеющему именем в настоящий момент. Вызов отправляется 3 раза с интервалом 500 мс в форме запроса на определение имени. Если на компьютере, владеющем искомым именем, установлено несколько сетевых адаптеров, то сервер WINS проверяет все IP-адреса данной системы, пока не получит ответ или не переберет все адреса. После успешного ответа системы, владеющей именем в настоящий момент, сервер WINS посылает клиенту WINS, пытающемуся зарегистрировать имя, отрицательный ответ. Если же владелец имени не отвечает, то сервер WINS посылает клиенту WINS, пытающемуся зарегистрировать имя, положительный ответ.

Процесс установления связи в ЛВС TCP/IP между двумя NetBIOS-компьютерами с использованием «имя NetBIOS/IP-адрес» происходит следующим образом. В среде WINS при запуске клиент WINS регистрирует свою привязку «имя NetBIOS/IP-адрес» на соответствующем сервере WINS. После того как клиент WINS выполняет команду для связи с другим компьютером, вместо широковещания по локальной сети запрос на разрешение имени передается непосредственно серверу WINS. Если сервер WINS находит в своей БД привязку «имя NetBIOS/IP-адрес» для конечной системы, то он возвращает WINS-клиенту IP-адрес конечного компьютера. Поскольку привязки «имя NetBIOS/IP-адрес» обновляются в БД WINS динамически, содержащаяся в ней информация всегда соответствует текущему положению дел.

6.2. Мониторинг сети, средства контроля и их оптимизация

6.2.1. Мониторинг сети

Управление сетями — это прежде всего мониторинг, контроль и их оптимизация по функционированию. Это формирует следующие задачи:

• поиск неисправностей в сетях, шлюзах и важных серверах;

• разработка схем уведомления администратора о наличии проблем;

• общий мониторинг сети в целях распределения нагрузки в ней и планирования ее дальнейшего расширения;

• документирование и визуализация работы сети;

• управление сетевыми устройствами с центральной станции.

В отдельной сети Ethernet формальные процедуры управления сетью внедрять, как правило, не следует. Достаточно провести тщательное тестирование сети после ее прокладки и время от времени проверять уровень нагрузки.

По мере роста сети процедуры управления должны становиться более систематизированными. В сети, где несколько подсетей объединяются посредством мостов или маршрутизаторов, решение управленческих задач можно автоматизировать с помощью командных сценариев и простейших программ. Если в организации задействованы протоколы глобальных сетей или сложные ЛВС, то рассмотрите вопрос приобретения выделенных станций управления сетью со специальным программным обеспечением.

В некоторых случаях усложнение системы управления сетью объясняется потребностью обеспечения ее надежности. Во многих организациях бывает так, что возникновение проблемы в сети приводит к остановке всей деятельности. Если подобные задержки недопустимы, то лучше приобрести и установить высококлассную корпоративную систему управления сетью.

К сожалению, даже самая лучшая система не поможет предупредить все проблемы. Нужно иметь хорошо документированную схему сети и высококвалифицированный обслуживающий персонал.

Существует несколько хороших инструментов, позволяющих искать неисправности в сети на уровне TCP/IP. Большинство этих средств выдает низкоуровневую информацию, поэтому, для того чтобы пользоваться ими, нужно понимать принципы работы протоколов TCP/IP и маршрутизации. С другой стороны, источником сетевых проблем могут являться и ошибки в работе таких высокоуровневых протоколов, как DNS, NFS и HTTP.

В данном подразделе рассмотрена общая стратегия поиска неисправностей.

Когда в сети возникает неисправность, первым желанием часто оказывается желание побыстрее все устранить. Нужно сделать паузу и обдумать возможные способы решения проблемы, а не предпринимать необдуманных действий. Самая большая ошибка заключается во внесении в неисправную сеть нецелесообразных изменений.

Для мониторинга собственной сети следует выполнять следующие рекомендации:

• вносить пошаговые изменения в конфигурацию и выпол
нять проверку работоспособности сети после каждого измене-

ния, чтобы убедиться в совпадении полученного эффекта с ожидаемым;

е задокументировать возникшую ситуацию и все вносимые изменения;

• сначала исследовать сетевую конфигурацию клиента, затем проверить физическое соединение клиента с сетевым оборудованием, само сетевое оборудование и аппаратные сетевые средства сервера и его программную конфигурацию;

• регулярно обмениваться мнением с сотрудниками. Большая часть сетевых проблем касается многих людей: пользователей, провайдеров, системных администраторов, инженеров по телекоммуникациям, сетевых администраторов и т.д. Постоянный контакт позволит не мешать друг другу при решении проблемы;

• работать в команде. Многолетний опыт показывает, что люди совершают меньше ошибок, если им оказывают поддержку;

• помнить о многоуровневой структуре сетевых средств. Нужно начать с верхнего или нижнего уровня и последовательно продвигаться по стеку протоколов, проверяя работу программных и аппаратных компонентов.

В архитектуре TCP/IP описываются уровни абстракции, на которых функционируют различные компоненты сети. Например, протокол HTTP тесно связан с протоколом TCP, который, в свою очередь, основан на протоколе IP, а последний взаимодействует с протоколом Ethernet, работоспособность которого зависит от целостности сетевого кабеля. Можно существенно уменьшить время поиска неисправности, если предварительно разобраться, средства какого уровня ведут себя неправильно.

Весь мониторинг сети состоит из ряда проверок сети и анализа пакетов и производится командой ping.

Команда ping очень проста. Она посылает ICMP-пакет ECHO_REQUEST конкретному компьютеру и ждет ответа. Несмотря на свою простоту команда ping стала одним из основных инструментов, использующихся при отладке сетей.

Команду ping можно применять для проверки работоспособности отдельных компьютеров и сегментов сети. В обработке ее запроса участвуют таблицы маршрутизации, физические компоненты сетей и сетевые шлюзы, поэтому для достижения положительного результата сеть должна находиться (в большей или меньшей мере) в рабочем состоянии. Если не работает команда, то можно быть совершенно уверенным в том, что более сложные средства также не станут функционировать. Однако это правило неприменимо в сетях, где брандмауэры блокируют эхо-запросы ICMP. Прежде чем грешить на контролируемый компьютер, который якобы игнорирует команду, надо убедиться, что ее работе не препятствует брандмауэр. В конце концов, следует отключить на ко-

роткое время «вмешивающийся не в свои дела» брандмауэр и проверить работоспособность сети.

Команда ping поддерживается во всех системах. Большинство версий команды работает в бесконечном цикле, если не задан аргумент «число пакетов». Команда ping -s в Solaris выдает расширенную информацию, которая в других операционных системах сообщается по умолчанию. Чтобы прервать выполнение команды, нажмите комбинацию клавиш [Ctrl] + [C].

Информация о компьютере beast включает его IP-адрес, порядковый номер ICMP-пакета и время полного обхода (время, затраченное на прохождение пакета к пункту назначения и обратно). Такая информация, очевидно, свидетельствует о том, что компьютер beast работает и подключен к сети.

В нормально функционирующей сети команда ping позволяет выяснить, включен компьютер или нет. Если же точно известно, что контролируемый компьютер включен и работает корректно, то с помощью данной команды можно получить полезную информацию о состоянии сети. Пакеты, отправляемые командой ping, как и любые другие пакеты, маршрутизируются средствами протокола IP, и успешное получение такого пакета после завершения им кругового маршрута свидетельствует о том, что все компоненты сети между источником и приемником пакета функционируют правильно, хотя бы в первом приближении.

Порядковый номер ICMP-пакета — особенно полезный элемент информации. Несмотря на то что протокол IP не гарантирует доставки пакетов, пакеты будут пропадать только в том случае, если сеть слишком загружена. Потерю пакетов нужно обязательно выявлять, потому что этот факт иногда маскируется протоколами более высокого уровня. Может показаться, что сеть функционирует нормально, но на самом деле она работает гораздо медленнее, чем должна (не только из-за повторной передачи пакетов, но и из-за «накладных расходов», требуемых для выявления и обработки пропавших пакетов соответствующими протоколами.

Если не все пакеты доходят до адресата, то нужно запустить программу traceroute (она описана далее), с тем чтобы выяснить маршрут, по которому пакеты следуют к компьютеру-адресату. Затем, используя команду ping, следует проверить все промежуточные шлюзы, через которые пролегает маршрут, и узнать, на каком этапе теряются пакеты. Чтобы точно диагностировать проблему, следует отправить такое количество пакетов, которое позволит получить статистически достоверные результаты. С достаточной степенью вероятности можно утверждать, что неисправность будет найдена на участке между последним шлюзом, для которого количество потерянных пакетов не больше некоторой заданной величины, и шлюзом, при обращении к которому количество потерянных пакетов превышает эту величину.

Время полного обхода, сообщаемое командой ping, дает представление об общей скорости передачи пакета по сети. Колебания этого значения, как правило, не являются признаком проблем. Иногда пакеты задерживаются на десятки и сотни миллисекунд без какой-либо очевидной причины — просто так работают протокол IP и сама ОС Unix. Но все-таки следует ожидать, что время полного обхода для большинства пакетов будет постоянным, за некоторыми исключениями. Большинство современных маршрутизаторов обеспечивает выдачу ответов на ICMP-запросы с ограничениями по скорости, т. е. маршрутизатор может задержать ответ на пакет команды ping в связи с общим ограничением трафика протокола ICMP.

Команда ping позволяет задавать размер посылаемого эхо-пакета. Если передается пакет, длина которого превышает максимально допустимое для данной сети значение (в частности, 1 500 байт в сети Ethernet), то включается принудительная фрагментация. Это позволяет выявлять ошибки передачи данных в самом носителе и другие низкоуровневые ошибки, например проблемы, связанные с перегрузкой сети ATM.

В Solaris и HP-UX нужная длина пакета указывается в конце команды ping:

```
% ping cuinfo.cornell.edu 1500
```

В Red Hat Linux и FreeBSD длина пакета в байтах задается флагом «-s». Так как слишком большие пакеты могут вызвать пробле-, мы в сети, в FreeBSD эту опцию может указывать только пользователь root:

```
# ping -s 1500 cuinfo.cornell.edu
```

При работе с командой ping следует придерживаться следующих ограничений. Во-первых, сложно отличить неисправность сети от неисправности сервера, пользуясь только этой командой. Сообщение команды ping о потере пакетов свидетельствует лишь о том, что какой-то компонент работает неправильно.

Во-вторых, команда ping не позволяет получить информацию о состоянии исследуемого компьютера. Эхо-запросы обрабатываются в стеке протокола IP и не требуют, чтобы на зондируемом компьютере выполнялся серверный процесс. Наличие ответа является гарантией лишь того, что компьютер включен и ядро системы функционирует. Для проверки работы отдельных служб, таких как HTTP и DNS, следует применять высокоуровневые средства.

Отслеживание IP-пакетов по программе traceroute позволяет установить последовательность шлюзов, через которые проходит IP-пакет на пути к пункту своего назначения. Почти все современные операционные системы содержат ту или иную версию данной программы. Она вызывается текстом:

traceroute *имя_компьютера*

У нее много опций, большинство из которых в повседневной работе не применяется. *Имя компьютера* может быть задано в символической или числовой форме, а выходная информация может быть представлена в виде списка узлов, начиная с первого шлюза и заканчивая пунктом назначения.

Например, на компьютере jaguar команда traceroute drevil описывается следующим текстом:

```
% traceroute drevil
traceroute to drevil (192.225.55.137), 30 hops max, 38 byte
packets
1 xor-gw2  (192.108.21.254) 0.840 ms  0.693 ms  0.671 ms
2 xor-gw4  (192.225.56.10)  4.642 ms  4.582 ms  4.674 ms
3 drevil   (192.225.55.137) 7.959 ms  5.949 ms  5.908 ms
```

Эта информация свидетельствует о том, что для попадания с компьютера jaguar на компьютер drevil пакеты должны пройти два наших внутренних шлюза. Кроме того, показано время полного обхода для каждого шлюза — проведено по три замера. Обычно число переходов от одного узла Интернета к другому составляет от 10 до 12.

Программа traceroute осуществляет запись искусственно заниженного значения в поле TTL (Time To Live — время жизни, или предельное число переходов) исходящего пакета. Когда пакет приходит на очередной шлюз, его значение TTL уменьшается на единицу. Если шлюз обнаруживает, что значение TTL стало равным нулю, то он удаляет пакет и возвращает узлу-отправителю специальное ICMP-сообщение.

Для первых нескольких пакетов программа traceroute задает значение TTL равным 1. Первый шлюз, получивший пакет (в нашем примере это xor-gw2), обнаруживает, что его время жизни истекло. Тогда он отбрасывает пакет и посылает компьютеру jaguar ICMP-сообщение, в поле отправителя которого указывается IP-адрес шлюза. Программа traceroute обращается к службе DNS и по имеющемуся адресу находит имя шлюза.

Для получения данных о следующем шлюзе посылается очередная группа пакетов, поле TTL которых равно 2. Первый шлюз маршрутизирует эти пакеты и уменьшает значение TTL на единицу. Второй шлюз удаляет пакеты и генерирует описанное ранее ICMP-сообщение. Этот процесс продолжается до тех пор, пока пакеты не достигнут требуемого компьютера; значение TTL при этом будет равно числу переходов.

Большинство маршрутизаторов посылает свои ICMP-сообще-ния через тот интерфейс, который является «ближайшим» к узлу-отправителю. Если, наоборот, запустить программу traceroute на машине-получателе, чтобы узнать маршрут к исходному компью-

теру, то, скорее всего, будет выдан другой список IP-адресов, соответствующий тому же набору маршрутизаторов.

Программа traceroute посылает для каждого значения TTL три пакета, что иногда приводит к неожиданным результатам. Если промежуточный шлюз распределяет трафик по нескольким маршрутам, то эти пакеты могут возвращаться разными компьютерами. В таком случае программа traceroute сообщает обо всех полученных ответах.

Рассмотрим пример, в котором посредством программы traceroute определяется маршрут с компьютера в домене colorado.edu к домену xor.com:

Если программа traceroute не работает (или работает очень медленно), это может быть вызвано превышением периода тайм-аута при попытках узнать имя компьютера посредством службы DNS. Если на том компьютере, с которого производится трассировка, не функционирует DNS, то можно воспользоваться командой traceroute -n. Она будет выводить только IP-адреса шлюзов.

Получение информации о состоянии сети осуществляется с помощью команды netstat. Она выдает различную информацию о состоянии сетевого программного обеспечения, включая статистику сетевых интерфейсов, данные о маршрутизации и таблицы соединений, и по ним оценивается функционирование сети. Команда netstat включена во все операционные системы, но в каждой из них поддерживаются разные наборы опций.

Можно выделить четыре наиболее распространенных варианта использования команды netstat:

- проверка состояния сетевых соединений;
- получение статистических данных о различных сетевых протоколах;
- анализ информации о конфигурации интерфейсов;
- изучение таблицы маршрутизации.

При контроле состояния сетевых соединений команда netstat выдает информацию о состоянии активных TCP- и UDP-портов. Неактивные серверы, ожидающие запросов на установление соединений, как правило, не отображаются, но о них сообщается с помощью команды netstat -a. Текст результата такого сообщения можно представить в следующем виде:

```
% netstat -a
Active Internet connections (including servers)'
Proto  Recv-Q  Send-Q Local Address Foreign Address (state)
tcp4   0       0      *.6013       *.*             LISTEN
tcp46  0       0      *.6013       *.*             LISTEN
tcp4   0       0      nimi.ssh     xor.com.4105    ESTABLISHED
tcp4   0       20     nimi.ssh     xor.com.1612    ESTABLISHED
tcp4   0       0      *.13500      *.*             LISTEN
tcp4   0       0      nimi.ssh     135.197.2.114.883 ESTABLISHED
```

```
tcp4   0      0      nimi.1599     xor.com.telnet  ESTABLISHED
tcp4   0      0      *.ssh         *.*             LISTEN
tcp46  0      0      *.ssh         *.*             LISTEN
tcp4   0      0      nimi.ssh      135.197.2.114.776 ESTABLISHED
tcp4   0      0      *.cvsup       *.*             LISTEN
udp4   0      0      *.syslog      *.*
udp    0      0      *.ntalk       *.*
…
```

Этот результат получен на компьютере nimi. Вывод команды свидетельствует о наличии нескольких входящих соединений по протоколу SSH, одного исходящего telnet-соединения и группы портов, ожидающих установления соединения.

Адреса представлены в формате *имя компьютера.сервис,* где сервис — номер порта. Для известных сервисов порты указаны в символическом виде (соответствия между номерами портов и их именами определены в файле /etc/services). При наличии опции -n все адреса отображаются в числовом виде.

В колонках Recv-Q и Send-Q показывается, сколько запросов находится во входящих и исходящих очередях на компьютере. На другом конце соединения размеры очередей могут быть другими. Желательно, чтобы эти значения были близки к нулю. Конечно, если команда netstat запускается через сетевой терминал, для ее соединения размер исходящей очереди, скорее всего, никогда не будет равен нулю.

Состояние соединения имеет значение только для протокола TCP. Протокол UDP не проверяет факт установления соединения. Наиболее распространенными являются состояния: ESTABLISHED (установлено) — для активных соединений; LISTENING (ожидание) — для серверов, ожидающих поступления запросов (при отсутствии опции -a обычно не показываются).

Эта информация полезна главным образом для устранения проблем на более высоком уровне, если, конечно, базовые сетевые средства работают нормально. Команда netstat позволяет проверить правильность настройки серверов и диагностировать определенные виды нарушений связи, особенно при работе с протоколом TCP. Например, если соединение находится в состоянии SYN_SENT, то это означает наличие процесса, который пытается установить контакт с несуществующим или недоступным сервером.

Если команда netstat сообщает о большом количестве соединений, находящихся в состоянии SYN_WAIT, то компьютер, вероятно, не в состоянии обработать запросы на установление соединений. Такая ситуация может быть вызвана ограничениями системного ядра или злонамеренными попытками вызвать перегрузку.

Просмотр информации о конфигурации интерфейса осуществляется с помощью команды netstat -i.

Команда netstat -i сообщает о состоянии сетевых интерфейсов. Приведем результаты, полученные на компьютере evolve, работающем под управлением Solaris:

```
% netstat -i
Name Mtu   Net/Dest   Ipkts  Ierrs  Opkts   Oerrs   Collis
180  8232  Joopback   11650          0       11650   0 0
hme0 1500  evolve     16438  0       18356   0       110
hme1 1500  evolve-bl  94852  7       379410  13      487
```

Указанный компьютер имеет два сетевых интерфейса. В колонках Ipkts и Opkts указывается количество пакетов, принятых и переданных через каждый интерфейс с момента начальной загрузки системы. В колонках Ierrs и Oerrs приводится число ошибок в принимаемых и передаваемых данных; здесь учитывается много разных типов ошибок и отображается наличие какого-то их числа.

Количество ошибок должно составлять менее 1 % от числа пакетов. Если частота появления ошибок высока, сравните эти показатели на нескольких соседних компьютерах. Большое число ошибок на одном компьютере свидетельствует о наличии проблемы в его интерфейсе или соединении, тогда как высокая частота ошибок, возникающих на всех компьютерах, в большинстве случаев обусловлена наличием проблемы в среде передачи.

Количество коллизий (collis) — это показатель степени загруженности сети, а их наличие свидетельствует о проблемах с кабелями. Коллизия является одной из разновидностей ошибки, их число команда netstat подсчитывает отдельно. В колонке Collis указывается число конфликтов, произошедших при отправке пакетов. Это число следует использовать для вычисления доли ошибочных пакетов от общего количества отправленных пакетов (Opkts).

Непрерывный режим работы команды netstat особенно эффективен при выслеживании источника ошибок. Команда netstat -i может сообщить о существовании проблем, но не выявляет причины ошибок: то ли это постоянно возникающая аппаратная проблема, то ли кратковременное, но фатальное событие. Наблюдение за сетью при различных уровнях загруженности позволяет получить гораздо более полное представление о том, что происходит. Здесь можно задать команду ping с большой длиной пакетов и наблюдать за выводом команды netstat.

Проверку таблицы маршрутизации можно осуществить через команду netstat -r, которая отображает таблицу маршрутизации ядра. Приведем пример, полученный на компьютере, который работает под управлением Solaris и имеет два сетевых интерфейса:

```
. netstat -r -n
Routing Table
Destination   Gateway         Flags  Ref   Use    Interface
192.225.44.0  192.225.44.88   U      3     1841   hme0
192.168.3.0   192.168.3.12    U      2     1317   hme1
10.0.0.0      192.168.3.252   UG     0     4      hme1
default       192.225.44.254  UG     0     91668
127.0.0.1     127.0.0.1       UH     0     543    100
…
```

Пункты назначения и шлюзы могут быть представлены либо доменными именами, либо IP-адресами. Опция -n задает вывод IP-адресов.

В колонке Flags отображаются флаги, характеризующие маршрут: «U» (up) — активный; «G» (gateway) — шлюз; «H» (host) — узловой (связан с конкретным адресом, а не сетью). Флаг «D» (не показан) обозначает маршрут, полученный в результате переадресации по протоколу ICMP. Флаги «G» и «H» вместе обозначают маршрут к компьютеру, проходящий через промежуточный шлюз. Остальные поля содержат статистические данные о маршруте: текущее число TCP-соединений по этому маршруту, количество отправленных пакетов и имя используемого интерфейса. Точный вид представленных данных зависит от конкретной операционной системы.

Приведенный вариант команды netstat целесообразен для проверки правильности таблицы маршрутизации. Особенно важно убедиться в наличии и корректности стандартного маршрута. Иногда он обозначается в виде адреса со всеми нулями (0.0.0.0), иногда — словом «default».

Анализ статистических материалов различных сетевых протоколов осуществляется с помощью команды netstat -s, которая выдает содержимое всевозможных счетчиков, используемых в сетевых программах. Информация разбивается на разделы в соответствии с протоколами: IP, ICMP, TCP и UDP. При этом можно получить листинги команды netstat -s.

Если ошибки контрольных сумм отсутствуют, то это свидетельствует о том, что аппаратное соединение работает нормально. Также важен тот факт, что пакеты не отбрасывались из-за недостатка свободной памяти (последняя строка). Для получения более подробной информации об использовании памяти сетевыми службами целесообразно применять опцию —m при запуске команды netstat в Solaris или FreeBSD.

6.2.2. Анализаторы пакетов как средство контроля сети

Анализаторы пакетов относятся к инструментальным средствам. Анализаторы пакетов полезны как для решения множества про-

блем, так и для выявления новых. Время от времени полезно запускать эти программы и проверять, нормально ли обрабатывается сетевой трафик.

Так, программы tcpdump, snoop и nettl следят за трафиком в сети и регистрируют либо выводят на экран пакеты, которые удовлетворяют заданным критериям. Например, можно перехватывать все пакеты, посылаемые на какой-то компьютер или с него, либо TCP-пакеты, относящиеся к конкретному сетевому соединению.

Поскольку анализаторам необходимо уметь перехватывать пакеты, которые компьютер обычно не получает (или на которые не обращает внимания), базовые сетевые аппаратные средства должны разрешать доступ к каждому пакету. Это характерно для широковещательных технологий, в частности Ethernet, а также для некоторых видов сетей Token Ring, в которых отправитель пакета удаляет его из кольца после полного обхода контура.

Анализаторы пакетов должны иметь доступ к низкоуровневому трафику, поэтому их работе могут мешать сетевые мосты, одной из функций которых является препятствие распространению ненужных пакетов. Однако с помощью анализаторов возможно получение полезной информации даже в сетях с мостами. Можно, например, обнаружить проблемы, затрагивающие широковещательные и групповые пакеты. Объем выдаваемой информации зависит от модели моста.

Аппаратный интерфейс должен не только иметь возможность получать доступ ко всем сетевым пакетам, но и содержать механизм, обеспечивающий передачу этих пакетов вверх на программный уровень. Ведь обычно адреса пакетов проверяются на аппаратном уровне, а ядру показываются лишь широковещательные (групповые) пакеты и те пакеты, которые адресованы данному компьютеру. В беспорядочном режиме (promiscuous mode) интерфейс позволяет ядру получать все сетевые пакеты, даже если они предназначены для других компьютеров.

Анализаторы пакетов, как правило, поддерживают многие форматы пакетов, используемые стандартными демонами Unix, и часто могут отображать содержимое пакетов в удобном для пользователя виде. Это облегчает пользователю анализ сеанса между двумя программами. Некоторые анализаторы кроме заголовка пакета выводят и содержимое пакета в текстовом виде, что полезно для исследования протоколов верхних уровней. Так как некоторые из этих протоколов пересылают информацию (в том числе и пароли) по сети в незашифрованном виде, следует заботиться о сохранении конфиденциальности пользовательских данных.

Каждая из рассматриваемых нами операционных систем имеет анализатор пакетов. В связи с тем, что анализатору необходим доступ к пакетам на самом низком уровне, он должен запускаться от имени пользователя root. Подобное ограничение снижает шан-

сы обычных пользователей получить доступ ко всему сетевому трафику, но на самом деле этот барьер можно преодолеть. Во многих организациях анализаторы пакетов удалены с большинства компьютеров для уменьшения риска злоупотребления этими программами. Если данная мера невозможна, то следует проверять интерфейсы системы, чтобы они не работали в беспорядочном режиме без ведома или согласия администратора.

Анализатор пакетов в Solaris — это программа snoop. Используя ее с помощью аргументов командной строки, можно задать перехват пакетов определенного типа, конкретного компьютера, протокола, порта и т.д.

Если программа запущена без аргументов, то она анализирует пакеты, проходящие через первый из найденных ею интерфейсов. Обычно это тот интерфейс, который приведен первым в выводе команды netstat -i (исключая интерфейс обратной связи). Для указания конкретного интерфейса применяется опция -d *имя интер-фейса.*

Имя интерфейса следует вводить в том виде, в котором оно сообщается командой netstat -i (например, для первого интерфейса Ethernet часто используется имя hmeO). Опция -V позволяет получить развернутую информацию, а при наличии опции -v выводится несколько дополнительных поясняющих строк для каждого пакета.

Синтаксис командной строки программы snoop достаточно сложен, но все ее опции хорошо описаны на соответствующей man-странице. В командную строку можно помещать выражения, содержащие такие ключевые слова, как host, port, tcp, udp nip, а также обозначения операций and, or или not.

Если с помощью программы telnet зарегистрироваться на удаленном узле, а затем запустить анализатор snoop, то придется отфильтровать пакеты самого сеанса от общего трафика. Например, чтобы проигнорировать трафик, направленный к компьютеру evolve или идущий от него, следует задать такую команду:

```
# snoop not host evolve
```

Если нужно исследовать неработающий DNS-сервер с именем mrhat, надо воспользоваться командой

```
# snoop host mrhat | grep DNS
```

В этом случае утилита grep позволит исключить вывод ненужной информации.

Анализатор пакетов в HP- UX — это программа nettl (означает «крапива, раздражать, сердить») — очень мощная программа, способная работать в быстрых сетях, но конфигурировать ее настолько сложно, что для быстрой отладки сети она непригодна. Тем, кто планирует осуществлять анализ пакетов с компьютера,

работающего под управлением HP-UX, рекомендуется инсталлировать программу tcpdump.

Программа nettl входит в пакет Network Tracing and Logging (трассировка пакетов и регистрация событий в сети) системы HP-UX. По умолчанию эта программа запускается на этапе начальной загрузки системы. Если ее использование не планируется, то ее надо отключить. Для этого в файле /etc/rc.config.d/nettl необходимо установить переменную NETTL равной нулю.

Программа nettl считывает параметры своей конфигурации из файла /etc/nettlgen.conf.

Самый лучший анализатор — программа tcpdump — входит в комплект поставки систем Red Hat Linux и FreeBSD и уже давно считается промышленным стандартом. Его исходные коды имеются в HP-UX, Solaris и большинстве других операционных систем. Работа с этим анализатором напоминает работу с программой snoop.

По умолчанию программа tcpdump использует первый найденный ею сетевой интерфейс. Если она выбрала не тот интерфейс, то посредством опции -i следует задать нужный. В случае неисправности службы DNS или при необходимости видеть адреса компьютеров, воспользуйтесь опцией -n. Эта опция имеет большое значение, так как медленная работа DNS может вызвать отбрасывание пакетов до того, как они будут проанализированы программой tcpdump. Опция -v позволяет получить более детальное описание каждого пакета, а самые подробные результаты выдаются при задании опции -vv. Если указана опция -w, то программа сохраняет перехваченные пакеты в файле. Для чтения пакетов из файла предназначена опция -r.

Далее представлены результаты работы программы tcpdump, запущенной на узле jaguar.xor.com. Спецификация host jaguar задает получение информации только о тех пакетах (получаемых и отправляемых), которые имеют непосредственное отношение к компьютеру jaguar.

```
# tcpdump host jaguar
13:40:23 jaguar.xor.com.1697 > xor.com.domain: A?
cs.colorado.edu.
13:40:23 xor.com.domain > jaguar.xor.com.1697:
Amroe.cs.colorado.edu
13:40:23 jaguar.xor.com.1698 > xor.com.domain: PTR?
5.96.138.128.in-addr.arpa.
13:40:23 xor.com.domain > jaguar.xor.com.1698: PTR
mroe.cs.colorado.edu.
```

В первой строке вывода содержится информация о том, что с компьютера jaguar в домен xor.com отправлен пакет с запросом к службе DNS, касающимся имени cs.colorado.edu. Во второй стро-

ке приводятся сведения об ответном пакете, где говорится о том, что указанное имя является псевдонимом узла mroe.cs.colorado.edu. Далее выдаются данные о пакете с запросом доменного имени, соответствующего IP-адресу компьютера mroe. В последней строке сообщается результат запроса.

6.3. Маршрутизация и удаленный доступ

Предоставление клиентам удаленного доступа к ресурсам сети, а также создание виртуальных частных сетей обеспечивается службой маршрутизации и удаленного доступа RRAS. Поскольку RRAS полностью поддерживает буквы дисков и имена UNC (Universal Naming Convention — универсальные правила именования), большинство приложений не требует модификации для работы с удаленным доступом. Серверы Windows 2000 и Unix обслуживают два типа удаленных подключений: подключение по коммутируемой (телефонной) линии и виртуальная частная сеть (VPN — Virtual Private Network).

Клиент удаленного доступа может устанавливать временное телефонное подключение к физическому порту на сервере удаленного доступа, пользуясь услугами поставщика телекоммуникаций, по аналоговой линии, линиям ISDN (цифровая сеть комплексных услуг) или X.25. В данном случае это прямое физическое соединение клиента и сервера. Передаваемые по такому каналу данные можно шифровать, хотя это и не обязательно.

В отличие от прямого подключения по телефону работа через VPN — это логическое соединение, типичным случаем которого является подключение клиента по телефону через Интернет к серверу корпоративной сети. При этом клиент использует туннельные специальные протоколы, основанные на TCP/IP. Для гарантии безопасности рекомендуется шифровать данные, передаваемые по VPN-подключению.

Служба RRAS включает в себя функции преобразования сетевых адресов NAT, мультипротокольной маршрутизации, протокол туннелирования канального уровня (L2TP), службу проверки подлинности в Интернете (IAS — Internet Authentication Service) и политики удаленного доступа (RAP — Remote Access Policies).

В Windows 2000 реализована функция, называемая обнаружением маршрутизатора (Router Discovery). Она обеспечивает настройку и обнаружение шлюзов по умолчанию. При использовании DHCP или при ручной настройке параметров стандартного шлюза невозможно приспособиться к изменениям сети. Обнаружение маршрутизатора позволяет клиентам динамически находить маршрутизаторы и при сбое в сети переключаться на резервные маршрутизаторы.

NAT позволяет подключаться к Интернету с любого компьютера ЛВС через один IP-адрес. NAT — это маршрутизатор, преобразующий IP-адреса ЛВС в действительные адреса Интернета. Server Windows 2000 включает в себя полную реализацию NAT, называемую Connection Sharing (общее подключение), и неконфигури-руемую версию Shared Access (общий доступ).

Server Windows 2000 реализует ограниченную форму многоадресной маршрутизации, используя многоадресный проксиузел для расширения многоадресной поддержки до полноценного многоадресного маршрутизатора.

Протокол L2TP соответствует канальному уровню модели OSI и применяется для VPN.

Служба IAS представляет собой сервер Remote Authentication Dial-In User Service (RADIUS), позволяющий проводить аутентификацию, авторизацию и учет удаленных пользователей, которые подключаются к серверу доступа к сети (Network Access Server — NAS). В свою очередь, NAS (например, сервер RRAS в Windows 2000) может быть клиентом или сервером RADIUS.

Политики удаленного доступа настраиваются из Internet Authentication Service (Служба проверки подлинности в Интернете) и Routing and Remote Access.

Для инсталляции службы RRAS необходимо выполнить следующие действия:

1) запустить оснастку «Routing and Remote Access»;

2) правой кнопкой мыши щелкнуть по имени компьютера, выбрать команду *Настроить* и включить маршрутизацию и удаленный доступ (Configure And Enable Routing And Remote Access);

3) в окне мастера установки сервера RRAS щелкнуть по кнопке *Далее (Next);*

4) в окне *Общие параметры* (Common Configurations) установить переключатель *Сервер удаленного доступа* (Remote Access Server), а затем щелкнуть по кнопке *Далее (Next);*

5) убедиться, что в окне *Протоколы удаленных клиентов* (Remote Client Protocols) в списке протоколов перечислен TCP/IP. Удостовериться, что выбран параметр «Yes, All The Required Protocols Are On This List» («Да, все требуемые протоколы присутствуют в списке»), и щелкнуть по кнопке *Далее (Next);*

6) в окне *Назначение IP-адресов* (IP Address Assignment) щелкнуть по переключателю *Из заданного диапазона адресов* (From A Of Specified Range Of Address) и затем — по кнопке *Далее;*

7) в окне *Назначение диапазонов IP-адресов (Address Range Assignment)* щелкнуть по кнопке *New (Создать).* В полях «Начальный IP-адрес» (Address Range Assignment), «Конечный IP-адрес» (End Of IP Address) и «Количество адресов» (Number Of Addresses) вве сти нужные значения. Щелкнуть по кнопке *ОК,* чтобы закрыть окно *Новый диапазон адресов,* а затем — по кнопке *Далее (Next);*

8) убедиться, что в окне *Управление несколькими серверами удаленного доступа* (Managing Remote Access Servers) выбран параметр *Нет, не настраивать данный сервер для работы с RADIUS-сервером* (No, I Don't Want To Set This Server Up To RADIUS Now), затем щелкнуть по кнопке *Далее {Next);*

9) щелкнуть по кнопке *Finish {Готово);*

10) щелкнуть по кнопке *ОК* в ответ на любое сообщение.

Контрольные вопросы

1. Классифицируйте и опишите адреса Интернета классов *А, В* и *С.*

2. Перечислите стандартные утилиты и службы TCP/IP на прикладном уровне.

3. Что такое транспортные протоколы и как организована связь между компьютерами?

4. Какие типы IP-адресов вы знаете?

5. Приведите краткое описание сетевых служб.

6. Опишите, как организован мониторинг сети.

7. Как производится проверка доступности компьютера, отслеживание IP-пакетов и получение информации о состоянии сети?

8. Как осуществляется контроль сетевых соединений?

9. Опишите основные анализаторы пакетов. Каково их назначение?

10. С помощью каких служб организованы маршрутизация и удаленный доступ в сети ИС?

УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ, СЕТЕВЫМИ СЛУЖБАМИ, ДИСКАМИ, СЛУЖБОЙ ПЕЧАТИ

7.1. Технологии работы системного администратора при администрировании подсистем ИС. Обязанности системного администратора в сети Windows

Задачи, функции и основные процедуры административного управления были рассмотрены в гл. 1. Для практического применения технологий администрирования целесообразно рассмотреть основные процессные и функциональные обязанности администратора при управлении информационной сетью на примере операционной системы Windows разных модификаций.

При планировании администрирования системы целесообразно выделить следующие основные процессные обязанности при управлении:

- пользователями и их группами;
- сетевыми службами;
- использованием дискового пространства;
- подсистемой печати;
- присвоением имен и управлением доступом в систему;
- определением системной политики;
- установкой и конфигурацией аппаратных устройств;
- установкой программного обеспечения;
- установкой сети;
- архивированием (резервным копированием) информации;
- созданием и управлением счетами пользователей;
- контролем защиты;
- определением и управлением подсистемами;
- системными ресурсами;
- мониторингом производительности;
- планированием нагрузки;
- лицензиями;
- документированием системной конфигурации.

В некоторых некрупных системах (например, до 15...20 рабочих мест, расположенных локально в пределах одного небольшого здания) на системного администратора также возлагаются обя-

занности по поддержке пользователей. Эти обязанности занимают большую часть рабочего времени, поэтому на более крупных информационных системах рекомендуется освободить системного администратора от работ по оказанию помощи пользователям.

В дополнительные обязанности системного администратора входят следующие:

- подготовка квалифицированных пользователей для выполнения ими обязанностей по ведению архивов;
- ответы на вопросы и требования пользователей сети, относящиеся к возможностям их доступа к сетевым ресурсам, а также о производительности ежедневной работы;
- участие в работах по развитию и модернизации корпоративной сети;
- ведение журнала системной информации.

Для системного администратора ОС Windows основные процессные обязанности управления могут быть описаны набором известных процедур. При этом совсем не обязательно, чтобы эти функции выполнял один человек. Во многих организациях работа распределяется среди нескольких администраторов. В любом случае необходим хотя бы один человек, который понимал бы все поставленные задачи и обеспечивал их выполнение другими людьми.

Процедура *подключения и удаления пользователей* заключается в создании аккаунтов для новых пользователей и удалении аккаун-тов тех пользователей, которые уже не работают. Это является обязанностью системного администратора. Процесс включения и удаления пользователей можно автоматизировать, но некоторые решения, от которых зависит включение нового пользователя, должен принимать системный администратор.

Если необходимо прекратить доступ пользователя к системе, то его аккаунт должен быть отключен. Все файлы, относящиеся к этому аккаунту, необходимо удалить, чтобы они не занимали места на диске.

Процедура *подключения и удаления аппаратных средств* осуществляется в случаях приобретения новых аппаратных средств или подключения уже имеющихся аппаратных средств к другой машине. При этом систему нужно сконфигурировать таким образом, чтобы она распознала и использовала эти средства. Изменение конфигурации может быть как простой задачей (например, подключение принтера), так и более сложной (например, подключение дисковода).

Резервное копирование является одной из наиболее важных задач системных администраторов, которую они, к сожалению, чаще всего игнорируют или выполняют «спустя рукава». Процедура резервного копирования очень утомительна и занимает много времени, но выполнять ее необходимо. Ее можно автоматизировать или поручить подчиненным, но все равно системный администт-

ратор обязан убедиться в том, что резервное копирование выполнено правильно и по графику.

Инсталляция и тестирование новых программных средств осуществляется после приобретения нового программного обеспечения. Если программы работают нормально, то пользователям необходимо сообщить об их наличии и местонахождении. Локальное программное обеспечение следует инсталлировать туда, где его можно будет легко отличить от программных средств, поставляемых в составе операционной системы (например, Windows). Это значительно упрощает задачу расширения операционной системы, поскольку исчезает опасность уничтожения локального программного обеспечения в ходе подобного расширения.

Мониторинг системы использует множество обязательных для исполнения ежедневных операций (например, проверка правильности функционирования электронной почты и телеконференций, просмотр регистрационных файлов на предмет наличия ранних признаков неисправностей, контроль за подключением локальных сетей, контроль за наличием системных ресурсов (в частности, контроль за наличием свободного пространства на диске) и т.д.).

Процедура *поиска неисправностей* необходима, так как различные операционные системы и аппаратные средства, на которых они работают, время от времени выходят из строя. Задача администратора — диагностировать сбои в системе и в случае необходимости вызвать специалистов. Как правило, найти неисправность бывает намного сложнее, чем устранить ее.

Ведение локальной документации способствует выявлению отличий инсталлируемых программных средств от средств базовой конфигурации. Настраивая конфигурацию под конкретные требования, обнаруживается, что она значительно отличается от конфигурации, описанной в документации (базовой конфигурации). Поэтому системный администратор должен документировать все инсталлируемые программные средства, не входящие в стандартный комплект поставки, документировать разводку кабелей, вести записи по обслуживанию всех аппаратных средств, регистрировать состояние резервных копий, документировать локальные процедуры и правила работы с системой и др.

Контроль защиты процессов переработки информации в И С — также очень важная процедура. Системный администратор должен реализовывать стратегию защиты и периодически проверять, не нарушена ли защита системы. В системах с низким уровнем безопасности эта процедура может быть сведена к нескольким текущим проверкам на предмет несанкционированного доступа. В системах с высоким уровнем безопасности обычно применяется сложная система ловушек и программ контроля.

Оказание помощи пользователям в решении различных проблем редко включается в должностную инструкцию системного администратора, так как выполнение подобного рода обязанностей «съедает» большую часть рабочего времени. К системным администраторам обращаются с самыми разными проблемами, начиная с «Вчера моя программа работала, а сегодня нет! Что вы поменяли?» и заканчивая «Я пролила кофе на клавиатуру! Теперь нужно полить ее водой, чтобы смыть кофе?».

Функциональные обязанности системного администратора в ОС Windows можно подразделить на восемь групп.

1. Доставка, установка и настройка лицензионного программного обеспечения.
   1.1. Операционных систем.
   1.2. Офисных пакетов программ.
   1.3. Дополнительного ПО.
2. Установка, настройка и администрирование лицензионных операционных систем.
   2.1. Windows 95/98/ME.
   2.2. Windows NT4 Workstation/ Windows 2000 Professional.
   2.3. Windows NT4/2000 Server.
   2.4. Novell Netware.
3. Проверка работоспособности серверов и их администрирование (аудит событий).
4. Помощь в приобретении, подключении и настройке дополнительного оборудования (принтеры, модемы и другие внешние устройства).
5. Антивирусная защита компьютеров, сетей и серверов клиента.
   5.1. Проверка компьютеров клиента антивирусными программами.
   5.2. Продажа, установка и настройка постоянной комплексной антивирусной защиты.
6. Тестирование и техническое обслуживание компьютеров.
   6.1. Проверка и регламентные работы по обслуживанию ПО заказчика.
   6.2. Техническое обслуживание, экстренные выезды и телефонные консультации по проблемам компьютерного оборудования.
7. Тестирование и техническое обслуживание сети.
   7.1. Проверка активного оборудования.
   7.2. Проверка прохождения сигнала в кабельной системе.
   7.3. Проверка соединений кабельной системы и активного оборудования.
   7.4. Экстренные выезды и телефонные консультации по проблемам, связанным с сетевым оборудованием.
8. Консультации по обновлению программного обеспечения и модернизации оборудования (upgrade).

В организациях и фирмах администрирование как служба документально оформляется должностными инструкциями и другими организационными формулярами. Проект типовой должностной инструкции администратора сети представлен в Приложении.

7.2. Технологии управления сетевыми службами администрирования

7.2.1. Основные положения по управлению сетевыми службами

За последние 10 лет сети быстро усложнялись и разрастались, что вызвало потребность в разработке средств сетевого управления. Поставщики операционных систем и организации по стандартизации подходили к решению этой задачи разными путями. Самым значительным результатом стала разработка ряда стандартных протоколов управления сетевыми устройствами и множества высокоуровневых программных средств, которые их используют.

Протоколы управления сетями определяют стандартный подход к выявлению сетевых соединений устройства, его конфигурации и общего состояния. Кроме того, протоколы позволяют модифицировать часть этой информации, чтобы стандартизировать управление различными видами аппаратуры на сетевом уровне и осуществлять это управление с центральной станции.

Наиболее распространенным протоколом управления, используемым в сетях TCP/IP, является SNMP (Simple Network Management Protocol — простой протокол управления сетью). Основные положения по нему были рассмотрены в подразд. 3.2. Несмотря на свое название этот протокол достаточно сложен. Он определяет иерархическое пространство имен для объектов управления и способ чтения и записи данных, относящихся к этим объектам, на каждом узле иерархии. Он также задает способ, которым управляемые сущности («агенты») посылают сообщения о происходящих событиях («прерывания») станциям управления. Ядро протокола является простым; самая сложная часть SNMP находится над протокольным уровнем и заключается в соглашениях по построению пространства имен и соглашениях по форматированию элементов данных на узле иерархии. Протокол SNMP широко поддерживается разработчиками ПО.

Имеется и ряд других стандартов управления сетями. Многие из них созданы организацией DMTF (Distributed Management Task Force — рабочая группа по разработке распределенных систем управления), которая реализовала такие концепции, как WBEM (Web-Based Enterprise Management — система управления предприятием, основанная на использовании Web-технологий), DMI

(Desktop Management Interface — интерфейс управления компьютером) и CIM (Conceptual Interface Model — концептуальная модель интерфейса). Некоторые из этих концепций, в частности DMI, приняты рядом известных фирм-производителей и могут служить полезным дополнением (а иногда и заменой) протоколу SNMP. Однако в настоящее время основным средством управления сетями является SNMP.

Поскольку SNMP — абстрактный протокол, для его использования нужна программа-сервер («агент») и программа-клиент («менеджер»). (Как ни странно, серверная сторона SNMP является управляемым элементом, а клиентская — управляющим). Клиентом может быть как простая утилита, работающая в режиме командной строки, так и выделенная станция управления, на мониторе которой в графическом виде отображается сеть вместе со всеми неполадками.

Выделенные станции управления сетями — главная причина существования протоколов управления. Большинство программных продуктов позволяет строить не только логическую, но и топографическую модель сети. Обе эти модели выводятся на экран, при этом постоянно отображается текущее состояние каждого компонента.

Как график может показать скрытый смысл, заложенный в заполненной цифрами странице, так и станция управления сетью способна обобщить и представить состояние крупной сети в форме, удобной для понимания. Другим способом такую информационную сводку получить практически невозможно.

Основное преимущество SNMP заключается в том, что абсолютно все типы сетевых аппаратных средств выводятся на один уровень. Unix-системы в основном похожи друг на друга, чего нельзя сказать о маршрутизаторах, шлюзах и остальных низкоуровневых компонентах. При использовании протокола SNMP все они начинают «общаться» на одном языке и могут зондироваться, сбрасываться в начальное состояние и конфигурироваться с центральной станции. Очень удобно, когда есть один согласованный интерфейс, применимый ко всем сетевым устройствам.

7.2.2. Управление сетью на основе протокола SNMP

Когда в начале 1990-х гг. протокол SNMP впервые появился на рынке, сотни компаний выпустили собственные пакеты управления по протоколу SNMP. Кроме того, многие поставщики аппаратных и программных средств стали включать в свои продукты SNMP-агенты.

В SNMP данные организованы иерархически, причем структура иерархии жестко определена. Это позволяет пространству данных оставаться универсальным и расширяемым, по крайней мере, теоретически. Большие его области оставлены для перспективного использования; дополнения поставщиков операционных систем локализуются в определенных диапазонах во избежание конфликтов. Для формирования пространства имен применяются так называемые базы управляющей информации MIB (Management Information Base). Это структурированные текстовые файлы, которые содержат описания данных, доступных по протоколу SNMP. Ссылки на конкретные переменные, описываемые в базе, называются идентификаторами объектов (Object Identifier — OID).

В основном SNMP-переменные содержат данные целого и строкового типов, а также пустые значения. Данные базовых типов разрешается объединять в последовательности, а каждую последовательность можно многократно повторять, создавая таким образом таблицу. В большинстве реализаций SNMP поддерживаются и другие типы данных.

Иерархия SNMP напоминает иерархию имен файловой системы. В качестве символа-разделителя здесь используется точка, а каждому узлу иерархии присваивается не имя, а номер. Для облегчения ссылок узлам присваиваются также текстовые имена, но схема именования выходит за рамки самой иерархии и определяется на высоком уровне (это похоже на связь между именами компьютеров и их IP-адресами). Например, идентификатор OID, соответствующий показателю общего времени работы системы, выглядит так: 1.3.6.1.2.1.1.3. В более понятной форме его можно записать следующим образом:

```
iso.org.dod.internet.mgmt.mib-2.system.sysUpTime
```

Верхние уровни иерархии SNMP носят искусственный характер и обычно не содержат никаких полезных данных. Интересная информация появляется только на уровне iso. org. dod. internet. mgmt (OID равен 1.3.6.1.2).

Основная административная база данных SNMP для протоколов TCP/IP (MIB-I) определяет доступ к наиболее важным управляющим данным: информации о системе, ее интерфейсах, преобразовании адресов и протоколах (IP, ICMP, TCP, UDP и др.). В документе RFC1213 описана новая, более полная версия этой базы, получившая название MIB-II. Большинство поставщиков, выпускающих SNMP-серверы, поддерживает MIB-II. В табл. 7.1 приведена выборка узлов из базы имен MIB-II и их содержание.

Помимо основной административной базы существуют базы для различных типов аппаратных интерфейсов и протоколов. Име-

Таблица 7.1

Некоторые узлы из базы имен MIB-II и их содержание

OID	Тип	Содержание
system. sysDescr	Строка	Информация о системе: производитель, модель, тип ОСи т. д.
system.sysLocation	Строка	Физическое местонахождение компьютера
system.sysContact	Строка	Информация о владельце компьютера
system. sysName	Строка	Имя системы (обычно это полное DNS-имя)
interfaces.ifNumber	Целое	Количество имеющихся сетевых интерфейсов
intrefaces.ifTable	Таблица	Таблица с информацией о каждом интерфейсе
ip.ipForwarding	Целое	1, если система является шлюзом, иначе 2
ip.ipAddrTable	Таблица	Таблица данных IP-адресации (маски и т.д.)
ip.ipRouteTable	Таблица	Системная таблица маршрутизации
icmp.icmplnRedirects	Целое	Число полученных переадресующих ICMP-пакетов
icmp.icmplnEchos	Целое	Число полученных пакетов команды ping
tcp.tcpConnTable	Таблица	Таблица текущих TCP-соединений
udp.udpTable	Таблица	Таблица с информацией о UDP-сокетах, через которые серверы ожидают прием запросов

ются также базы данных по отдельным поставщикам и по конкретным изделиям.

MIB — это лишь соглашение об именовании управляющих данных. Для того чтобы эта схема заработала, ее необходимо подкрепить программой-агентом, которая будет обеспечивать соответствие содержимого SNMP-переменных и текущего состояния устройства. Код для основной базы MIB (в настоящее время MIB-II) поставляется с большинством SNMP-агентами Unix. Некоторые агенты разрешают подключать дополнительные базы данных.

В пространстве имен SNMP определены всего четыре базовые операции: get *{прочитать),* get-next *{прочитать следующий),* set *{записать)* и trap *{прерывание).*

Операции get и set — базовые операции чтения и записи данных на узле иерархии, который определяется конкретным значением OID. Операция get-next используется для последовательного прохода по базам MIB, а также для чтения таблиц.

Прерывание (операция trap) — это неожиданное, асинхронное уведомление клиента о том, что на сервере произошло интересное событие. Определен ряд стандартных прерываний включая уведомления вида «я только что включился», сообщения об отказах и восстановлении сетевых каналов, а также сообщения, связанные с различными проблемами маршрутизации и аутентификации. Широко распространены и нестандартные прерывания, например такие, которые просто используются для отслеживания значений требуемых SNMP-переменных. Если эти значения выходят за границы установленного диапазона, то выдается соответствующее сообщение. Способ определения получателей таких сообщений зависит от реализации агента.

Поскольку сообщения SNMP потенциально могут изменять информацию о конфигурации компьютеров, необходим какой-то механизм защиты информации. Простейшая защита основана на концепции «имени сообщества» (community name — синоним слова «пароль»). Доступу только для чтения соответствует один пароль («имя сообщества»), а доступу для записи — другой.

Версия 3 стандарта SNMP включает в себя методы управления доступом с высокой степенью безопасности. Использование этих методов ограничивается возможностями сетевых аппаратных средств, но есть основания ожидать изменений в лучшую сторону.

Для удаленного мониторинга в SNMP используется база MIB — RMON (remote monitoring — удаленный мониторинг). Она накапливает данные об общих характеристиках сети (т. е. таких, которые не относятся к какому-то конкретному устройству). Сетевые анализаторы, или «зонды», могут собирать информацию о загруженности и производительности сети. Полезные данные группируются, предварительно обрабатываются, и их важная часть доставляется на центральную станцию управления для анализа и графического воспроизведения. Многие зонды имеют буферы для перехваченных пакетов и могут работать подобно программе tcpdump.

База RMON описана в документе RFC1757, который был принят в качестве чернового стандарта в 1995 г. База разделяется на девять групп RMON. Каждая группа хранит собственный набор статистических данных. Если сеть достаточно велика и имеет много глобальных соединений, то необходимо рассмотреть возможность приобретения зондов для снижения SNMP-трафика через глобальные соединения. При наличии итоговых статистических данных отпадет необходимость в удаленном сборе первичных дан-

ных. Многие мосты и маршрутизаторы поддерживают базы RMON и хранят в них собственные статистические данные.

Многие производители операционных систем и сетевого оборудования поставляют свою продукцию с готовыми к использованию SNMP-агентами. Пароль доступа только для чтения чаще всего равен «public», а пароль доступа для записи иногда задается как «private» или «secret». Мы сталкивались со многими производителями, использующими такое решение. Это удобно для системных администраторов, но также удобно и для хакеров. Тем, кто планирует использовать SNMP, советуем сконфигурировать агентов так, чтобы пароли и для чтения, и для записи было трудно угадать.

Операционные системы Solaris, HP-UX, UCD-агент поставляются с неплохими SNMP-агентами. UCD-агент системы FreeBSD находится в каталоге /usr/ports/net/ucd-snmp. В стандартном дистрибутиве Red Hat поддержка протокола SNMP отсутствует.

SNMP-агент в Solaris располагает солидными средствами управления сетями. В дополнение к мощному SNMP-агенту эта система также обеспечивает поддержку интерфейса DMI.

Главным SNMP-агентом является демон /usr/lib/snmp/snmpdx, конфигурация которого хранится в файле /etc/snmp/conf/ snmpd.conf. В этот файл можно записывать значения многих переменных MIB, а также основные параметры конфигурации агента. Например, можно задать строку описания системы (sysdescr), узлы, которым требуется посылать уведомляющие сообщения (параметр trap), и пароли для чтения и записи (read-community, write-community). После изменения содержимого конфигурационного файла его уничтожают и запускают заново демон snmpdx, чтобы внесенные изменения вступили в силу.

Демон snmpdx извлекает информацию о безопасности из файла /etc/snmp/conf/snmpdx.acl. В этом файле перечислены IP-адреса компьютеров, которым разрешен доступ к локальному SNMP-агенту. Каждый набор компьютеров может иметь собственный пароль («имя сообщества») для чтения и записи данных. Такие возможности существенно повышают безопасность протокола SNMP.

В своем дистрибутивном варианте система Solaris на этапе начальной загрузки запускает два процесса, связанных с интерфейсом DMI: первый — это демон /usr/lib/dmi/dmispd, который непосредственно отвечает на DMI-запросы; второй — это демон /usr/ lib/dmi/snmpXdmid, который преобразует SNMP-запросы в формат DMI и передает их демону dmispd. Ответ последнего преобразуется демоном snmpXdmid и возвращается обратно SNMP-серверу snmpdx. Параметры преобразования SNMP/DMI определяются содержимым файлов, находящихся в каталоге /var/dmi/map.

Если в системе отсутствуют средства DMI-управления или их использование не планируется, то следует запретить запуск всех

DMI-процессов при начальной загрузке системы. Для этого необходимо переименовать файл /etc/rc3.d/S77dmi в /etc/rc3.d/s77dmi. Если требуется отключить демон snmpXdmid, то переименуйте его конфигурационный файл snmpXdmid.conf в snmpXdmid.conf.orig.

Компания Hewlett-Packard для управления сетями масштаба предприятия разработала пакет HP Open View. Так как эта компания — признанный лидер в разработке средств управления сетями, факт включения SNMP-агента в дистрибутив HP-UX не стал неожиданностью. Только вместо единого агента в HP-UX используется набор специализированных субагентов. Такая схема позволяет разработчикам добавлять необходимые субагенты для новых аппаратных или программных компонентов без изменения всей системы.

Главным агентом является демон /usr/sbin/snmpdm, но он никогда не запускается непосредственно. Для этой цели служит сценарий /usr/sbin/snmpdm, который кроме агента snmpdm запускает нужные субагенты для сбора данных.

Агент читает свои установки из файла /etc/SnmpAgent.d/ snmpd.conf. Кроме того, конфигурационные параметры могут быть заданы в строке запуска сценария snmpd.

В файле snmpd.conf можно использовать только пять ключевых слов.

Ключевые слова get-community-name и set-community-name задают пароли для чтения и записи данных. Выражений, определяющих пароли, может быть несколько, однако управление доступом не должно различаться для разных групп компьютеров. Любой пароль, указанный в любой инструкции set-community-name, действителен для любой поддерживаемой операции чтения или записи.

Ключевым словом trap-dest задается имя или IP-адрес SNMP-клиента, который будет принимать уведомления о прерываниях. Клиентов может быть несколько, и уведомления посылаются во все пункты назначения.

Ключевые слова «location» и «contact» задают значения объектов sysLocation и sysContact базы MIB-II.

С помощью флага «-т» можно контролировать объем журнальной информации, выдаваемой сценарием snmpd, например по аргументу *маска:* snmpd-m *маска.*

Аргумент *маска* должен представлять собой побитовое объединение флагов, выбираемых из табл. 7.2.

К сожалению, в HP-UX SNMP-агент не использует систему Syslog. Стандартный файл регистрации — /var/adm/snmpd.log; другой файл можно задать с помощью опции -1.

В настоящее время дистрибутив UCD (University of California at Davis) широко распространен в качестве бесплатной реализации протокола SNMP для Unix. Мы рекомендуем использовать этот

Таблица 7.2

Флаги для сценария snmpd в HP-UX

Флаг	Функция
0	Отключить журнальную регистрацию
1	Регистрировать отказы в аутентификации
2	Регистрировать ошибки
4	Регистрировать запросы на конфигурирование
8	Регистрировать SNMP-транзакции
16	Регистрировать добавляемые объекты
32	Распечатывать все пакеты в шестнадцатеричном виде
64	Регистрировать сообщения о трассировке

пакет в тех системах, которые не имеют собственных SNMP-аген-тов. В состав пакета входит SNMP-агент, несколько утилит командной строки и даже библиотека для разработки SNMP-приложе-ний. Далее рассмотрена работа самого агента. Последнюю версию пакета можно получить на Web-узле ucd-snmp.ucdavis.edu. С конца 2000 г. проект перешел под управление компании SourceForge и стал называться Net-SNMP. Изменилось и местонахождение Web-узла (теперь его адрес — net-snmp.sourceforge.net).

Как и в других реализациях SNMP, UCD-агент собирает данные о локальном компьютере и предоставляет их SNMP-менед-жерам по сети. По умолчанию инсталлируются базы MIB, содержащие статистические данные об использовании сетевого интерфейса, памяти, дисков, процессов и центрального процессора. Возможности агента достаточно обширны, так как он может запустить любую Unix-команду и представить ее выходные данные в качестве SNMP-ответа. Это позволяет посредством протокола SNMP осуществлять мониторинг практически любых событий, происходящих в системе.

По умолчанию агент инсталлируется под именем /usr/sbin/snmpd. Обычно он запускается на этапе начальной загрузки системы и считывает параметры своей конфигурации из файлов, находящихся в каталоге /etc/snmp. Наиболее важный из этих файлов — snmpd.conf; он содержит большинство конфигурационных параметров и описание множества доступных методов сбора данных. При разработке пакета его авторы полагали, что пользователи должны редактировать только файл snmpd.local.conf. Но на практике приходится хотя бы один раз изменять и файл snmpd.conf, чтобы отключить те методы сбора данных, использование которых не планируется.

Таблица 7.3

Опции демона snmpd пакета UCD

Опция	Функция
-1 *файл*	Направлять журнальную информацию в *файл*
-a	Регистрировать адреса всех SNMP-соединений
-d	Регистрировать содержимое каждого SNMP-пакета
-V	Включить режим подробного описания событий
-D	Регистрировать отладочную информацию
-h	Отображать все аргументы демона snmpd
-H	Отображать все директивы конфигурационного файла
-A	Добавлять данные в журнальный файл, а не перезаписывать его
-s	Направлять регистрационные сообщения в систему Syslog

Сценарий configure пакета UCD позволяет задать используемый по умолчанию журнальный файл и ряд других локальных параметров. С помощью опции -1, указываемой при вызове демона snmpd, можно выбрать другой журнальный файл, а посредством опции -s организуется направление журнальных сообщений в систему Syslog. Перечень наиболее важных опций демона snmpd приведен в табл. 7.3. Рекомендуется всегда задавать опцию -a. При поиске неисправностей удобно применять опции -V, -d и -D, которые позволяют получать более подробную информацию о происходящих в системе событиях.

Существует большое количество полезных модулей Perl для SNMP. Тем, кто собирается писать собственные сценарии управления сетью, рекомендуется обратиться в архив CPAN за примерами. Архив CPAN (Comprehensive Perl Archive Network — глобальная сеть архивов Perl-программ) содержит коллекцию полезных модулей Perl. (Обращайтесь по адресу www.cpan.org.)

7.2.3. Программы управления сетью

Наибольший интерес представляют утилиты пакета UCD.

Даже если система поставляется с собственным SNMP-серве-ром, для полноценного администрирования понадобится скомпилировать и инсталлировать семь клиентских утилит пакета UCD, перечисленных в табл. 7.4.

Перечисленные утилиты очень удобно использовать в сценариях. Например, часто требуется сценарий, в котором данные,

полученные утилитой snmpget, каждые несколько минут сохраняются в текстовом файле.

Примечательна также утилита snmpwalk. Начав с указанного идентификатора OID (или, по умолчанию, с начала базы MIB), она выполняет в цикле запрос get-next. В результате формируется полный список доступных идентификаторов OID и их значений.

Программа многомаршрутный визуальный анализатор трафика MRTG (Multi-Router Traffic Grapher) собирает данные SNMP и строит графики их изменения во времени. Программа написана преимущественно на языке Perl. Она оказывает неоценимую помощь в анализе использования системы и сетевых ресурсов.

Программа MRTG периодически запускается демоном сгоп и может получать данные от любого источника SNMP. При каждом запуске полученные данные сохраняются и строятся новые графики.

Эта свободно распространяемая программа имеет ряд особенностей. Во-первых, она, использует не требующую административного вмешательства базу данных фиксированного размера, в которую записываются только сведения, необходимые для создания графиков. Например, программа MRTG умеет сохранять одну выборку для каждой минуты дня, для каждого часа недели и для каждой недели года. Такая схема укрупнения позволяет предоставлять пользователям важную информацию, не требуя хранения несущественных деталей и затрат времени на администрирование базы данных.

Во-вторых, программа MRTG способна записывать значения и отображать графики их изменения во времени для любой SNMP-переменной. Вместе с SNMP-агентом пакета UCD программа

Таблица 7.4

Утилиты пакета UCD

Утилита	Назначение
snmpget	Получает от агента значение SNMP-переменной
snmpgetnext	Получает значение следующей переменной последовательности
snmpset	Передает агенту значение SNMP-переменной
snmptable	Получает таблицу значений SNMP-переменных
snmptranslate	Осуществляет поиск идентификаторов 01D и их описаний в иерархии базы MIB
snmptrap	Генерирует сообщение о прерывании
snmpwalk	Просматривает базу MIB начиная с заданного идентификатора OID

MRTG обеспечивает мониторинг практически всех системных и сетевых ресурсов. Эти графики характеризуют трафик, проходящий через сетевой интерфейс в течение дня и недели.

Идеи, заложенные в программе MRTG, получили развитие в новой системе RRDtool, созданной тем же автором. Концепция системы та же самая, но средства укрупнения данных и графические возможности усовершенствованы. В отличие от программы MRTG, система RRDtool не имеет собственных методов сбора информации. Данные должны быть получены другими программами.

В настоящее время сбор данных для системы RRDtool лучше всего осуществляет программа Cricket, написанная Джеффом Алленом (Jeff Allen). Она не ограничивается только данными SNMP и способна получать информацию почти от любого сетевого источника. Программа написана на языке Perl и может быть легко модифицирована для обработки новых источников данных.

Интерактивный сетевой административный центр NOCOL (Network Operation Center On-Line) представляет собой систему управления событиями. Эта система не поможет администратору выяснить, насколько возросла загруженность сети за последний месяц, зато она способна уведомить о крахе Web-сервера. Система может посылать сообщения на пейджеры обслуживающего персонала (или по электронной почте), информируя его о самых разных событиях.

В дистрибутив входят программы мониторинга, которые следят за различными проблемными компонентами сети. Можно создавать дополнительные мониторы на языках Perl или C. Базовые методы оповещения пользователей таковы: отправка сообщения по электронной почте, создание Web-страницы, отображение статусной информации посредством функций библиотеки curses и сброс сообщения на пейджер через модем. Как и в случае с программами мониторинга, разрешается дополнять этот список собственными методами.

Тем, кто не может себе позволить приобрести коммерческие средства управления сетью, рекомендуется использовать систему NOCOL.

Она очень'хорошо работает в сетях, где число узлов и контролируемых устройств не превышает 100. За дополнительной информацией можно обращаться по адресу www.netplex-tech.com. В настоящее время компания Netplex Technologies предлагает систему следующего поколения: SNIPS (System and Network Integrated Polling Software — интегрированная программа опроса системы и сети).

Далее приведены требования к системам управления сетью и их обоснования.

По требованию получения различных видов данных: для систем управления сетью важно уметь получать не только данные SNMP. Многие пакеты позволяют принимать информацию от большинства других сетевых служб, например выполнять SQL-запросы, обращаться к DNS и Web-серверам.

По качеству пользовательского интерфейса: важно, чтобы интерфейс позволял представлять информацию наглядно и понятно.

Дорогостоящие системы обычно позволяют выбирать между имеющимся графическим интерфейсом или Web-интерфейсом. Пакеты, разработчики которых учитывают рыночную конъюнктуру, поддерживают XML-шаблоны для представления данных.

По стоимости: некоторые пакеты имеют завышенную цену. Пакет OpenView компании Hewlett-Packard является одним из наиболее дорогостоящих, но в то же время одним из самых распространенных.

Для ряда корпораций престижно, что их сети управляются высококачественной коммерческой системой. Если для организации это не так важно, то надо обратить внимание на бесплатное программное обеспечение (например, MRTG или NOCOL).

По автоматизации обнаружения узлов: ряд систем обладает возможностью обнаруживать сеть. Отправляя широковещательные ping-пакеты, выполняя SNMP-запросы, просматривая таблицы маршрутизации и обращаясь к службе DNS, они способны идентифицировать все компьютеры и устройства в сети. Как правило, данная функция реализована хорошо, но она не всегда справляется со сложными сетями или сетями со «строгими» брандмауэрами.

По отчетности: многие программы способны отправлять предупреждения по электронной почте, выдавать сообщения на пейджеры и автоматически генерировать уведомления для популярных систем слежения за ошибками. Необходимо убедиться, что выбранная платформа позволяет гибко настраивать систему отчетности.

По возможностям конфигурирования: некоторые производители в своих разработках пошли гораздо дальше простого мониторинга и выдачи сообщений.

Их системы позволяют управлять конфигурацией компьютера или устройства. Например, система Cisco Works посредством специального интерфейса разрешает пользователю изменять конфигурацию маршрутизатора. Поскольку данные о конфигурации устройства необходимы для глубокого анализа сетевых проблем, можно предположить, что большинство новых программ будет располагать средствами изменения конфигурации сетевых компонентов.

7.3. Технологии управления дисками при администрировании ИС

7.3.1. Общие положения по управлению дисками в ИС

Эти процедуры рассмотрим на примере управления дисками при администрировании Windows NT. Они основываются на программе Disk Administrator, которая входит в состав средств администрирования Windows NT. Программа Disk Administrator позволяет:

- получать информацию о размерах разделов диска; объеме свободного пространства, оставшегося на диске для создания разделов; метке тома, букве дисков, типе и размере файловой системы;
- форматировать тома и назначать им метки;
- создавать и удалять разделы на жестком диске и определять логические диски;
- изменять назначения букв дисков (в том числе компакт-дисков);
- создавать, удалять и восстанавливать зеркально отображаемые наборы дисков;
- создавать и удалять распределенные по дискам наборы данных, а также регенерировать утраченные или ошибочные элементы данных с помощью контроля четности.

В Windows NT имеются широкие возможности управления дисками. В свободном пространстве на жестком диске можно создать до четырех разделов, а дополнительный раздел допускает разбиение на логические диски. В системную конфигурацию можно добавить дополнительные диски, восстановить сохраненную конфигурацию дисков, назначить имена каждому из основных разделов и логических дисков. Любой раздел, кроме системного, разрешается удалять.

Если вся работа выполняется только в операционной системе Windows NT, то весь диск можно отвести под один большой раздел, если необходимо иметь другие операционные системы (Unix, MS DOS), файловые системы которых несовместимы с Windows NT (для каждой из них целесообразно создать системный раздел). Исключением является возможность совместного размещения MS DOS и Windows NT в одном разделе, размеченном с помощью файловой системы FAT.

Программа инсталляции Windows NT предусматривает возможность разбиения жесткого диска на разделы в ходе установки. Программа Disk Administrator используется для изменения структуры разделов на имеющихся дисках и разбиения на разделы новых дисков.

Разделы, содержащие файлы для запуска компьютера и файлы операционной системы, называются системными и загрузочными.

Загрузочный раздел Windows NT представляет собой том с файловой системой NTFS или FAT, содержащий файлы операционной системы Windows NT. Раздел может быть одновременно как системным, так и загрузочным, хотя это и необязательно.

Работать с администратором дисков легко, однако необходимо иметь в виду следующее:

- изменения, внесенные с помощью Disk Administrator, будут действовать только после сохранения;
- если изменения сохранены, то, чтобы они подействовали, нужно остановить и снова запустить систему;
- для перезапуска нужно выйти из Disk Administrator. Если текущее местоположение не позволяет выполнить перезагрузку, то следует нажать комбинацию клавиш [Ctrl] + [Esc] для переключения в Program Manager;
- если к системе добавлен новый диск, то после повторного запуска он должен автоматически представляться в Disk Administrator. Если этого не происходит, значит инсталляция проведена с ошибками.

Для эффективной работы с Disk Administrator используется ряд специфических понятий, терминов и определений.

Физический диск — изделие (дисковод), каждому из которых присваивается один из неизменяемых номеров (0, 1, 2 и т.д.), а емкость диска фиксирована.

Раздел (partition) — часть жесткого диска, которая ведет себя как один физический жесткий диск. Разделы могут быть основными (primary) или дополнительными (extended).

Основной раздел — часть физического жесткого диска, помеченная как используемая для загрузки операционной системы. На диске допускается до четырех таких разделов (под разные системы). В Disk Administrator основной раздел показывается темной фиолетовой полосой в верхней части.

Дополнительные разделы — создаются из свободного пространства диска. Допускается только один такой раздел на каждом жестком диске, но он может быть разбит на мелкие части — логические диски.

В отличие от физического диска логический раздел представляет собой логический набор, логический диск, основной раздел или что-то другое — то, чему Disk Administrator может присваивать букву диска.

Можно менять присвоенные буквы и размеры логических дисков (хотя физически таких отдельных дисков не существует). Логический раздел может быть частью физического диска или занимать один (несколько) физический диск.

Системный раздел — раздел, содержащий аппаратно-зависи-мые файлы (Ntldr, Osloader.exe, Boot.ini и Ntdetect.com) для загрузки Windows NT.

Загрузочный раздел — раздел, содержащий файлы операционной системы Windows NT из каталогов % Systemroot % и % Systemroot %\System32.

Логический диск — раздел на одном диске, который функционирует как отдельная физическая сущность. Раздел допускается разбивать на любое число логических дисков. Однако NT Server поддерживает только 25 букв фиксированных дисков (вместе с гибким). Логический диск, на котором инсталлирована сама операционная система NT, не может превышать 2 Гбайт. Данный хранятся на логических дисках любого размера. Логические диски отображаются в Disk Manager голубой штриховкой.

Свободное пространство (free space) — дисковая память, не являющаяся частью раздела. Свободное пространство можно преобразовывать. В Disk Administrator оно графически изображается горизонтальной штриховкой.

SLED (Single Large Expensive Disk) — дорогостоящий одиночный диск большой емкости. Этим термином называют способ организации данных на одном очень большом и надежном диске.

RAID (Redundant Array of Inexpensive Disks) — массив резервных недорогих дисков, представляющий собой реализацию метода защиты данных путем комбинирования небольших недорогих дисков. За счет избыточности повышается отказоустойчивость. Существуют шесть видов реализации метода RAID. Все они работают по-разному и имеют различное применение. NT Server поддерживает уровни 0, 1 и 5.

Групповой том (набор томов) — диск или часть диска, скомбинированная с пространством на другом физическом диске и образующая один большой том. Ему присваивают обозначение диска. Применяется групповой том в целях эффективного использования дисковой памяти; можно создать большой том, располагая мелкими фрагментами свободного пространства. Групповой том можно расширять при наличии свободного пространства, но нельзя уменьшать.

Для этого его нужно удалить и создать новый. На экране Disk Administrator групповой том представляется желтой полосой в верхней части области.

Зеркально отображаемый набор — набор данных, содержащий основной экземпляр данных и его копию в области свободного пространства идентичного размера. Disk Administrator обозначает зеркально отображаемый набор данных малиновой полосой в верхней части области.

Фрагментированный (чередующийся) набор данных — такой набор, данные которого распределяются по нескольким дискам — трем и более, если используется контроль четности, или минимум двум, если такой контроль отсутствует. Этот подход обеспечивает защиту данных и уменьшение времени чтения.

Обычно на дисках массива выбирают свободные области, которые комбинируют во фрагментированный набор. Данные хранятся во фрагментах (stripes) определенного размера. Фрагмента -рованному набору можно присвоить обозначение диска, и после форматирования такой набор ведет себя как обычный диск.

Фрагментированные наборы данных представляются в интерфейсе Disk Administrator зеленым цветом. Тип набора определяется щелчком мыши по нему. При этом в строке состояния будет дано описание типа.

7.3.2. Технологический процесс управления дисками

Новый диск прежде всего необходимо отформатировать. Для выполнения этой операции нужно открыть папку My Computer или Explorer и щелкнуть правой кнопкой мыши по логическому диску. На экране появятся доступные варианты форматирования диска. Форматировать свободное пространство нельзя, поэтому сначала нужно создать раздел или логический диск. Для этого надо на форматируемом разделе выделить его, а затем в меню Partition выбрать команду Commit Change Now. Когда информация о разделе сохранится, его нужно оставить подсвеченным и выбрать в меню Tools команду Format.

В диалоговом окне Format следует выбрать файловую систему, которую предполагается использовать в разделе. Обычно все разделы имеют тип NTFS (в целях повышения защиты).

Единственное исключение может составлять загрузочный раздел, который может быть типа FAT. Это дает возможность при необходимости загрузиться с системной дискеты DOS.

Для форматирования дисков можно воспользоваться командной строкой MS DOS:

```
format буква_диска:/fs:файловая_система, например, format E:/
fs:ntfs
```

Присвоение меток разделам осуществляется командой Properties меню Tools администратора дисков или командой Label, вводимой с командной строки. Имеется возможность замены файловой системы раздела FAT на NTFS с помощью программы Convert, запускаемой с командной строки. При этом все данные на диске сохраняются. Обратный переход от NTFS к FAT программа Convert не выполняет.

Для хранения информации в Windows используются SLED-диски. Такой диск разбивается на логические диски. Делается это преобразованием свободного пространства в дополнительный раздел. Для этого нужно зайти в окно Disk Administrator,

выбрать требуемый диск и щелкнуть мышью на свободном пространстве.

Затем выбирают в меню Partition пункт «Extended Partition» (дополнительный раздел). В результате на экране появится диалоговое окно, запрашивающее размер дополнительного раздела. Здесь следует выбрать необходимый размер и щелкнуть по кнопке *ОК*.

Для создания логического диска необходимо щелкнуть мышью по области расширенного раздела (при этом он выделяется), а затем выбрать в меню Partition команду Create *(Создать)*. В появившемся на экране диалоговом окне Create Logical Drive нужно ввести желаемый размер логического диска или нажать клавишу [Enter] для выбора опции по умолчанию (выделяется все свободное пространство). После щелчка по кнопке Оологический диск будет создан.

После выхода окна из Disk Administrator появляется диалоговое окно, в котором для сохранения изменений нужно щелкнуть мышью по кнопке *ОК*. Disk Administrator подтверждает, что изменения внесены, и выводит окно с просьбой перезапуска системы для приведения в действие внесенных изменений. Если теперь щелкнуть по кнопке *ОК,* то система будет автоматически остановлена и перезапущена.

Логические диски можно удалять. Для этого выполняется следующая последовательность действий:

1) выбирается нужное имя диска в окне Disk Administrator и дается команда Delete из меню Partition;

2) в ответ на запрос системы дается подтверждение удаления диска.

В результате получается пустой раздел. Для его преобразования в свободное пространство нужно удалить и его.

При наличии SLED рано или поздно возникнет проблема с ограничением емкости и приходится применять еще один (или более) диск. Чтобы эффективно использовать дисковую память, можно скомбинировать два (или более) диска в групповой том. У такого тома есть существенный недостаток. Если откажет один из дисков, то остальная часть группового тома станет недоступной. Поэтому важно не забывать о резервном копировании.

Для создания группового тома (набора томов) нужно заархивировать имеющиеся на дисках данные, убедиться в наличии свободного пространства и выполнить следующую последовательность действий:

1) открыть окно Disk Administrator;

2) выделить на жестких дисках свободные области, последовательно щелкнув по ним мышью при нажатой клавише [Ctrl];

3) перейти в меню Partition и выбрать команду Create Volume Set *(Создать набор томов)*. На экране появится диалоговое окно, в котором выводится минимальный и максимальный размеры тома;

4) ввести нужный размер группового тома и щелкнуть по кнопке *OK*. Произойдет возврат в экран Disk Administrator. Члены группового тома будут отображены желтым цветом.

Полученный диск уже будет иметь обозначение, но пока не отформатирован. Чтобы это сделать, надо воспользоваться меню Tools или командной строкой (см. ранее).

При реорганизации данных на дисках может возникнуть потребность в удалении группового тома или расширении его. Также для создания тома меньшего размера необходимы его удаление и последующее создание нового тома. Расширение тома не требует его удаления; в этом случае к существующему тому нужно добавить область свободного пространства.

Для удаления тома необходимо выполнить следующую последовательность действий:

1) перейти в Disk Administrator;

2) щелкнуть мышью по групповому тому, который нужно удалить. Его контур становится черным;

3) в меню Partition выбрать Delete. На экране появится сообщение с просьбой подтвердить удаление тома и напоминанием о том, что данные тома будут потеряны (их следует заранее архивировать);

4) для продолжения нужно щелкнуть мышью по кнопке *Yes*.

После удаления группового тома задействованная для него об ласть снова становится свободной.

Для расширения группового тома необходимо:

1) в окне Disk Administrator выбрать существующий групповой том или основной раздел, который уже был отформатирован и не является частью зеркально отображаемого или фрагментирован-ного набора (расширить можно только уже отформатированный групповой том);

2) перейти в меню Partition и выбрать в нем пункт Extend Volume Set («Расширить групповой том»). Как и при создании томов других типов, на экране появится диалоговое окно, показывающее минимальный и максимальный размеры тома;

3) ввести нужный размер тома и щелкнуть мышью по кнопке *OK*.

Для группового тома действуют три ограничения:

1) изложенную процедуру нельзя использовать для уменьшения размера тома;

2) невозможно расширить групповой том, если раздел содержит системные файлы. Disk Administrator не позволит добавить свободное пространство к такому разделу;

3) не допускается комбинировать два групповых тома, а также добавлять к групповому тому логический диск.

Чередующиеся (фрагментированные) наборы создаются примерно так же, как и наборы томов, однако ограничений здесь

больше. Все входящие в чередующийся набор разделы должны находиться на разных дисках, общее число которых не может превышать 32. Администратор дисков проводит выравнивание всех объединяемых разделов по размеру. Данные чередующегося набора записываются как последовательность полос, каждая из которых проходит через все диски. Такая процедура эквивалентна RAID уровня 0.

Время доступа к такому набору данных значительно уменьшается, поскольку операции чтения/записи будут выполняться одновременно на нескольких (минимум двух) дисках. Однако если что-то случится с одним из участвующих в наборе дисков, все распределенные по дискам данные будут потеряны.

Для создания набора распределяемых по дискам данных без контроля четности нужно выполнить следующие действия:

1) в окне Disk Administrator выбрать две (или более) области свободного пространства на нескольких дисках (щелкнуть мышью в областях свободного пространства при нажатой клавише [Ctrl]);

2) в меню Partition выбрать команду Create Stripe Set *(Создать набор полос)*. На экране появится окно с минимальным и максимальным размерами создаваемого диска;

3) выбрать нужный размер набора дисков и щелкнуть мышью по кнопке *OK*.

Теперь Disk Administrator поровну распределит заданный объем между доступными дисками и присвоит всему набору одну букву. Чтобы изменения вступили в силу, следует перезагрузить систему. Созданный набор необходимо отформатировать.

Для удаления фрагментированного набора данных нужно выполнить следующие действия:

1) выбрать в окне Disk Administrator удаляемый набор;

2) в меню Partition выбрать команду Delete;

3) подтвердить удаление набора, для чего щелкнуть мышью по кнопке *Yes*.

Чередующиеся наборы с четностью предусматривают использование одного блока четности на каждую полосу данных. В результате набор должен включать в себя не менее трех дисков. Блоки четности равномерно распределены по разделам, что позволяет лучше сбалансировать ввод-вывод между дисками. Такая процедура эквивалентна RAID уровня 5.

Скорость чтения данных для чередующихся наборов с четностью выше, чем для зеркальных наборов, снижается. Так, при отказе одного из компонентов, например при сбое диска, скорость диска уменьшается из-за необходимости восстановления данных на основе сведений о четности.

В целом чередующиеся наборы с четностью имеют преимущество перед зеркальными наборами при работе с приложениями, требующими резервирования данных и выполняющими преиму-

щественно их чтение. Скорость записи здесь снижается за счет определения четности, и в обычном режиме любая операция записи требует втрое больше памяти, чем операция чтения. Более того, при сбое одного из разделов каждая операция чтения требует втрое больше памяти, чем обычно, что также связано с определением четности.

Для создания чередующегося набора с контролем четности необходимо выполнить следующую последовательность действий:

1) открыть окно Disk Administrator и выбрать области свобод ного пространства на трех или более дисках. Области свободного пространства необязательно должны быть равными;

2) в меню Fault Tolerance выбрать команду Create Stripe Set With Parity *(Создать чередующийся набор с контролем по четности).* На экране появится окно с минимальным и максимальным зна чениями размеров^ данного набора;

3) выбрать нужный размер форматируемого диска и щелкнуть мышью по кнопке *ОК.*

Созданному набору будет присвоено обозначение диска. После этого нужно выйти из Disk Administrator и перезапустить систему. После перезапуска нужно отформатировать новый раздел, в противном случае при попытке работать с диском на экран будет выведено сообщение об ошибке.

В случае невосстанавливаемой ошибки (даже если один из дисков набора затерт полностью) можно регенерировать записанные данные, используя информацию четности. Если попытаться выполнить запись на неисправный фрагментированный набор, на экране появится сообщение: «Диск, являющийся разделом отказоустойчивого тома, больше недоступен». В этом случае необходимо выполнить следующую последовательность действий:

1) установить новый диск и перезагрузить систему. Это дает возможность увидеть новый диск;

2) перейти в Disk Administrator, выбрать фрагментированный набор, который нужно исправить, и задать новый фрагмент свободного пространства, не меньший по объему, чем размер других членов набора;

3) в меню Fault Tolerance выбрать команду Regenerate *{Регенерация).*

Тогда произойдет перезапуск системы, а затем в фоновом режиме инициализируется процесс регенерации. Хотя процесс регенерации потребует некоторого времени, он не помешает работе с сервером. Когда фрагментированный набор будет исправлен, ему нужно присвоить новую букву диска и перезапустить компьютер. Отказавшая часть набора резервируется как неиспользуемая и называется зависшей. Такой диск в окне Disk Administrator имеет под номером запись OFF-UNE («Не используется»).

Следует иметь в виду, что, хотя обращаться к информации чередующегося набора с четностью можно даже при отказе одного из дисков, нужно как можно скорее регенерировать набор. Дело в том, что чередование с четностью позволяет справиться только с однократной ошибкой.

Поэтому если с набором произойдет что-то еще, данные будут потеряны.

Если возникает необходимость в удалении набора с четностью, то нужно выполнить следующие действия:

1) выбрать удаляемый диск в окне Disk Administrator;

2) в меню Partition воспользоваться командой Delete. На экране появится предупреждение о потере всех данных с просьбой подтвердить удаление;

3) щелкнуть мышью по кнопке *Yes.*

В результате будет удален фрагментированный набор вместе с информацией четности.

Для защиты информации NT Server предлагает два метода: зеркальное отображение дисков и чередование данных с контролем четности.

Если в системе имеется несколько дисков, то можно задать зеркальное отображение раздела одного диска на свободное пространство другого. Зеркальное отображение дисков эквивалентно RAID уровня 1. При каждой операции записи данных на один диск, участвующий в наборе, данные одновременно записываются и на другой диск. Производительность от этого не снижается, так как каждый диск выполняет операцию самостоятельно. К тому же при считывании данные можно извлекать сразу с двух дисков. Зеркальные наборы более дорогостоящие по сравнению с чередующимися наборами, но обеспечивают большую надежность хранения данных.

Система NT Server позволяет организовать также дублирование дисков (disk duplexing) — почти то же самое, что и зеркальное отображение (disk mirroring), но в этом случае каждый диск имеет собственный контроллер, поэтому данные не будут уязвимы в случае отказа как одного диска, так и одного контроллера.

Создание зеркальной копии диска не повлияет на данные, имеющиеся на нем. Для задания зеркального отображения дисков необходимо:

1) в окне Disk Administrator щелкнуть мышью по разделу, для которого нужно создать зеркальную копию;

2) нажать клавишу [Ctrl] и одновременно щелкнуть мышью по свободному пространству другого диска, не меньшему по размеру, чем набор, для которого нужно создать зеркальную копию;

3) в меню Fault Tolerance *(Отказоустойчивость)* выбрать команду Establish Mirror *(Установка зеркала).*

В результате Disk Administrator создаст на свободном пространстве раздел для зеркального отображения, который ассоциируется с той же буквой диска, что и исходный набор.

Если с одной половиной зеркального набора происходит что-то непоправимое (например, отказ аппаратного компонента), то следует разделить набор и превратить оставшуюся целой часть в отдельный раздел или логический диск. После этого зеркальный набор можно воссоздать, используя свободное место на другом диске.

Для разделения зеркально отображаемого набора данных следует:

1) открыть Disk Administrator и выбрать зеркальный набор. На экране появится сообщение о том, что один (или более) диск с того времени, как был последний раз запущен Disk Administrator, находится в автономном режиме (off-line). Также сообщается, что информация о конфигурации потерянных дисков будет сохранена. В ответ нужно щелкнуть мышью по кнопке *О К;*

2) выбрать в меню Fault Tolerance *(Отказоустойчивость)* команду Break Mirror *(Разрыв зеркала).* На экране появится сообщение: «Все данные зеркального набора будут утеряны. Вы уверены, что хотите разрушить зеркальный набор и удалить компоненты раздела?». Нужно щелкнуть по кнопке *Yes.*

После разбиения зеркального набора исправный раздел сохраняет букву диска, а неисправному разделу присваивается следующая доступная буква.

Для восстановления разделенного зеркального набора дисков нужно в окне Disk Administrator выбрать хорошую половину зеркального набора и область в закрашенном зеленым цветом свободном пространстве, которая должна быть не меньше по размеру. После этого в меню Fault Tolerance следует дать команду Establish Mirror. Новый зеркальный набор обозначится малиновым цветом.

7.3.3. Управление дисками по обеспечению ИБ в сети

В гл. 4 были рассмотрены общие положения обеспечения ИБ при администрировании ИС. Больший же интерес представляет использование методологии NTFS 5.0 для обеспечения безопасности и надежности хранения данных на дисковых накопителях при управлении ими в процессе администрирования.

Рассмотрим возможности NTFS 5.0 в этих процессах. К таким возможностям относятся:

- назначение разрешений для файлов;
- квоты дискового пространства;
- передача прав владения файлом или папкой;
- точки соединения NTFS;

• отслеживание связей;
• шифрующая файловая система.

Устанавливая пользователям определенные разрешения для файлов и папок, администраторы могут защищать конфиденциальную информацию от несанкционированного доступа.

Для назначения пользователю или группе разрешения на доступ к определенному файлу необходимо:

1) щелкнуть правой клавишей мыши по требуемому файлу. Выбрать из контекстного меню команду *Свойства* (Properties);

2) в появившемся окне перейти на вкладку *Безопасность* (Security);

3) в группе «Имя» (Name) показаны пользователи и группы, которым предоставлены разрешения для данного файла. Для добавления или удаления кого-либо из списка следует щелкнуть по кнопке *Добавить* (Add) или *Удалить* (Remove);

4) щелкнуть по кнопке *Добавить.* Откроется окно диалога *Выбор:* «Пользователи, Компьютеры или Группы» (Select Users, Computers or Groups);

5) выбрать нужный объект в группе «Имя» (Name) и щелкнуть по кнопкам *Добавить* (Add), а затем (Ж для возврата в предыдущее окно;

6) в группе «Разрешения» (Permissions) назначить или запретить нужные стандартные разрешения для файлов. Каждое из этих стандартных разрешений состоит из наборов специальных разрешений, задающих возможность выполнения конкретного действия с файлами или каталогами (табл. 7.5);

7) если требуется задать более тонкие настройки доступа к файлу, щелкнуть по кнопке *Дополнительно.* На экране появится окно *Параметры управления доступом* (Access Control Settings). На вкладке *Разрешения* будут показаны список пользователей или групп и предоставленные им разрешения для данного объекта;

8) чтобы отредактировать разрешения для пользователя (группы), нужно выбрать соответствующую строку и щелкнуть по кнопке *Показать/Изменить* (View/Edit);

9) в новом окне *Элемент разрешения* (Permission Entry) можно установить разрешения, не объединенные в стандартные разрешения.

Аналогично устанавливаются разрешения для папок (здесь свой набор разрешений). Следует иметь в виду, что разрешения доступа к файлам имеют приоритет над разрешениями доступа к папкам.

В предыдущих версиях Windows NT любой пользователь мог распоряжаться всем пространством жестких дисков серверов. Это усложняло администрирование дисковой памяти. В Windows 2000 администратор может квотировать (ограничивать) размер дискового пространства сервера, к которому обращается пользователь.

Таблица 7.5

Выбор специальных разрешений и их стандартное наполнение

Специальные разрешения	Стандартные наполнения				
	Полный доступ	Изменить	Чтение и выпол-нение	Чтение	Запись
Обзор папок/ Выполнение файлов	x	x	x	—	—
Содержание папок/ Чтение данных	x	x	x	x	—
Чтение атрибутов	x	x	x	x	—
Чтение дополнительных атрибутов	x	x	x	x	—
Создание файлов/ Записьданных	x	x	—	—	x
Создание папок/ Дозапись данных	x	x	—	—	x
Запись атрибутов	x	x	—	—	x
Запись дополнительных атрибутов	x	x	—	—	x
Удаление подпапок и файлов	x	—	—	—	—
Удаление	x	x	—	—	—
Чтение разрешений	x	x	x	—	x
Смена разрешений	x	—	—	—	—
Смена владельца	x	—	—	—	—
Синхронизация	x	x	x	—	x

Примечание. Знаком «x» обозначены виды стандартных наполнений для специальных разрешений.

Для установления квоты лицо, обладающее необходимыми полномочиями, должно выполнить следующие действия:

1) щелкнуть правой кнопкой мыши по конфигурируемому тому и в появившемся контекстном меню выбрать команду *Свойства;*

2) на экране появится окно *Свойства,* в котором нужно перейти на вкладку *Квота* (Quota);

3) установить флажок «Включить управление квотами» (Enable quota management) или флажок «Не вьщелять место на диске при

превышении квоты» (Deny disk space to users exceeding quota limit). В первом случае будет осуществляться мягкий режим контроля, во втором — более жесткий режим контроля, при котором в случае превышения квоты пользователю будет отказано в доступе к тому;

4) установить размер выделяемой квоты и порог, превышение которого вызовет запись предупреждения в журнал событий;

5) чтобы узнать, какие пользователи превысили выделенную им квоту (в мягком режиме), нужно щелкнуть по кнопке *Записи квот* (Quota Entries). Появится окно *Записи квот,* в котором будет отображен список пользователей с параметрами их квот и объемом используемого ими дискового пространства;

6) для коррекции параметров квоты пользователя дважды щелкнуть по соответствующей строке и в появившемся диалоговом окне *Параметры квоты* (Quota Settings) установить требуемые значения;

7) щелкнуть по кнопке *ОК.*

В Windows NT 4.0 право владения файлом или папкой являлось характеристикой, жестко привязанной к создателю данного объекта. Право владения не могло быть передано другому пользователю, за исключением администратора. В Windows 2000 любой пользователь (имеющий необходимые полномочия) может назначить себя владельцем какого-либо объекта файловой системы.

Для передачи владения объектом файловой системы или просмотра текущего владельца этим объектом необходимо:

1) открыть окно свойств этого объекта, щелкнув по нему правой клавишей мыши, и перейти на вкладку *Безопасность;*

2) щелкнуть по кнопке *Дополнительно* и в появившемся окне *Параметры управления доступом* перейти на вкладку *Владелец* (Owner);

3) текущий владелец объекта показан в поле «Текущий владелец этого элемента» (Current owner of this item). Выбрать строку с именем пользователя из списка «Изменить владельца на» (Change owner to) для передачи права владения;

4) щелкнуть по кнопкам *Применить* (Apply), а затем *ОК.*

Файловая система NTFS 5.0 позволяет создавать общее пространство имен хранения информации путем создания точек соединения (junction point) NTFS. Это новое средство, позволяющее отображать целевую папку в пустую папку, находящуюся в пространстве имен файловой системы NTFS 5.0 локального компьютера. Целевой папкой может служить любой допустимый путь Windows 2000. В этом смысле точки соединения NTFS похожи на точки соединения распределенной файловой системы DFS, т.е. оба эти механизма отображают одно пространство имен хранения на другое. Точки соединения NTFS прозрачны для приложений. Это означает, что приложение или пользователь, осуществляю-

щий доступ к локальной папке NTFS, автоматически направляется к другой папке.

Для создания точки соединения можно использовать утилиту mountvol.exe и оснастку «Управление дисками» (Disk Management). В первом случае работа осуществляется из командной строки, во втором случае используется графический интерфейс, что более удобно.

Для создания точки соединения необходимо:

1) запустить оснастку «Управление дисками»;

2) щелкнуть Правой кнопкой мыши по нужному тому файловой системы и выбрать в контекстном меню команду *Изменение буквы диска и пути диска* (Change Drive Letter and Path);

3) в появившемся диалоговом окне *Изменение буквы диска или путей* (Change Drive Letter or Path) щелкнуть по кнопке *Добавить* (Add). Откроется окно диалога;

4) в новом окне выбрать положение переключателя «Подключить» как следующую папку NTFS (Mount in this NTFS folder) и в текстовом поле указать новый путь к тому;

5) щелкнуть по кнопке *ОК*.

Для удаления точки соединения нужно в оснастке «Управление дисками» щелкнуть правой кнопкой мыши по нужному тому и в появившемся меню выбрать команду *Изменение буквы диска и пути диска.* Затем в открывшемся окне следует выбрать нужный путь и щелкнуть по кнопке *Удалить.* В заключительном окне подтвердить правильность выполняемого действия.

Вплоть до появления Windows 2000 предыдущие операционные системы не обеспечивали связь между ярлыком и соответствующим ему ресурсом, если ресурс переносился в другое место или переименовывался. В Windows 2000 появилась служба отслеживания изменившихся связей (Distributed Link Tracking), позволяющая приложениям находить ресурс, соответствующий данному ярлыку, и связи OLE даже в случае, если ресурс был переименован или перенесен в другое место дерева папок. Однако в полной мере эта служба работает только при перемещении ресурса в пределах файловой системы NTFS 5.0.

Кроме рассмотренных возможностей файловой системы NTFS 5.0 следует остановиться на ее шифрующей файловой системе (EFS), которая позволяет пользователям шифровать и расшифровывать файлы и применяется для защиты файлов от несанкционированного физического доступа (например, при хищении компьютера или его жесткого диска). Для обеспечения секретности данных в процессе шифрования применяется открытый ключ пользователя. Посторонние не смогут расшифровать информацию без соответствующего закрытого ключа. Для каждого зашифрованного файла создается специальный восстанавливающий ключ. Его использует компетентный администратор в экстренных ситуациях

(например, в случае отсутствия сотрудника или при потере закрытого ключа).

Шифрование/расшифровка проводится в ходе ввода-вывода автоматически и практически не влияет на производительность. Система EFS также поддерживает шифрование/расшифровку файлов на удаленных томах NTFS. Файлы могут быть экспортированы в зашифрованном виде, но по умолчанию данные перемещаются по сети незашифрованными. Для шифрования данных при перемещении по сети Windows 2000 поддерживает сетевые протоколы SSL, TLS и Ispec.

Использовать систему EFS можно двумя путями: с помощью утилиты командной строки cipher и с помощью Windows Explorer. Синтаксическое использование утилиты cipher имеет следующий вид:

cipher[/ез/d][/s:каталог][/a][/i][/f][/q][/h][/k]путь[...]]

Значения параметров шифрования/расшифровки приведены в табл. 7.6.

Например, для того чтобы зашифровать папку C:\My Documents, нужно набрать в командной строке

```
c:\cipher /E «My Documents»
```

Для того чтобы зашифровать все файлы с расширением doc, нужно ввести команду

```
c:\cipher /E /A*.doc
```

Так как шифрование и дешифрование выполняются автоматически, пользователь может работать с файлом так же, как и до установки его криптозащиты. Все остальные пользователи, которые пытаются получить доступ к зашифрованному файлу, получат сообщение об ошибке доступа, поскольку они не владеют необходимым личным ключом, позволяющим им расшифровать файл.

Кроме использования утилиты cipher шифрование информации можно выполнить с помощью *Проводника* (Explorer) системы Windows 2000. Для этого необходимо:

1) указать мышью файл или папку, которые требуется зашифровать. Щелкнуть правой клавишей мыши и выбрать в контекстном меню команду *Свойства;*

2) в открывшемся окне *Свойства* на вкладке *Общие* (General) щелкнуть по кнопке *Другие* (Advanced). Появится окно диалога *Дополнительные атрибуты* (Advanced Attributes);

3) установить флажок «Шифровать содержимое для защиты данных» (Encrypt contents to secure data) и щелкнуть по кнопке *OK;*

4) вернувшись в окно свойств зашифровываемого файла (папки), щелкнуть по кнопке *О К;*

5) в появившемся диалоговом окне указать режим шифрования. При шифровании папки можно указать следующие режимы:

Таблица 7.6

Значения параметров шифрования/расшифровки

Параметр	Описание
/e	Зашифровывает указанные папки. Папки маркируются так, что добавленные впоследствии файлы будут также зашифрованы
/d	Расшифровывает указанные папки. Папки маркируются так, что добавленные впоследствии файлы зашифрованы не будут
/s:dir	Выполняет выбранную операцию в указанной папке и во всех подпапках
/a	Выполняет операцию как для файлов, так и для каталогов
/i	Продолжает выполнение указанной операции даже после обнаружения ошибок. По умолчанию работа cipher останавливается, если встречаются ошибки
/f	Принудительно шифрует все выбранные объекты, даже если они уже зашифрованы
/q	Выводит только наиболее важную информацию
/h	Отображает скрытые или системные файлы
Д	Создает новый ключ шифрования файла для пользователя, запустившего cipher
Путь	Определяет шаблон имени, имя файла или имя папки полностью

• «Только к этой папке» (Apply changes to this folder);

• «К этой папке и всем вложенным папкам и файлам» (Apply changes to this folder, subfolder and files).

Для дешифрования файлов и каталогов нужно в окне свойств объекта на вкладке *Общие* щелкнуть по кнопке *Другие.* В открывшемся окне в группе «Атрибуты сжатия и шифрования» сбросить флажок «Шифровать содержимое для защиты данных».

Оснастка «Управление дисками» (Disk Management) заменила в Windows 2000 программу *Администратор дисков* (Disk Administrator), входившую в прежние версии Windows NT.

Оснастка «Управление дисками» включает в себя ряд дополнительных средств и возможностей:

• поддержка разделов и логических дисков Windows NT 4.0 и томов дисковых систем Windows 2000;

• управление дисковой системой в реальном времени (без отключения сервера и прерывания работы пользователей);

• удаленное и локальное управление дисковой системой;
• понятный и простой в работе интерфейс пользователя.

В отличие от предыдущих операционных систем Windows, позволяющих создавать только устройства с базовым режимом хранения информации (basic storage), Windows 2000 обеспечивает работу с новым типом устройств — устройствами с динамическим режимом хранения данных (dynamic storage). Диск, инициализированный для динамического хранения, называется *динамическим диском*. На нем могут находиться простые, составные, чередующиеся, зеркальные тома и тома RAID-5. Именно динамическое хранение данных позволяет управлять дисками и томами без перезагрузки операционной системы. Однако том, состоящий из нескольких дисков, должен иметь один режим хранения данных.

При работе с динамическими дисками оснастка «Управление дисками» позволяет выполнить следующие функции:

• создавать и удалять простые (simple, SLED), составные (spanned), чередующиеся (stripped), зеркальные (mirrored) тома, а также тома RAID-5;
• форматировать тома для файловой системы FAT или NTFS;
• расширять том на дополнительные диски;
• восстанавливать зеркальные тома и тома RAID-5;
• повторно инициализировать отключенный диск;
• изменять динамический режим хранения на базовый.

При работе с базовыми томами оснастка позволяет:

• создавать и удалять основной (primary) и дополнительный (extended) разделы;
• создавать и удалять логические устройства внутри дополнительного раздела;
• форматировать разделы, присваивать им метки, а также помечать разделы как активные;
• инициализировать диски;
• уничтожать наборы томов (volume set), чередующиеся (stripe set), зеркальные наборы (mirror set) и чередующиеся наборы с четностью (striped set with parity);
• отключать зеркальный диск;
• восстанавливать зеркальный набор;
• восстанавливать чередующиеся наборы с четностью;
• изменять базовый режим хранения данных на динамический.

Как для базовых, так и для динамических томов оснастка по
зволяет:

• контролировать информацию о дисках (объем, доступное свободное пространство, текущий статус);
• просматривать свойства томов и разделов;
• устанавливать и изменять назначение имен томам жестких дисков или разделам, а также устройствам CD-ROM;

Таблица 7.7

Сравнительные характеристики организации базовых и динамических дисков

Базовый диск	Динамический диск
Системный и загрузочный разделы	Системный и загрузочный тома
Основной раздел	Простой том
Дополнительный раздел	Простые тома и свободное пространство диска
Логическое устройство	Простой том
Набор томов	Составной том
Чередующийся набор	Чередующийся том
Зеркальный набор	Зеркальный том
Чередующийся набор с четностью	Том RAID-5

• устанавливать и проверять назначения общего доступа к тому или разделу.

Сравнительные характеристики организации базовых и динамических дисков приведены в табл. 7.7.

Оснастку «Управление дисками» можно использовать как самостоятельно, так и в составе основного инструмента администрирования Windows 2000 — оснастки «Управление компьютером» (Computer Management).

Контрольные вопросы

1. Опишите процессные и функциональные обязанности системного администратора в ОС Windows.
2. Что такое протокол SNMP и как он используется при администрировании сети?
3. Какие программы управления сетью вы знаете?
4. Сформулируйте основные требования к системам управления сетью.
5. Что из себя представляет программа Disk Administrator?
6. Опишите специфические понятия и термины программы Disk Administrator.
7. Что из себя представляет технологический процесс управления дисками?
8. Что такое SLED-диск?
9. Как используются уровни RAID в Disk Administrator?
10. Как осуществляется управление дисками по обеспечению ИБ в сети?
11. Что из себя представляет программа «Оснастка управления дисками»?

ПРИЛОЖЕНИЕ

Проект типовой должностной инструкции администратора сетей

1. Общие положения.

1.1. Администратор сетей относится к категории специалистов.

1.2. На должность администратора сетей назначается лицо, имеющее высшее профессиональное образование, без предъявления требований к стажу работы.

Администратор сетей 2-й категории — лицо, имеющее высшее профессиональное образование и стаж работы в должности администратора сетей или других инженерно-технических должностей, замещаемых специалистами с высшим профессиональным образованием, не менее трех лет.

Администратор сетей 1-й категории — лицо, имеющее высшее профессиональное образование и стаж работы в должности администратора сетей 2-й категории не менее трех лет.

1.3. Администратор сетей назначается на должность и освобождается от нее приказом руководителя организации по представлению руководителя структурного подразделения (непосредственного руководителя).

1.4. В своей деятельности администратор сетей руководствуется:

- нормативными документами по вопросам выполняемой работы;
- методическими материалами по соответствующим вопросам;
- приказами и распоряжениями руководителя организации;
- уставом организации;
- правилами трудового распорядка;
- настоящей должностной инструкцией.

1.5. Администратор сетей должен знать:

- нормативно-методические, организационно-распорядительные, другие руководящие и нормативные документы вышестоящих и других органов, касающиеся методов программирования и использования вычислительной техники при обработке информации и применения современных информационных технологий в вычислительных процессах;
- аппаратное и программное обеспечение сетей;
- нормализованные языки программирования;
- виды технических носителей информации, правила их хранения и эксплуатации;
- действующие стандарты, системы счислений, шифров и кодов;
- методы программирования;
- технико-эксплутационные характеристики, конструктивные особенности, назначения и режимы работы оборудования сетей, правила его технической эксплуатации;
- принципы простейшего ремонта аппаратного обеспечения;

• системы организации комплексной защиты информации;
• порядок оформления технической документации;
• передовой опыт в области современных информационных технологий;
• основы экономики, организации труда и управления;
• основы трудового законодательства;
• правила и нормы охраны труда и пожарной безопасности и т.д.

1.6. Администратор сетей подчиняется непосредственно начальнику структурного подразделения (непосредственно руководителю) _____ .

1.7. В случае временного отсутствия администратора сетей (отпуск, болезнь и пр.) его обязанности исполняет назначенный в установленном порядке заместитель, который приобретает соответствующие права и несет полную ответственность за качественное и своевременное исполнение возложенных не него обязанностей.

2. Функции. На администратора сетей возлагаются следующие функ ции.

2.1. Оперативно-техническое руководство и обеспечение бесперебойного функционирования локальной вычислительной сети.

2.2.' Контроль за техническим состоянием технических средств вычислительной сети.

2.3. Выявление и устранение сбоев в работе сети.

2.4. Обеспечение взаимодействия с другими сетями передачи данных.

2.5. Методическое обеспечение соответствующих вопросов и др.

3. Должностные обязанности. Для выполнения возложенных на него функций администратор сетей осуществляет следующие обязанности.

3.1. Организует и обеспечивает бесперебойное функционирование локальной вычислительной сети.

3.2. Устанавливает на серверы и рабочие станции сетевой программное обеспечение, конфигурирует систему на сервере.

3.3. Обеспечивает интегрирование программного обеспечения на файл-серверах, серверах систем управления базами данных и на рабочих станциях.

3.4. Поддерживает рабочее состояние программного обеспечений сервера.

3.5. Обеспечивает защиту от несанкционированного доступа к информации, просмотра или изменения системных файлов и данных, а также безопасность межсетевого взаимодействия.

3.6. Организует доступ к локальным и глобальным сетям, в том числе в сеть Интернет; обмен информацией с другими организациями с использованием электронной почты.

3.7. Регистрирует пользователей, назначает идентификаторы и пароли.

3.8. Проводит обучение и консультирование пользователей при работе в локальной вычислительной сети, сети Интернет, использовании электронной почты, ведению архивов.

3.9. Разрабатывает инструкции по работе с сетевым программным обеспечением и обеспечивает ими пользователей.

3.10. Устанавливает ограничение для пользователей по использова нию рабочей станции или сервера; времени; степени использования ре сурсов.

3.11. Составляет график архивации данных.

3.12. Ведет журнал архивации данных и степени использования носителей.

3.13. Разрабатывает схему послеаварийного восстановления работоспособности локальной вычислительной сети.

3.14. Проводит тестовые проверки и профилактические осмотры вычислительной техники с целью своевременного обнаружения и ликвидации неисправностей.

3.15. Составляет заявки на ремонт неисправного, а также приобретение нового и модернизацию устаревшего сетевого оборудования.

3.16. Осуществляет контроль за монтажом оборудования специалистами сторонних организаций и др.

4. Права. Администратор сетей имеет право:

• знакомиться с проектами решений руководства организаций, касающихся его деятельности;

• вносить на рассмотрение руководства предложения по совершенствованию работы, связанной с предусмотренными настоящей инструкцией обязанностями;

• запрашивать и получать от специалистов подразделений информацию и документы, необходимые для выполнения своих должностных обязанностей;

• устанавливать и изменять правила пользования сетей;

• сообщать своему непосредственному руководителю о всех выявленных в процессе осуществления должностных обязанностей недостатках в деятельности организации (ее структурных подразделениях) и вносить предложения по их устранению в пределах своей компетенции;

• привлекать специалистов соответствующих структурных подразделений к выполнению возложенных на него функций в случае, если это предусмотрено положениями о структурных подразделениях, в противном случае — с разрешения руководства организации;

• требовать от своего непосредственного руководителя, руководства организации оказания содействия в осуществлении им своих должностных обязанностей и прав и др.

5. Ответственность. Администратор несет ответственность:

• за ненадлежащее исполнение (неисполнение) своих должностных обязанностей, за неправильность и неполноту использования предоставленных прав, предусмотренных настоящей должностной инструкцией, в пределах, определенных действующим трудовым законодательством;

• за правонарушение, совершенное в процессе осуществления своей деятельности, в пределах, определенных действующим законодательством, уголовным и гражданским законодательствами;

• за причинение материального ущерба в пределах, определенных действующими трудовым и гражданским законодательствами.

СПИСОК ЛИТЕРАТУРЫ

1. Администрирование сети на основе Microsoft Windows 2000. Учебный курс MCSE : пер. с англ. — 2-е изд., перераб. — М. : Русская редакция, 2001.

2. *Андерсон К.* Локальные сети. Полное руководство : пер. с англ. / К.Андерсон, М. Минаси. - К.: ВЕК+ ; М.: ЭНТРОП ; СПб.: КОРОНАпринт, 1999.

3. *Анин Б. Ю.* Защита компьютерной информации / Б. Ю. Анин. — СПб.: БХВ-Петербург, 2000.

4. *Вишневский А.* Сетевые технологии Windows 2000 для профессионалов / А. Вишневский. — СПб. : Питер, 2000.

5. Компьютерные системы и сети : учеб. пособие / [В. П. Косарев и др.]; под ред. В. П. Косарева и Л. В. Еремина. — М.: Финансы и статистика, 3999.

6. Компьютерные технологии обработки информации : учеб. пособие / [С.В.Назаров, В.Ф.Першиков, В.А.Тафинцев и др.] ; под ред. С.В.Назарова. — М. : Финансы и статистика, 1995.

7. *Корнеев И. К.* Информационные технологии в управлении : учеб. пособие / И. К. Корнеев, Т. А. Година. — М. : Финстатинформ, 1999.

8. *Крутое СВ.* Защита в операционных системах / С.В.Крутов, И.В.Мацкевич, В.Г.Проскурин. — М. : Радио и связь, 2000.

9. *Лепаж И.* Unix. Библия пользователя : пер. с англ. / Ив Лепаж, Пол Яррера. — 2-е изд. — М. : Изд. дом «Вильяме», 2001.

10. *Мельников В. П.* Информационная безопасность и защита информации : учеб. пособие / В.П.Мельников, С.А.Клейменов, А.М.Петраков ; под ред. С. А. Клейменова. — М.: Изд. центр «Академия», 2006.

11. *Милославская Н.Г.* Интрасети : доступ в Internet, защита : учеб. пособие / Н. Г. Милославская. — М.: ЮНИТИ, 1999.

12. *Назаров СВ.* Администрирование локальных сетей Windows NT/ 2000/NET: учеб. пособие / С. В. Назаров. — 2-е изд., перераб. и доп. — М.: Финансы и статистика, 2003.

13. *Новиков Ю.* Локальные сети : архитектура, алгоритмы, проектирование / Ю. Новиков. - М. : ЭКОМ, 2000.

14. *Ногл М.* TCP/IP. Иллюстрированный учебник / М. Ногл. — М. : ДМК Пресс, 2001.

15. Обеспечение информационной безопасности машиностроительных предприятий : учебник. Кн. 1 и 2 / под ред. В. П. Мельникова. — М.: Сатурн-С, 2006.

16. *Олифер В. Г.* Компьютерные сети. Принципы, технологии, протоколы : учебник/ В.Г.Олифер, Н.А.Олифер. — 2-е изд. — СПб. : Питер-пресс, 2002.

17. *Олифер В. Г.* Новые технологии и оборудование IP-сетей / В. Г. Оли-фер, Н. А. Олифер. — СПб. : БХВ - Санкт-Петербург, 2000.

18. *Прокофьев Н.* Типовые задачи администрирования сети Windows 2000 / Н. Прокофьев // КомпьютерПресс. — 2001. - № 12. - С. 134-137.

19. Ресурсы Windows NT : пер. с англ. — СПб.: BHV — Санкт-Петербург, 1995.

20. Технологии корпоративных сетей. Энциклопедия. — СПб.: Питер, 1999.

21. *Хоффман П.* Internet / П. Хоффман. — К. : Диалектика, 2001.

22. Microsoft Windows 2000 Server. Русская версия / [А.Г.Андреев, Е.Ю.Беззубов, М.М.Емельянов и др.] ; под ред. А.Н.Чекмарева и Д.Б.Вишнякова. — СПб.: БХВ — Санкт-Петербург, 2001.

23. Unix : руководство системного администратора. Для профессиона лов / [Э. Немет, Г.Снайдер, С.Сибасс, Т.Хейн]. — 3-е изд. — СПб. : Пи тер ; К. : Изд. группа BHV, 2005.

ОГЛАВЛЕНИЕ

Учебное издание

Клейменов Сергей Анатольевич,
Мельников Владимир Павлович,
Петраков Александр Михайлович

Администрирование в информационных системах

Учебное пособие

Редактор *О. А. Туваева*
Технический редактор *О. Н. Крайнова*
Компьютерная верстка: *О. В. Пешкешова*
Корректоры *Н. Т.Захарова, Н.Л.Котелина*

Изд. № 101114050. Подписано в печать 17.03.2008. Формат 60x90/16.
Гарнитура «Тайме». Печать офсетная. Бумага офсетная № 1. Усл. печ.
л. 17,0. Тираж 3 000 экз. Заказ № 26250.

Издательский центр «Академия», www.academia-moscow.ru
Санитарно-эпидемиологическое заключение № 77.99.02.953.Д.004796.07.04 от 20.07.2004.
117342, Москва, ул. Бутлерова, 17-Б, к. 360. Тел./факс: (495) 330-1092, 334-8337.

Отпечатано в полном соответствии с качеством диапозитивов, предоставленных
издательством в ОАО «Саратовский полиграфкомбинат». 410004, г. Саратов, ул.
Чернышевского, 59. www.sarpk.ru.