МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ИНСТИТУТ ТЕХНОЛОГИЙ (ФИЛИАЛ) ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ» В Г. ВОЛГОДОНСКЕ РОСТОВСКОЙ ОБЛАСТИ

(Институт технологий (филиал) ДГТУ в г. Волгодонске)

АДМИНИСТРИРОВАНИЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Учебно-методическое пособие
для студентов направления
09.03.02 Информационные системы и технологии

Волгодонск,

2021

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Совместная работа в любой сфере человеческой деятельности предполагает использование некого набора правил, позволяющего избежать различных нештатных ситуаций, недопонимания, обеспечить эффективное взаимодействие между работающими вместе сотрудниками и параметры производственного процесса.

Увеличивающаяся степень информатизации современного общества требует использования на предприятиях различных информационных систем (ИС), строящихся, как правило, на базе информационно-вычислительных компьютерных сетей различного масштаба.

Если использование небольшой группы автономных компьютеров требует самой минимальной регламентации, то объединение их в сеть приводит к необходимости создания более развернутого и жесткого набора правил. А коль скоро правила созданы, необходимо следить за их выполнением, что и является одной из основных целей администрирования.

Качественный состав задач администрирования и их приоритеты изменяются с ростом системы, изменением ее функциональности. Так, например, небольшой сетью из 10–15 машин, не подключенной к Интернету, вполне может управлять один администратор, совмещая эти обязанности с обязанностями прикладного программиста. При этом, как правило, большинство настроек устанавливается по умолчанию и от администратора не требуется знания многих тонкостей.

Дальнейший рост системы требует выделения администратора как отдельной штатной единицы, причем не только из-за возрастающего объема рутинной работы (работа с бюджетами пользователей, архивирование данных, организация поддержки сетевой печати и т.п.), но и из-за появления принципиально новых задач.

При достижении некоторого критического порога возникает необходимость в дифференциации функций управления и разделения их между несколькими сотрудниками, т.е. создания группы администрирования.

В настоящее время в связи с интеграцией корпоративных сетей передачи данных все более остро встает проблема управления распределенными гетерогенными сетями, состоящими из множества локальных сетей, функционирующих на основе различных стандартов и протоколов.

Создание системы интегрированного сетевого управления требует решения целого ряда задач. В их число входят:

- традиционные задачи сетевого управления (управление конфигурацией, управление производительностью, управление сбоями, управление безопасностью, учет использования ресурсов);
- управление распределенными приложениями в гетерогенных сетях;

- мониторинг текущего состояния системно-технического обеспечения организации (ведение визуализированной базы данных, содержащей полную информацию как о технических, так и об учетных параметрах всего технического и программного обеспечения, имеющегося в той или иной организации);
- поддержка принятия решений по модернизации технического и программного обеспечения с учетом текущего состояния технического прогресса, информации о производителях и поставщиках технических и программных средств и о сравнительных характеристиках этих продуктов;
- управление модернизацией (контроль и управление установкой нового технического и программного обеспечения, включая оптимизацию этого процесса);
- моделирование работы существующих сетей (включая анализ нагрузок на отдельные их участки и поддержку принятия решений по перепланированию).

Следует заметить, что ни один из имеющихся на сегодняшний день на рынке программного обеспечения продуктов не решает целиком ни одной из перечисленных задач. Поэтому наиболее целесообразным решением в данном случае является либо разработка такой интегрированной системы самостоятельно, либо заказ на её разработку фирме-системному интегратору.

Организация управления большими системами остается одной из немногих областей, где невозможно предложить полностью готовые решения; здесь всегда необходим творческий подход и учет всех уникальных особенностей конкретной системы. Создавать систему администрирования своими силами, привлекать специализированную фирму или вообще поручить эту задачу сторонней организации – в каждом конкретном случае решает руководство компании, но необходимые исходные данные и экономические выкладки должны предоставлять специалисты в области информационных технологий.

В данном учебно-методическом пособии рассмотрены ключевые аспекты администрирования информационных систем применительно к информационно-вычислительным компьютерным сетям различного масштаба.

1. ОСНОВЫ АДМИНИСТРИРОВАНИЯ И УПРАВЛЕНИЯ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

1.1. Основные понятия

В общем случае под *администрированием* понимают управление программно-аппаратными ресурсами информационной системы с целью достижения максимальной производительности, удобства использования, обеспечения бесперебойной работы, сохранности и защиты информации. Рассмотрим основные понятия данной предметной области.

Информационная система – инженерное изделие, спроектированное на системной основе, представляющее собой совокупность программных и технических средств, а также реализованного банка данных (банка знаний), позволяющих с помощью специально разработанных в рамках системы методов, методик и нормативных ограничений (стандартов) эффективно в интересах и по запросам пользователя автоматически и однозначно поддерживать сбор, поиск, распознавание, получение, хранение, защиту, обработку, передачу и представление информации.

Жизненный цикл ИС – непрерывный процесс функционирования ИС с момента принятия решения о создании ИС до изъятия из эксплуатации. Существует международный стандарт, регламентирующий жизненный цикл ИС: ISO/IEC 12207. Выделяют следующие основные процессы жизненного цикла ИС.

Разработка – включает в себя стратегическое планирование, анализ, проектирование и реализацию (программирование), работы по созданию информационного программного обеспечения, оформление проектной и эксплуатационной документации, подготовка материалов для тестирования программных продуктов, разработка обучающих документов и программ для персонала.

Эксплуатация – включает подготовительную и основную стадии.

Подготовительная стадия содержит:

1) конфигурирование базы данных и рабочих мест пользователей;
2) обеспечение пользователей эксплуатационной документацией;
3) обучение персонала.

Основная стадия включает:

1) непосредственно эксплуатацию;
2) локализацию проблем и устранение причин их возникновения;
3) модификацию программного обеспечения;
4) совершенствование, развитие и модернизацию системы.

Сопровождение ИС. Наличие квалифицированного технического обслуживания (ТО) на этапе эксплуатации ИС является необходимым условием для решения поставленных перед ней задач, причём ошибки об-

служивания могут приводить к скрытым или явным финансовым потерям, сравнимым со стоимостью самой ИС. Можно выделить следующие основные задачи организации технического обслуживания ИС:

1) выделение наиболее ответственных узлов системы и критичности их простоя;
2) определение задач технического обслуживания и их разделение на внутренние (решаемые обслуживающим персоналом) и внешние (решаемые специализированным сервисом). Таким образом, чётко определяется круг исполняемых функций и разделяется ответственность;
3) проведение анализа имеющихся внутренних и внешних ресурсов для ТО по следующим критериям: наличие гарантии на оборудование, состояние ремонтного фонда, квалификация персонала;
4) подготовка плана проведения ТО, определение этапов проведения, сроков выполнения, затрат, ответственности исполнителей.

Информационно-вычислительная сеть (ИВС) – комплекс программно-аппаратных средств для обеспечения автоматизации производства и других сфер жизнедеятельности человека, включающий в качестве составной части кабельное и сетеобразующее оборудование.

Администратор ИВС (Administrator) – должностное лицо, ответственное за работоспособность и надлежащее функционирование всех частей ИВС. У администратора крупных ИВС могут находиться в подчинении администраторы частей и подсистем ИВС – например, администратор ЛВС, администратор сетевой операционной системы, администратор баз данных, а также технический персонал. Администратор подсистемы ИВС отвечает за работоспособность и надлежащее функционирование вверенных ему компонентов этой подсистемы ИВС.

Пользователь ИВС (User) – физическое лицо, имеющее доступ к определённым ресурсам ИВС, идентифицируемое учётной записью пользователя. Администратор ИВС также является пользователем ИВС, обладая в общем случае неограниченным доступом ко всем ресурсам ИВС.

Учётная запись пользователя (Account) – запись в специализированной базе данных (БД учётных записей), содержащая информацию о пользователе ИВС в виде набора уникальных реквизитов. Используется для идентификации пользователя в системе, проверки полномочий пользователя и обеспечения доступа к тем или иным ресурсам системы. Характеризуется атрибутами: имя для входа, пароль, профиль в системе, список принадлежности к группам и т.д. Пароль служит для защиты учётной записи от несанкционированного использования.

Регистрация пользователя в системе (Registration) – создание администратором (или другим уполномоченным лицом) учётной записи для данного физического лица.

Аутентификация в системе (Authentication) – процесс установления подлинности пользователя ИВС. Заключается в предъявлении пользователем своего имени для входа и пароля, а также в проверке системой наличия в БД учётных записей данной учётной записи и соответствия указанных пользователем атрибутов с хранящимися в БД. После успешной аутентификации в системе для пользователя на время сеанса работы создаётся маркер безопасности, отражающий его цифровой идентификатор в системе, а также его принадлежность группам пользователей, профилям и другим объектам системы безопасности.

Ресурсы ИВС (Resurses) – физические и логические объекты ИВС, имеющие определённую функциональность, доступную для использования. Примеры физических ресурсов – сервер ЛВС, каталог совместного использования на сервере, сетевой принтер; логических ресурсов – пользователь, группа пользователей, профиль в системе, очередь на печать и т.п.

Права доступа к ресурсу (Access rights to the resourse) – степень свободы действий пользователя (просмотр, использование, владение) по отношению к данному ресурсу.

Назначение прав доступа к ресурсу (User's rights assignment) – процедура создания в системе специальной записи, с помощью которой учётной записи пользователя или её аналогу (группе пользователей) присваиваются определённые права доступа к ресурсу. Назначение прав доступа в современных ИВС осуществляется через списки управления доступом (Acces control List/ACL).

Список управления доступом (Acces control List/ACL) – в виде отдельных записей хранит информацию о том, кто обладает правами на ресурс и каковы эти права. Например, для одного пользователя в ACL каталоге файловой системы могу быть указаны права на чтение, а для другого пользователя – права на чтение и запись.

Авторизация/Проверка прав доступа (Authorization/Rights verification) – процесс установления системой соответствия запрошенных прав доступа к ресурсу и фактических прав пользователя на ресурс и формирование управляемой реакции: разрешить или отвергнуть доступ пользователя к ресурсу. Например, пользователь выполняет операцию открытия файла на запись (запрашиваемые права), обладая при этом только правом просмотра (фактические права). Система запретит выполнение операции, мотивируя своё поведение недостатком прав у пользователя.

Аудит/контроль использования ресурсов (Audit) – процесс контроля использования ресурсов, включающий возможность ведения журнала попыток доступа к ресурсам. Журнал аудита ведётся на основе данных, поступающих от процедур авторизации.

Совместное использование ресурса (Resource sharing) – использование ресурса двумя и более пользователями ИВС.

1.2. Функциональные области администрирования информационных систем

Рассмотрим основные аспекты администрирования крупных информационных систем.

Первый (и самый очевидный) аспект администрирования – это *работа с пользователями*. Сюда входит создание и удаление пользовательских бюджетов (учетных записей), их блокировка и разблокирование, настройка сценариев входа, консультирование пользователей по различным аспектам работы с системой и нахождению тех или иных ресурсов. Здесь главное – найти разумную грань, чтобы администратор не был ответствен за смену картриджа в локальном принтере пользователя – это все-таки задача службы технической поддержки. Более того, во многих компаниях на службу технической поддержки возлагают обязанности по установке и настройке сетевого клиентского программного обеспечения на компьютерах пользователей.

Процесс создания и удаления пользователей можно автоматизировать, но некоторые решения, от которых зависит включение нового пользователя, должен принимать администратор.

Другая не менее важная задача – это *управление данными*. Предоставление пользователям прав на доступ к конкретным ресурсам, профилактическое обслуживание баз данных (индексация, оптимизация, упаковка), организация резервного копирования.

Процедура резервного копирования довольно утомительна и отнимает много времени, но выполнять ее необходимо. Ее можно автоматизировать, но системный администратор обязан убедиться в том, что резервное копирование выполнено правильно и в соответствии с графиком. Практически любая сетевая операционная система содержит механизмы для создания резервных копий или зеркального ведения дисков. Например, в UNIX-системах самое распространенное средство создания резервных копий и восстановления данных – команды *dump* и *restore*. В большинстве случаев информация, хранящаяся в компьютерах, стоит дороже самих компьютеров. Кроме того, ее гораздо труднее восстановить.

Существуют сотни весьма изобретательных способов потерять информацию. Ошибки в программном обеспечении зачастую портят файлы данных. Пользователи случайно удаляют то, над чем работали всю жизнь. Хакеры и раздраженные служащие стирают данные целыми дисками. Проблемы с аппаратными средствами и стихийные бедствия выводят из строя целые машинные залы. Поэтому ни одну систему нельзя эксплуатировать без резервных копий.

При правильном подходе создание резервных копий данных позволяет администратору восстанавливать файловую систему (или любую ее часть) в том состоянии, в котором она находилась на момент последнего снятия резервных копий. Резервное копирование должно производиться тщательно и строго по графику.

Поскольку многие виды неисправностей способны одновременно выводить из строя сразу несколько аппаратных средств, резервные копии следует записывать на съемные носители, CD-диски, ZIP-дискеты и т.д. Например, копирование содержимого одного диска на другой, конечно, лучше, чем ничего, но оно обеспечивает весьма незначительный уровень защиты от отказа контроллера.

Анализ производительности и оптимизация системы. Большинство систем имеют оптимальные настройки «по умолчанию» и не требуют особого вмешательства. Однако узкие места все же могут возникать. Производители известных сетевых операционных систем на основе богатого опыта эксплуатации выводят наборы эмпирических правил, помогающих администратору вносить изменения в настройки с минимальным риском, ухудшить другие показатели или сделать систему неработоспособной. Такие рекомендации имеются, в частности, у фирм Novell и Sun Microsystems, администратору остается только их изучить и знать перечень параметров, которые необходимо контролировать. Многих проблем можно избежать еще на стадии планирования сети. В частности, неправильный выбор типов кадров Ethernet и их соотношения может привести к резкому снижению производительности или нарушению работы системы при отключении одного из компонентов.

С предыдущей задачей связана задача *учета системных ресурсов*. Учет ресурсов позволяет заметить тенденции к появлению узких мест до того, как появятся проблемы с производительностью, и провести соответствующую модернизацию. Кроме того, система учета совершенно необходима при платном использовании ресурсов. Сюда относится контроль использования дискового пространства, печати, учет трафика.

Техническое обслуживание и модернизация. Если собственно техническое обслуживание (очистка от пыли, смазка вентиляторов, подтяжка креплений, контроль состояния аккумуляторов, изменение физической топологии сети и т.п.) может осуществляться службой технической поддержки, то грамотное формулирование заявок на изменение аппаратной конфигурации, организация закупки дополнительных лицензий или обновленной версии программного обеспечения – задача администратора.

Для того чтобы принять правильное решение о модернизации системы, системному администратору необходимо проанализировать производительность системы. Конечными узлами сети являются компьютеры, и от их производительности и надежности во многом зависят характеристики всей сети в целом. Именно компьютеры являются теми устройствами в сети, которые реализуют протоколы *всех уровней*, начиная от физического и канального (сетевой адаптер и драйвер) и заканчивая прикладным уровнем (приложения и сетевые службы операционной системы). Следовательно, оптимизация компьютера включает две достаточно независимые задачи.

Во-первых, выбор таких параметров конфигурации программного и аппаратного обеспечения, которые гарантировали бы оптимальные показатели производительности и надежности этого компьютера как отдельного элемента сети. Такими параметрами являются, например, тип используемого сетевого адаптера, размер файлового кэша, влияющий на скорость доступа к данным на сервере, производительность дисков и дискового контроллера, быстродействие центрального процессора и т.п.

Во-вторых, выбор таких параметров протоколов, установленных в данном компьютере, которые гарантировали бы эффективную и надежную работу коммуникационных средств сети. Поскольку компьютеры порождают большую часть кадров и пакетов, циркулирующих в сети, то многие важные параметры протоколов формируются программным обеспечением компьютеров, например начальное значение поля TTL (Time-to-Live) протокола IP, размер окна неподтвержденных пакетов, размеры используемых кадров.

Тем не менее, выполнение вычислительной задачи может потребовать участия в работе нескольких устройств. Каждое устройство использует определенные ресурсы для выполнения своей части работы. Плохая производительность обычно является следствием того, что одно из устройств требует намного больше ресурсов, чем остальные. Чтобы исправить положение, необходимо выявить устройство, которое расходует максимальную часть времени при выполнении задачи. Такое устройство называется у*зким местом (bottleneck).* Например, если на выполнение задачи требуется 3 секунды и 1 секунда тратится на выполнение программы процессором, а 2 секунды на чтение данных с диска, то диск является узким местом.

Определение узкого места – критический этап в процессе улучшения производительности. Замена процессора в предыдущем примере на другой, в два раза более быстродействующий процессор, уменьшит общее время выполнения задачи только до 2,5 секунд, но принципиально исправить ситуацию не сможет, поскольку узкое место устранено не будет. Если же мы приобретем диск и контроллер диска, которые будут в два раза быстрее прежних, то общее время уменьшится до 2 секунд.

Если администратор всерьез недоволен быстродействием системы, исправить положение можно следующими способами:

- обеспечив систему достаточным ресурсом памяти. Объем памяти – один из основных факторов, влияющих на производительность;
- устранив некоторые проблемы, созданные как пользователями (одновременный запуск слишком большого количества заданий, неэффективные методы программирования, выполнение заданий с избыточным приоритетом, а также объемных заданий в часы пик), так и самой системой (квоты, учет времени центрального процессора);

- организовав жесткие диски и файловые системы так, чтобы сбалансировать нагрузку на них и таким образом максимально повысить пропускную способность средств ввода-вывода;
- осуществляя текущий контроль сети, чтобы избежать ее перегрузки и добиться низкого коэффициента ошибок. Сети UNIX/Linux можно контролировать с помощью программы *netstat*. Если речь идет о сетевых операционных системах семейства Windows, то поможет утилита *Performance Monitor*;
- откорректировав методику компоновки файловых систем в расчете на отдельные диски;
- выявив ситуации, когда система совершенно не соответствует предъявляемым к ней требованиям.

Эти меры перечислены в порядке убывания эффективности.

Инсталляция новых программных средств. После приобретения нового программного обеспечения его нужно инсталлировать и протестировать. Если программы работают нормально, необходимо сообщить пользователям об их наличии и местонахождении.

Как правило, самой ответственной и самой сложной задачей системного администратора являются инсталляция и конфигурирование операционной системы (ОС). Во многих современных операционных системах разработчики идут по пути исключения многих непродуктивных параметров системы, с помощью которых администраторы способны влиять на производительность ОС. Вместо этого в операционную систему встраиваются адаптивные алгоритмы, которые определяют рациональные параметры системы во время ее работы. С помощью этих алгоритмов ОС может динамически оптимизировать свои параметры в отношении многих известных сетевых проблем, автоматически перераспределяя свои ресурсы и не привлекая к решению администратора.

Существуют различные критерии оптимизации производительности операционной системы. К числу наиболее распространенных критериев относятся:

- наибольшая скорость выполнения определенного процесса;
- максимальное число задач, выполняемых процессором за единицу времени. Эта характеристика также называется пропускной способностью компьютера. Она определяет качество разделения ресурсов между несколькими одновременно выполняемыми процессами;
- освобождение максимального количества оперативной памяти для самых приоритетных процессов, например процесса, выполняющего функции файлового сервера, или же для увеличения размера файлового кэша;
- освобождение наибольшего количества дисковой памяти.

Обычно при оптимизации производительности ОС администратор начинает этот процесс при заданном наборе ресурсов. В общем случае одновременно улучшить все критерии производительности невозможно. Например, если целью является увеличение доступной оперативной памяти, то администратор может увеличить размер страничного файла, но это приведет к уменьшению доступного дискового пространства.

После инсталляции и оптимальной настройки операционной системы начинается практически бесконечный процесс установки программного обеспечения. И здесь на первый план выходят проблемы совместимости различных программ, а если устанавливается серверное программное обеспечение – то еще и о безопасности.

Очень часто как отдельную функцию выделяют *задачу управления аппаратным обеспечением, активным сетевым оборудованием* и сетью в целом.

Для корректной работы устройств в сети требуется их правильно инсталлировать и установить рабочие параметры.

В случае приобретения новых аппаратных средств или подключения уже имеющихся аппаратных средств к другой машине 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 (подключение нового диска).

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.

Концентраторы и коммутаторы редко являются источником проблем, однако одной из наиболее распространенных проблем такого рода является отсутствие питания. Иногда неисправный сетевой адаптер может нарушить работу порта в концентраторе. Для проверки адаптера необходимо пользоваться диагностическими программами из комплекта адаптера.

Немаловажным компонентом администрирования системы является *обеспечение информационной безопасности*. Особенностью любой сетевой системы является то, что ее компоненты распределены в пространстве, а связь между ними осуществляется физически – при помощи сетевых соединений (коаксиальный кабель, витая пара, оптоволокно и т.д.) и программно – при помощи механизма сообщений. К сетевым системам наряду с *обычными* (локальными) атаками, осуществляемыми в пределах одной операционной системы, применим специфический вид атак, обусловленный распределенностью ресурсов и информации в пространстве, – так называемые сетевые (или удаленные) атаки. Они характеризуются тем, что,

во-первых, злоумышленник может находиться за тысячи километров от атакуемого объекта, а во-вторых, нападению может подвергнуться не конкретный компьютер, а информация, передающаяся по сетевым соединениям.

Системный администратор должен реализовывать стратегию защиты и периодически проверять, не нарушена ли защита системы.

Естественно, абсолютная защита сети невозможна, однако задача каждого администратора – сделать все возможное для максимального ее улучшения. При построении системы защиты разумно придерживаться следующих принципов:

- актуальность. Защищаться следует от реальных атак, а не от фантастических или же архаичных;
- разумность затрат. Поскольку 100 % защиты все равно не обеспечить, необходимо найти тот рубеж, за которым дальнейшие траты на повышение безопасности превысят стоимость той информации, которую может украсть злоумышленник.

Очень часто сотрудники предприятия оказываются самым слабым звеном в системе его безопасности, поэтому системному администратору следует уделять больше внимания работе с пользователями системы. Иначе простой листочек бумаги с паролем, лежащий на рабочем месте забывчивой сотрудницы, сделает бесполезной выверенную настройку межсетевого экрана.

Для усиления безопасности компьютерных систем компании разумными могут считаться следующие шаги:

- привлечение внимания людей к вопросам безопасности;
- осознание сотрудниками всей серьезности проблемы и принятие в организации политики безопасности;
- изучение и внедрение необходимых методов и действий для повышения защиты информационного обеспечения.

Сюда же входит составление плана доступа пользователей к ресурсам (в соответствии с принятой в компании политикой информационной безопасности) и контроль его исполнения. К функциям обеспечения безопасности относятся также отслеживание появления различных уязвимостей в используемых операционных системах, организация получения и установки «заплаток» (patches).

Требуется создать и разработать различные варианты политики безопасности, определить правила корректного использования телефонов компьютеров и другой техники. Необходимо учитывать и неосведомленность в области безопасности, поскольку любые средства технического контроля могут быть использованы ненадлежащим образом.

И последняя (по порядку изложения, но не по значимости) задача – это *задача аудита*, данные которого используются почти всеми приведенными выше задачами.

Существует великое 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 и за наличием системных ресурсов.

Системный администратор должен документировать все инсталлируемые программные средства, не входящие в стандартный пакет поставки, документировать разводку кабелей, вести записи по обслуживанию всех аппаратных средств, регистрировать состояние резервных копий и документировать правила работы с системой.

Также следует учитывать, что система учета, ядро, различные утилиты – все эти программы выдают данные, которые регистрируются и, в конце концов, попадают на ваши диски. Эти данные тоже являются локальной документацией, характеризующей работу конкретной системы. Однако срок полезной службы большинства данных ограничен, поэтому их нужно обобщать, упаковывать и, наконец, выбрасывать.

Процедура ведения файлов регистрации в любой операционной системе представляет собой набор процедур, которые повторяются через определенное время в одном и том же порядке. Следовательно, ее необходимо автоматизировать.

В UNIX-системах для этой цели используется процесс *cron*, а программа *syslog* может удачно применяться в качестве полной системы регистрации. Она отличается высокой гибкостью и позволяет сортировать сообщения системы по источникам и степени важности, а затем направлять их в разные пункты назначения: в файлы регистрации, на терминалы пользователей и даже на другие машины. Одной из самых ценных особенностей этой системы является ее способность централизовать регистрацию для сети.

Администраторы Windows 2003 могут для тех же целей использовать утилиту *Performance Monitor*, разработанную для фиксации активности компьютера в реальном масштабе времени. С ее помощью можно определить большую часть узких мест, снижающих производительность. *Performance Monitor* основан на ряде счетчиков, которые фиксируют такие характеристики, как число процессов, ожидающих завершения операции с диском, число сетевых пакетов, передаваемых в единицу времени, процент использования процессора и др.

Performance Monitor генерирует полезную информацию посредством следующих действий:

- наблюдения за производительностью в реальном времени и в исторической перспективе;
- определения тенденций во времени;
- определения узких мест;
- отслеживания последствий изменения конфигурации системы;

- наблюдения за локальным или удаленными компьютерами;
- предупреждения администратора о событиях, связанных с превышением некоторыми характеристиками заданных порогов.

С целью обеспечения непротиворечивости получаемой информации доступ к подсистеме аудита должен быть ограничен. Причем лицо, ответственное за подсистему аудита, не должно иметь административных полномочий по управлению системой и данным, по которым аудит ведется. Такое разделение позволит существенно повысить уровень безопасности: если человек знает, что его действия протоколируются, то он воздержится от попыток совершения каких-либо манипуляций с информацией во вред компании. По этой же причине он оказывается защищенным от давления со стороны третьих лиц совершить нечто противоправное.

Итак, на основе изложенного можно выделить пять категорий административного персонала, обеспечивающего эксплуатацию информационной системы:

Администратор 1. Оптимизация настроек. Мониторинг производительности. Модернизация. Техническое обслуживание и профилактика. Организация резервного копирования.

Администратор 2. Регистрация новых пользователей. Отслеживание изменения статуса пользователей (ведение и хранение учетных карт). Консультация пользователей. Смена и восстановление пароля, решение других проблем.

Администратор 3. Организация размещения данных. Назначение/изменение прав доступа. Планирование резервного копирования и хранение резервных копий. Восстановление данных (совместно с администратором 1).

Администратор безопасности системы. Участие в разработке матрицы доступа к ресурсам. Контроль за соблюдением политики безопасности при эксплуатации. Отслеживание информации об уязвимостях системы и своевременное принятие мер. Периодическое практическое тестирование защищенности системы.

Аудитор. Настройка подсистемы регистрации. Организация архивирования и хранения журналов регистрации. Анализ журналов регистрации.

Следует сказать несколько слов об организации процесса администрирования ИС.

Во-первых, все аспекты деятельности всех администраторов должны быть обеспечены нормативными и методическими документами. Это защитит как интересы руководства компании, так и администраторов. Кроме того, как показывает опыт, наличие типовых инструкций позволяет четче действовать в нестандартных ситуациях. Состав пакета нормативных документов может быть примерно следующим:

1) положение о локальной сети компании;
2) инструкция администратору серверов;
3) инструкция администратору баз данных;

4) инструкция пользователю;
5) инструкция администратору информационной безопасности;
6) инструкция аудитору;
7) процедура оформления доступа к ресурсам;
8) инструкция по резервному копированию и восстановлению информации;
9) инструкция по антивирусной безопасности;
10) инструкция о парольной защите.

Как правило, непосредственно процесс администрирования должен осуществляться со специальных административных станций, выделенных в логический (или физический) сегмент. Такой подход решит многие проблемы с безопасностью: перехват парольной и другой важной управляющей информации при передаче ее по сети или вводе с клавиатуры, заражение вирусами. В зависимости от потенциальных возможностей администратора и ценности циркулирующей в системе информации, станции администрирования могут быть размещены в защищенной зоне и снабжаться дополнительными средствами защиты.

Конкретный выбор распределения обязанностей в плане допустимого и недопустимого совмещения функций осуществляется руководством компании. Здесь очень важно не ошибиться, так как слишком большое сосредоточение полномочий может нанести вред компании (обидевшись на низкую зарплату, администратор может разрушить систему) и самому администратору (на него могут оказать давление злоумышленники), а недостаток прав и их сильное распыление могут привести к недопустимым задержкам при выходе из нестандартных ситуаций.

При распределении обязанностей следует учитывать психологический аспект, особенно для администраторов, непосредственно контактирующих с пользователями. Вежливо, но твердо проводить администрирование, не забывая при этом, что система построена не для оттачивания мастерства администратора, а ради той самой «прослойки между креслом и терминалом», называемой пользователем, под силу далеко не каждому профессионалу в области информационных технологий.

Вполне естественным желанием администратора является желание избавить себя от лишних забот, проведя максимальную автоматизацию рутинных процедур. Многие разрабатывают с этой целью небольшие утилиты и скрипты. Однако на рынке представлено достаточно большое количество специализированных средств, позволяющих перевести труд администраторов на качественно новый уровень и унифицировать управление разнородными системами. Это такие средства, как ManageWise, ZenWorks, HP OpenView, NetView (Tivoli) от IBM, Spectrum от Cabletron; Solstice от SunSoft, CA Unicenter от Computer Associates и др.

Кроме перечисленных интегрированных продуктов, существует множество решений от сравнительно небольших фирм, в которых реализованы отдельные функции, причем обычно далеко не в полном объеме. При

этом продукты третьих фирм не обладают средствами интеграции друг с другом и обычно не поддерживают разработку дополнительных модулей (add-on's) сторонними разработчиками, не имеют средств работы с внешними базами данных (Oracle, Informix, Ingres) и поддерживают ограниченный спектр сетевых устройств.

1.3. Пример типовой должностной инструкции сетевого администратора

1.3.1. Общие положения

Администратор сетей относится к категории специалистов. 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.

Администратор сетей назначается на должность и освобождается от нее приказом руководителя организации по представлению руководителя структурного подразделения (непосредственного руководителя).

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. Администратор сетей должен знать:

- нормативно-методические, организационно-распорядительные, дру- гие руководящие и нормативные документы вышестоящих и дру- гих органов, касающиеся методов программирования и использо- вания вычислительной техники при обработке информации и применения современных информационных технологий в вычис- лительных 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.

Администратор сетей подчиняется непосредственно начальнику структурного подразделения (непосредственно руководителю). 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.

1.3.2. Функции администратора сетей

На администратора сетей возлагаются следующие функции:

- оперативно-техническое руководство и обеспечение бесперебойного функционирования локальной вычислительной сети;
- контроль за техническим состоянием технических средств вычислительной сети;
- выявление и устранение сбоев в работе сети;
- обеспечение взаимодействия с другими сетями передачи данных;
- методическое обеспечение соответствующих вопросов.

1.3.3. Должностные обязанности

Для выполнения возложенных на него функций администратор сетей осуществляет следующие обязанности:

- организует и обеспечивает бесперебойное функционирование локальной вычислительной сети;
- устанавливает на серверы и рабочие станции сетевое программное обеспечение, конфигурирует систему на сервере;
- обеспечивает интегрирование программного обеспечения на файл-серверах, серверах систем управления базами данных и на рабочих станциях;
- поддерживает рабочее состояние программного обеспечения сервера;

- обеспечивает защиту от несанкционированного доступа к информации, просмотра или изменения системных файлов и данных, а также безопасность межсетевого взаимодействия;
- организует доступ к локальным и глобальным сетям, в том числе в сеть Интернет; обмен информацией с другими организациями с использованием электронной почты;
- регистрирует пользователей, назначает идентификаторы и пароли;
- проводит обучение и консультирование пользователей при работе в локальной вычислительной сети, сети Интернет, использовании электронной почты, ведению архивов;
- разрабатывает инструкции по работе с сетевым программным обеспечением и обеспечивает ими пользователей;
- устанавливает ограничение для пользователей: по использованию рабочей станции или сервера; времени; степени использования ресурсов;
- составляет график архивации данных;
- ведет журнал архивации данных и степени использования носителей;
- разрабатывает схему послеаварийного восстановления работоспособности локальной вычислительной сети;
- проводит тестовые проверки и профилактические осмотры вычислительной техники с целью своевременного обнаружения и ликвидации неисправностей;
- составляет заявки на ремонт неисправного, а также приобретение нового и модернизацию устаревшего сетевого оборудования;
- осуществляет контроль за монтажом оборудования специалистами сторонних организаций.

1.3.4. Права администратора сетей

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.

1.3.5. Ответственность администратора

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;
- правонарушение, совершенное в процессе осуществления своей деятельности, – в пределах, определенных действующим законодательством, уголовным и гражданским законодательствами;
- причинение материального ущерба – в пределах, определенных действующими трудовым и гражданским законодательствами.

2. СРЕДСТВА МОНИТОРИНГА, УПРАВЛЕНИЯ И АНАЛИЗА КОМПЬЮТЕРНЫХ СЕТЕЙ

2.1. Классификация средств мониторинга и анализа

Всё многообразие средств, применяемых для мониторинга и анализа вычислительных сетей, можно разделить на несколько крупных классов:

Системы управления сетью (Network Management Systems) – централизованные программные системы, которые собирают данные о состоянии узлов и коммуникационных устройств сети, а также данные о трафике, циркулирующем в сети. Эти системы не только осуществляют мониторинг и анализ сети, но и выполняют в автоматическом или полуавтоматическом режиме действия по управлению сетью – включение и отключение портов

устройств, изменение параметров мостов адресных таблиц мостов, коммутаторов и маршрутизаторов и т.п. Примерами систем управления могут служить популярные системы HP OpenView, SunNet Manager, IBM NetView.

Средства управления системой (System Management) часто выполняют функции, аналогичные функциям систем управления, но по отношению к другим объектам. В первом случае объектом управления является программное и аппаратное обеспечение компьютеров сети, а во втором – коммуникационное оборудование. Вместе с тем, некоторые функции этих двух видов систем управления могут дублироваться, например, средства управления системой могут выполнять простейший анализ сетевого трафика.

Встроенные системы диагностики и управления (Embedded systems). Эти системы выполняются в виде программно-аппаратных модулей, устанавливаемых в коммуникационное оборудование, а также в виде программных модулей, встроенных в операционные системы. Они выполняют функции диагностики и управления только одним устройством, и в этом их основное отличие от централизованных систем управления. Примером средств этого класса может служить модуль управления коммутатором Distrebuted 5000, реализующий функции автосегментации портов при обнаружении неисправностей, приписывания портов внутренним сегментам коммутатора и некоторые другие. Как правило, встроенные модули управления «по совместительству» выполняют роль SNMP-агентов, поставляющих данные о состоянии устройства для систем управления.

Анализаторы протоколов (Protocol analyzers). Представляют собой программные или аппаратно-программные системы, которые ограничиваются в отличие от систем управления лишь функциями мониторинга и анализа трафика в сетях. Хороший анализатор протоколов может захватывать и декодировать пакеты большого количества протоколов, применяемых в сетях – обычно несколько десятков. Анализаторы протоколов позволяют установить некоторые логические условия для захвата отдельных пакетов и выполняют полное декодирование захваченных пакетов, т.е. показывают в удобной для специалиста форме вложенность пакетов протоколов разных уровней друг в друга с расшифровкой содержания отдельных полей каждого пакета.

Оборудование для диагностики и сертификации кабельных систем. Условно это оборудование можно поделить на четыре основные группы: сетевые мониторы, приборы для сертификации кабельных систем, кабельные сканеры и тестеры (мультиметры).

Сетевые мониторы (называемые также *сетевыми анализаторами)* предназначены для тестирования кабелей различных категорий. Следует различать сетевые мониторы и анализаторы протоколов. Сетевые монито-

ры собирают данные только о статистических показателях трафика – средней интенсивности общего трафика сети, средней интенсивности потока пакетов с определенным типом ошибки и т.п.

Назначение *устройств для сертификации кабельных систем,* непосредственно следует из их названия. Сертификация выполняется в соответствии с требованиями одного из международных стандартов на кабельные системы.

Кабельные сканеры используются для диагностики медных кабельных систем.

Тестеры предназначены для проверки кабелей на отсутствие физического разрыва.

Экспертные системы. Этот вид систем аккумулирует человеческие знания о выявлении причин аномальной работы сетей и возможных способах приведения сети в работоспособное состояние. Экспертные системы часто реализуются в виде отдельных подсистем различных средств мониторинга и анализа сетей: систем управления сетями, анализаторов протоколов, сетевых анализаторов. Простейшим вариантом экспертной системы является контекстно-зависимая help-система. Более сложные экспертные системы представляют собой так называемые базы знаний, обладающие элементами искусственного интеллекта. Примером такой системы является экспертная система, встроенная в систему управления Spectrum компании Cabletron.

Многофункциональные устройства анализа и диагностики. В последние годы в связи с повсеместным распространением локальных сетей возникла необходимость разработки недорогих портативных приборов, совмещающих функции нескольких устройств: анализаторов протоколов, кабельных сканеров и даже некоторых возможностей ПО сетевого управления. В качестве примера такого рода устройств можно привести Compas компании Microtest Inc. или 675 LANMeter компании FlukeCorp.

2.2. Системы управления сетью

Любая сложная вычислительная сеть требует дополнительных специальных средств управления помимо тех, которые имеются в стандартных сетевых операционных системах. Это связано с большим количеством разнообразного коммуникационного оборудования, работа которого критична для выполнения сетью своих основных функций. Распределенный характер крупной корпоративной сети делает невозможным поддержание ее работы без централизованной системы управления, которая в автоматическом режиме собирает информацию о состоянии каждого концентратора, коммутатора, мультиплексора или маршрутизатора и предоставляет эту информацию оператору сети. Обычно система управления работает в автоматизированном режиме, выполняя наиболее простые действия по

управлению сетью автоматически, а сложные решения предоставляя принимать человеку на основе подготовленной системой информации. Система управления должна быть интегрированной. Это означает, что функции управления разнородными устройствами должны служить общей цели обслуживания конечных пользователей сети с заданным качеством.

Сами системы управления представляют собой сложные программно-аппаратные комплексы, поэтому существует граница целесообразности применения системы управления – она зависит от сложности сети, разнообразия применяемого коммуникационного оборудования и степени его распределённости по территории. В небольшой сети можно применять отдельные программы управления наиболее сложными устройствами, например коммутатором, поддерживающим технику VLAN. Обычно каждое устройство, которое требует достаточно сложного конфигурирования, производитель сопровождает автономной программой конфигурирования и управления. Однако при росте сети может возникнуть проблема объединения разрозненных программ управления устройствами в единую систему управления, и для решения этой проблемы придется, возможно, отказаться от этих программ и заменить их интегрированной системой управления.

2.2.1. Обзор задач сетевого управления

Системы управления корпоративными сетями существуют не очень давно. Одной из первых систем такого назначения, получившей широкое распространение, был программный продукт SunNet Manager, выпущенный в 1989 г. компанией SunSoft. SunNet Manager был ориентирован на управление коммуникационным оборудованием и контроль трафика сети. Именно эти функции чаще всего имеют в виду, когда говорят о системе управления сетью. Кроме систем управления сетями существуют и системы управления другими элементами корпоративной сети: системы управления ОС, СУБД, корпоративными приложениями. Применяются также системы управления телекоммуникационными сетями: телефонными, а также первичными сетями технологий PDH и SDH.

Независимо от объекта управления, желательно, чтобы система управления выполняла ряд функций, которые определены международными стандартами, обобщающими опыт применения систем управления в различных областях. Существуют рекомендации ITU-T X.700 и близкий к ним стандарт ISO 7498-4, которые делят задачи системы управления на пять функциональных групп:

- управление конфигурацией сети и именованием;
- обработка ошибок;
- анализ производительности и надежности;
- управление безопасностью;
- учет работы сети.

Рассмотрим задачи этих функциональных областей управления применительно к системам управления сетями.

Управление конфигурацией сети и именованием (Configuration Management). Эти задачи заключаются в конфигурировании параметров как элементов сети (Network Element, NE), так и сети в целом. Для элементов сети, таких как маршрутизаторы, мультиплексоры и т.п., с помощью этой группы задач определяются сетевые адреса, идентификаторы (имена), географическое положение и пр.

Для сети в целом управление конфигурацией обычно начинается с построения карты сети, т.е. отображения реальных связей между элементами сети и изменения связей между элементами сети – образование новых физических или логических каналов, изменение таблиц коммутации и маршрутизации.

Управление конфигурацией (как и другие задачи системы управления) может выполняться в автоматическом, ручном или полуавтоматическом режимах. Например, карта сети может составляться автоматически, на основании зондирования реальной сети пакетами-исследователями, а может быть введена оператором системы управления вручную. Чаще всего применяются полуавтоматические методы, когда автоматически полученную карту оператор подправляет вручную. Методы автоматического построения топологической карты, как правило, являются фирменными разработками.

Более сложной задачей является настройка коммутаторов и маршрутизаторов на поддержку маршрутов и виртуальных путей между пользователями сети. Согласованная ручная настройка таблиц маршрутизации при полном или частичном отказе от использования протокола маршрутизации (а в некоторых глобальных сетях, например X.25, такого протокола просто не существует) представляет собой сложную задачу. Многие системы управления сетью общего назначения ее не выполняют, но существуют специализированные системы конкретных производителей, например система NetSys компании Cisco Systems, которая решает ее для маршрутизаторов этой же компании.

Обработка ошибок (Fault Management). Эта группа задач включает выявление, определение и устранение последствий сбоев и отказов в работе сети. На этом уровне выполняется не только регистрация сообщений об ошибках, но и их фильтрация, маршрутизация и анализ на основе некоторой корреляционной модели. Фильтрация позволяет выделить из весьма интенсивного потока сообщений об ошибках, который обычно наблюдается в большой сети, только важные сообщения, маршрутизация обеспечивает их доставку нужному элементу системы управления, а корреляционный анализ позволяет найти причину, породившую поток взаимосвязанных сообщений (например, обрыв кабеля может быть причиной большого количества сообщений о недоступности сетей и серверов).

Устранение ошибок может быть как автоматическим, так и полуавтоматическим. В первом случае система непосредственно управляет оборудованием или программными комплексами и обходит отказавший элемент за счет резервных каналов и т.п. В полуавтоматическом режиме основные решения и действия по устранению неисправности выполняют люди, а система управления только помогает в организации этого процесса – оформляет квитанции на выполнение работ и отслеживает их поэтапное выполнение (подобно системам групповой работы).

В этой группе задач иногда выделяют подгруппу задач управления проблемами, подразумевая под проблемой сложную ситуацию, требующую для разрешения обязательного привлечения специалистов по обслуживанию сети.

Анализ производительности и надежности (Performance Management). Задачи этой группы связаны с оценкой на основе накопленной статистической информации таких параметров, как время реакции системы, пропускная способность реального или виртуального канала связи между двумя конечными абонентами сети, интенсивность трафика в отдельных сегментах и каналах сети, вероятность искажения данных при их передаче через сеть, а также коэффициент готовности сети или ее определенной транспортной службы. Функции анализа производительности и надежности сети нужны как для оперативного управления сетью, так и для планирования развития сети.

Результаты анализа производительности и надежности позволяют контролировать соглашение об уровне обслуживания (Service Level Agreement, SLA), заключаемое между пользователем сети и ее администраторами (или компанией, продающей услуги). Обычно в SLA оговариваются такие параметры надежности, как коэффициент готовности службы в течение года и месяца, максимальное время устранения отказа, а также параметры производительности, например, средняя и максимальная пропускная способности при соединении двух точек подключения пользовательского оборудования, время реакции сети (если информационная служба, для которой определяется время реакции, поддерживается внутри сети), максимальная задержка пакетов при передаче через сеть (если сеть используется только как транзитный транспорт). Без средств анализа производительности и надежности поставщик услуг публичной сети или отдел информационных технологий предприятия не сможет ни проконтролировать, ни тем более обеспечить нужный уровень обслуживания для конечных пользователей сети.

Управление безопасностью (Security Management). Задачи этой группы включают в себя контроль доступа к ресурсам сети (данным и оборудованию) и сохранение целостности данных при их хранении и передаче через сеть. Базовыми элементами управления безопасностью являются процедуры аутентификации пользователей, назначение и проверка прав дос-

тупа к ресурсам сети, распределение и поддержка ключей шифрования, управления полномочиями и т.п. Часто функции этой группы не включаются в системы управления сетями, а реализуются либо в виде специальных продуктов (например, системы аутентификации и авторизации Kerberos, различных защитных экранов, систем шифрования данных), либо входят в состав операционных систем и системных приложений.

Учет работы сети (Accounting Management). Задачи этой группы занимаются регистрацией времени использования различных ресурсов сети – устройств, каналов и транспортных служб. Эти задачи имеют дело с такими понятиями, как время использования службы и плата за ресурсы – billing. Ввиду специфического характера оплаты услуг у различных поставщиков и различными формами соглашения об уровне услуг, эта группа функций обычно не включается в коммерческие системы и платформы управления типа HP Open View, а реализуется в заказных системах, разрабатываемых для конкретного заказчика.

Модель управления OSI не делает различий между управляемыми объектами – каналами, сегментами локальных сетей, мостами, коммутаторами и маршрутизаторами, модемами и мультиплексорами, аппаратным и программным обеспечением компьютеров, СУБД. Все эти объекты управления входят в общее понятие «система», и управляемая система взаимодействует с управляющей системой по открытым протоколам OSI.

Однако на практике деление систем управления по типам управляемых объектов широко распространено. Ставшими классическими системы управления сетями, такие как SunNet Manager, HP Open View или Cabletron Spectrum, управляют только коммуникационными объектами корпоративных сетей, т.е. концентраторами и коммутаторами локальных сетей, а также маршрутизаторами и удаленными мостами, как устройствами доступа к глобальным сетям. Оборудованием территориальных сетей обычно управляют системы производителей телекоммуникационного оборудования, такие как RADView компании RAD Data Communications, MainStreetXpress 46020 компании Newbridge и т.п.

2.2.2. Функции систем управления системой

Рассмотрим, как преломляются общие функциональные задачи системы управления, определенные в стандартах X.700/ISO 7498-4, в задачи такого конкретного класса систем управления, как системы управления компьютерами и их системным и прикладным программным обеспечением. Их называют системами управления системой (System Management System).

Обычно система управления системой выполняет следующие функции.

Учет используемых аппаратных и программных средств (Configuration Management). Система автоматически собирает информацию об установленных в сети компьютерах и создает записи в специальной базе дан-

ных об аппаратных и программных ресурсах. После этого администратор может быстро выяснить, какими ресурсами он располагает и где тот или иной ресурс находится, например, узнать о том, на каких компьютерах нужно обновить драйверы принтеров, какие компьютеры обладают достаточным количеством памяти, дискового пространства и т.п.

Распределение и установка программного обеспечения. После завершения обследования администратор может создать пакеты рассылки нового программного обеспечения, которое нужно инсталлировать на всех компьютерах сети или на какой-либо группе компьютеров. В большой сети, где проявляются преимущества системы управления, такой способ инсталляции может существенно уменьшить трудоемкость этой процедуры. Система может также позволять централизованно устанавливать и администрировать приложения, которые запускаются с файловых серверов, а также дать возможность конечным пользователям запускать такие приложения с любой рабочей станции сети.

Удаленный анализ производительности и возникающих проблем (Fault Management and Performance Management). Эта группа функций позволяет удаленно измерять наиболее важные параметры компьютера, операционной системы, СУБД и т.д. (например, коэффициент использования процессора, интенсивность страничных прерываний, коэффициент использования физической памяти, интенсивность выполнения транзакций). Для разрешения проблем эта группа функций может давать администратору возможность брать на себя удаленное управление компьютером в режиме эмуляции графического интерфейса популярных операционных систем. База данных системы управления обычно хранит детальную информацию о конфигурации всех компьютеров в сети для того, чтобы можно было выполнять удаленный анализ возникающих проблем.

Примерами систем управления системами являются Microsoft System Management Server (SMS), CA Unicenter, HP Operations center и мн. др.

Как видно из описания функций системы управления системами, они повторяют функции системы управления сетью, но только для других объектов. Действительно, функция учета используемых аппаратных и программных средств соответствует функции построения карты сети, функция распределения и установки программного обеспечения – функции управления конфигурацией коммутаторов и маршрутизаторов, а функция анализа производительности и возникающих проблем – функции производительности.

Эта близость функций систем управления сетями и систем управления системами позволила разработчикам стандартов OSI не делать различия между ними и разрабатывать общие стандарты управления.

На практике уже несколько лет также заметна отчетливая тенденция интеграции систем управления сетями и системами в единые интегрированные продукты управления корпоративными сетями, например CA

Unicenter TNG или TME-10 IBM/Tivoli. Наблюдается также интеграция систем управления телекоммуникационными сетями с системами управления корпоративными сетями.

2.2.3. Архитектура систем управления сетями

Выделение в системах управления типовых групп функций и разбиение этих функций на уровни еще не дают ответа на вопрос, каким же образом устроены системы управления, из каких элементов они состоят и какие архитектуры связей этих элементов используются на практике.

Схема «менеджер – агент». В основе любой системы управления сетью лежит элементарная схема взаимодействия агента с менеджером. На основе этой схемы могут быть построены системы практически любой сложности с большим количеством агентов и менеджеров разного типа (рис. 1).

Рис. 1. Взаимодействие агента, менеджера и управляемого ресурса

Агент является посредником между управляемым ресурсом и основной управляющей программой-менеджером. Чтобы один и тот же менеджер мог управлять различными реальными ресурсами, создается некоторая модель управляемого ресурса, которая отражает только те характеристики ресурса, которые нужны для его контроля и управления. Например, модель маршрутизатора обычно включает такие характеристики, как количество портов, их тип, таблицу маршрутизации, количество кадров и пакетов протоколов канального, сетевого и транспортного уровней, прошедших через эти порты.

Менеджер получает от агента только те данные, которые описываются моделью ресурса. Агент же является некоторым экраном, освобождающим менеджера от ненужной информации о деталях реализации ресурса. Агент поставляет менеджеру обработанную и представленную в нормализованном виде информацию. На основе этой информации менеджер принимает решения по управлению, а также выполняет дальнейшее обобщение данных о состоянии управляемого ресурса, например, строит зависимость загрузки порта от времени.

Для получения требуемых данных от объекта, а также для выдачи на него управляющих воздействий агент взаимодействует с реальным ресурсом некоторым нестандартным способом. Когда агенты встраиваются в коммуникационное оборудование, то разработчик оборудования предусматривает точки и способы взаимодействия внутренних узлов устройства с агентом. При разработке агента для операционной системы разработчик агента пользуется теми интерфейсами, которые существуют в этой ОС, например интерфейсами ядра, драйверов и приложений. Агент может снабжаться специальными датчиками для получения информации, например датчиками релейных контактов или датчиками температуры.

Менеджер и агент должны располагать одной и той же моделью управляемого ресурса, иначе они не смогут понять друг друга. Однако в использовании этой модели агентом и менеджером имеется существенное различие. Агент наполняет модель управляемого ресурса текущими значениями характеристик данного ресурса, и в связи с этим модель агента называют базой данных управляющей информации – Management Information Base, MIB. Менеджер использует модель, чтобы знать о том, чем характеризуется ресурс, какие характеристики он может запросить у агента и какими параметрами можно управлять.

Менеджер взаимодействует с агентами по стандартному протоколу. Этот протокол должен позволять менеджеру запрашивать значения параметров, хранящихся в базе MIB, а также передавать агенту управляющую информацию, на основе которой тот должен управлять устройством. Различают управление inband, т.е. по тому же каналу, по которому передаются пользовательские данные, и управление out-of-band, т.е. вне канала, по которому передаются пользовательские данные. Например, если менеджер взаимодействует с агентом, встроенным в маршрутизатор, по протоколу SNMP, передаваемому по той же локальной сети, что и пользовательские данные, то это будет управление inband. Если же менеджер контролирует коммутатор первичной сети, работающий по технологии частотного уплотнения FDM, с помощью отдельной сети X.25, к которой подключен агент, то это будет управление out-of-band. Управление по тому же каналу, по которому работает сеть, более экономично, так как не требует создания отдельной инфраструктуры передачи управляющих данных. Однако способ out-of-band более надежен, так как он предоставляет возможность управлять оборудованием сети и тогда, когда какие-то элементы сети вышли из строя и по основным каналам оборудование недоступно. Стандарт многоуровневой системы управления TMN имеет в своем названии слово Network, подчеркивающее, что в общем случае для управления телекоммуникационной сетью создается отдельная управляющая сеть, которая обеспечивает режим out-of-band.

Обычно менеджер работает с несколькими агентами, обрабатывая получаемые от них данные и выдавая на них управляющие воздействия. Агенты могут встраиваться в управляемое оборудование, а могут и рабо-

тать на отдельном компьютере, связанном с управляемым оборудованием по какому-либо интерфейсу. Менеджер обычно работает на отдельном компьютере, который выполняет также роль консоли управления для оператора или администратора системы.

Модель «менеджер – агент» лежит в основе таких популярных стандартов управления, как стандарты Internet на основе протокола SNMP и стандарты управления ISO/OSI на основе протокола CMIP.

Агенты могут отличаться различным уровнем интеллекта – они могут обладать как самым минимальным интеллектом, необходимым для подсчета проходящих через оборудование кадров и пакетов, так и весьма высоким, достаточным для выполнения самостоятельных действий по выполнению последовательности управляющих действий в аварийных ситуациях, построению временных зависимостей, фильтрации аварийных сообщений и т.п.

В крупной корпоративной сети полностью централизованная система управления, построенная на базе единственного менеджера, вряд ли будет работать хорошо по нескольким причинам. Во-первых, такой вариант не обеспечивает необходимой масштабируемости по производительности, так как единственный менеджер вынужден будет обрабатывать весь поток сообщений от всех агентов, что при нескольких тысячах управляемых объектов потребует очень высокопроизводительной платформы для работы менеджера и перегрузит служебной управляющей информацией каналы передачи данных в той сети, где будет расположен менеджер. Во-вторых, такое решение не обеспечит необходимого уровня надежности, так как при отказе единственного менеджера будет потеряно управление сетью. В-третьих, в большой распределенной сети целесообразно располагать в каждом географическом пункте отдельным оператором или администратором, управляющим своей частью сети, а это удобнее реализовать с помощью отдельных менеджеров для каждого оператора.

Схема «менеджер – агент» позволяет строить достаточно сложные в структурном отношении распределенные системы управления.

Обычно распределенная система управления включает большое количество связок «менеджер – агент», которые дополняются рабочими станциями операторов сети, с помощью которых они получают доступ к менеджерам (рис. 2).

Каждый агент собирает данные и управляет определенным элементом сети. Менеджеры, иногда также называемые серверами системы управления, собирают данные от своих агентов, обобщают их и хранят в базе данных. Операторы, работающие за рабочими станциями, могут соединиться с любым из менеджеров и с помощью графического интерфейса просмотреть данные об управляемой сети, а также выдать менеджеру некоторые директивы по управлению сетью или ее элементами.

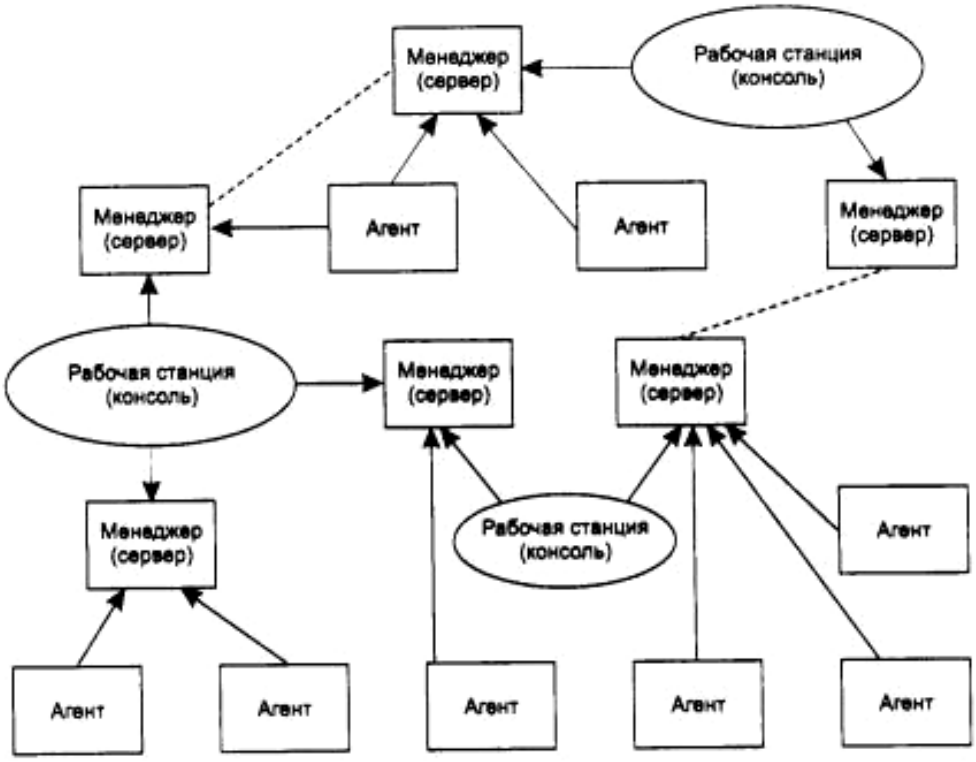

Рис. 2. Распределенная система управления на основе нескольких менеджеров и рабочих станций

Наличие нескольких менеджеров позволяет распределить между ними нагрузку по обработке данных управления, обеспечивая масштабируемость системы.

Как правило, связи между агентами и менеджерами носят более упорядоченный характер, чем тот, который показан на рисунке 2. Чаще всего используются два подхода к их соединению – одноранговый (рис. 3) и иерархический (рис. 4).

Рис. 3. Одноранговые связи между менеджерами

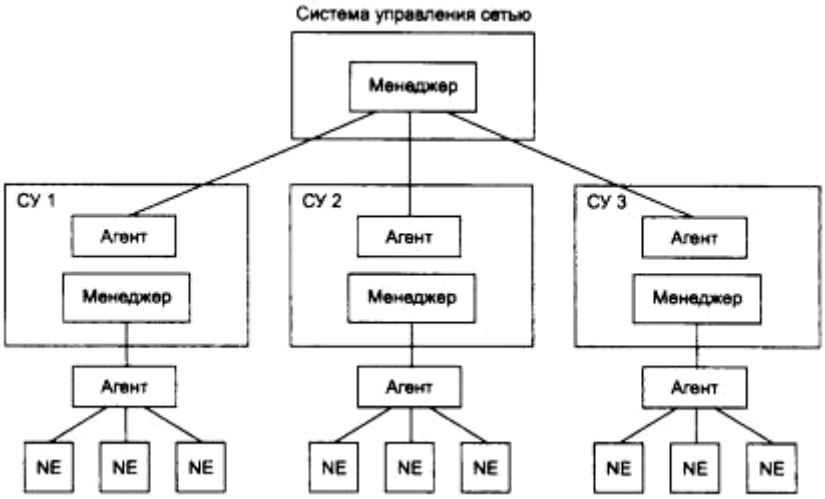

Рис. 4. Иерархические связи между менеджерами

В случае одноранговых связей каждый менеджер управляет своей частью сети на основе информации, получаемой от нижележащих агентов. Центральный менеджер отсутствует. Координация работы менеджеров достигается за счет обмена информацией между базами данных каждого менеджера.

Одноранговое построение системы управления сегодня считается неэффективным и устаревшим. Обычно оно вызвано тем обстоятельством, что элементарные системы управления построены как монолитные системы, которые первоначально не были ориентированы на модульность системы (например, многие системы управления, разработанные производителями оборудования, не поддерживают стандартные интерфейсы для взаимодействия с другими системами управления). Затем эти менеджеры нижнего уровня стали объединяться для создания интегрированной системы управления сетью, но связи между ними оказалось возможным создавать только на уровне обмена между базами данных, что достаточно медленно. Кроме того, в базах данных таких менеджеров накапливается слишком детальная информация об управляемых элементах сети (так как первоначально эти менеджеры разрабатывались как менеджеры нижнего уровня), вследствие чего такая информация малопригодна для координации работы всей сети в целом. Такой подход к построению системы управления называется подходом «снизу вверх».

Гораздо более гибким является иерархическое построение связей между менеджерами. Каждый менеджер нижнего уровня выполняет также функции агента для менеджера верхнего уровня. Такой агент работает уже с гораздо более укрупненной моделью (MIB) своей части сети, в которой собирается именно та информация, которая нужна менеджеру верхнего уровня для управления сетью в целом. Обычно для разработки моделей сети на разных уровнях проектирование начинают с верхнего уровня, на ко-

тором определяется состав информации, требуемой от менеджеров-агентов более низкого уровня, поэтому такой подход назван подходом «сверху вниз». Он сокращает объемы информации, циркулирующей между уровнями системы управления, и приводит к гораздо более эффективной системе управления.

2.2.4. Платформенный подход

При построении систем управления крупными локальными и корпоративными сетями обычно используется платформенный подход, когда индивидуальные программы управления разрабатываются не «с нуля», а используют службы и примитивы, предоставляемые специально разработанным для этих целей программным продуктом – платформой. Примерами платформ для систем управления являются такие известные продукты, как HP OpenView, SunNet Manager и Sun Soltice, Cdbletron Spectrum, IMB/Tivoli TMN10.

Эти платформы создают общую операционную среду для приложений системы управления точно так же, как универсальные операционные системы, такие как Unix или Windows, создают операционную среду для приложений любого типа, таких как MS Word, Oracle и т.п. Платформа обычно включает поддержку протоколов взаимодействия менеджера с агентами – SNMP и реже CMIP, набор базовых средств для построения менеджеров и агентов, а также средства графического интерфейса для создания консоли управления. В набор базовых средств обычно входят функции, необходимые для построения карты сети, средства фильтрации сообщений от агентов, средства ведения базы данных. Набор интерфейсных функций платформы образует интерфейс прикладного программирования (API) системы управления. Пользуясь этим API, разработчики из третьих фирм создают законченные системы управления, которые могут управлять специфическим оборудованием в соответствии с пятью основными группами функций.

Обычно платформа управления поставляется с каким-либо универсальным менеджером, который может выполнять некоторые базовые функции управления без программирования. Чаще всего к этим функциям относятся функции построения карты сети (группа Configuration Management), а также функции отображения состояния управляемых устройств и функции фильтрации сообщений об ошибках (группа Fault Management). Например, одна из наиболее популярных платформ HP OpenView поставляется с менеджером Network Node Manager, который выполняет перечисленные функции.

Чем больше функций выполняет платформа, тем лучше. В том числе и таких, которые нужны для разработки любых аспектов работы приложений, прямо не связанных со спецификой управления. В конце концов, приложения системы управления – это прежде всего приложения, а потом уже

приложения системы управления. Поэтому полезны любые средства, предоставляемые платформой, которые ускоряют разработку приложений вообще и распределенных приложений в частности.

Компании, которые производят коммуникационное оборудование, разрабатывают дополнительные менеджеры для популярных платформ, которые выполняют функции управления оборудованием данного производителя более полно. Примерами таких менеджеров могут служить менеджеры системы Optivity компании Bay Networks и менеджеры системы Trancsend компании 3Com, которые могут работать в среде платформ HP OpenView и SunNet Manager.

2.2.5. Стандарты систем управления

При формализации схемы «менеджер – агент» могут быть стандартизованы следующие аспекты ее функционирования:

- протокол взаимодействия агента и менеджера;
- интерфейс «агент – управляемый ресурс»;
- интерфейс «агент – модель управляемого ресурса»;
- интерфейс «менеджер – модель управляемого ресурса»;
- справочная система о наличии и местоположении агентов и менеджеров, упрощающая построение распределенной системы управления;
- язык описания моделей управляемых ресурсов, т.е. язык описания MIB;
- схема наследования классов моделей объектов (дерево наследования), которая позволяет строить модели новых объектов на основе моделей более общих объектов, например, модели маршрутизаторов на основе модели обобщенного коммуникационного устройства;
- схема иерархических отношений моделей управляемых объектов (дерево включения), которая позволяет отразить взаимоотношения между отдельными элементами реальной системы, например, принадлежность модулей коммутации определенному коммутатору или отдельных коммутаторов и концентраторов определенной подсети.

Существующие стандарты на системы управления отличаются тем, что в них могут быть стандартизованы не все перечисленные выше аспекты схемы «менеджер – агент».

В стандартах систем управления как минимум стандартизуется некоторый способ формального описания моделей управляемых объектов, а также определяется протокол взаимодействия между менеджером и агентом.

Сегодня на практике применяются два семейства стандартов управления сетями – стандарты Internet, построенные на основе протокола SNMP (Simple Network Management Protocol), и международные стандарты ISO/ITU-T, использующие в качестве протокола взаимодействия агентов и менеджеров протокол CMIP (Common Management Information Protocol).

Стандарты систем управления, основанных на протоколе SNMP, формализуют минимум аспектов системы управления, а стандарты ISO/ITU-T – максимум аспектов, как и большинство стандартов, разработанных ITU-T. Традиционно в локальных и корпоративных сетях применяются в основном системы управления на основе SNMP, а стандарты ISO/ITU-T и протокол CMIP находят применение в телекоммуникационных сетях.

3. ПРОТОКОЛЫ СЕТЕВОГО УПРАВЛЕНИЯ SNMP, RMON

3.1. Концепции SNMP-управления

Наиболее распространенным протоколом управления сетями является протокол *SNMP (Simple Network Management Protocol)*, его поддерживают сотни производителей. Главные достоинства протокола SNMP – простота, доступность, независимость от производителей. В значительной степени именно популярность SNMP задержала принятие CMIP, варианта управляющего протокола по версии OSI. Протокол SNMP разработан для управления маршрутизаторами в сети Internet и является частью стека TCP/IP.

SNMP – это протокол, используемый для получения от сетевых устройств информации об их статусе, производительности и характеристиках, которые хранятся в специальной базе данных сетевых устройств, называемой *MIB (Management Information Base)*. Существуют стандарты, определяющие структуру MIB, в том числе набор типов ее переменных (объектов в терминологии ISO), их имена и допустимые операции этими переменными (например, читать).

В MIB, наряду с другой информацией, могут храниться сетевой и/или MAC-адреса устройств, значения счетчиков обработанных пакетов и ошибок, номера, приоритеты и информация о состоянии портов. Древовидная структура MIB содержит обязательные (стандартные) поддеревья, а также в ней могут находиться частные (private) поддеревья, позволяющие изготовителю интеллектуальных устройств реализовать какие-либо специфические функции на основе его специфических переменных.

В системах управления, построенных на основе протокола SNMP, стандартизуются следующие элементы:

- протокол взаимодействия агента и менеджера;
- язык описания моделей MIB и сообщений SNMP – язык абстрактной синтаксической нотации ASN.1 (стандарт ISO 8824:1987, рекомендации ITU-T X.208);
- несколько конкретных моделей MIB (MIB-I, MIB-II, RMON, RMON-2), имена объектов которых регистрируются в дереве стандартов ISO.

Все остальное отдается на откуп разработчику системы управления. Протокол SNMP и тесно связанная с ним концепция SNMP MIB были разработаны для управления маршрутизаторами Internet как временное решение. Но, как это часто бывает со всем временным, простота и эффективность решения обеспечили успех этого протокола, который сегодня используется при управлении практически любыми видами оборудования и программного обеспечения вычислительных сетей. И хотя в области управления телекоммуникационными сетями наблюдается устойчивая тенденция применения стандартов ITU-T, в которые входит протокол CMIP, здесь имеется достаточно много примеров успешного использования SNMP-управления. Агенты SNMP встраиваются в аналоговые модемы, модемы ADSL, коммутаторы ATM и т.д.

SNMP – это протокол прикладного уровня, разработанный для стека TCP/IP, хотя имеются его реализации и для других стеков, например IPX/SPX. Протокол SNMP используется для получения от сетевых устройств информации об их статусе, производительности и других характеристиках, которые хранятся в базе данных управляющей информации MIB (Management Information Base). Простота SNMP во многом определяется простотой MIB SNMP, особенно их первых версий MIB I и MIB II. Кроме того, сам протокол SNMP также весьма несложен.

Существуют стандарты, определяющие структуру MIB, в том числе набор типов ее объектов, их имена и допустимые операции над этими объектами (например, «считать»).

Древовидная структура MIB содержит обязательные (стандартные) поддеревья, а также в ней могут находиться частные (private) поддеревья, позволяющие изготовителю интеллектуальных устройств управлять какими-либо специфическими функциями устройства на основе специфических объектов MIB.

Агент в протоколе SNMP – это обрабатывающий элемент, который обеспечивает менеджерам, размещенным на управляющих станциях сети, доступ к значениям переменных MIB и тем самым дает им возможность реализовывать функции по управлению и наблюдению за устройством (рис. 5).

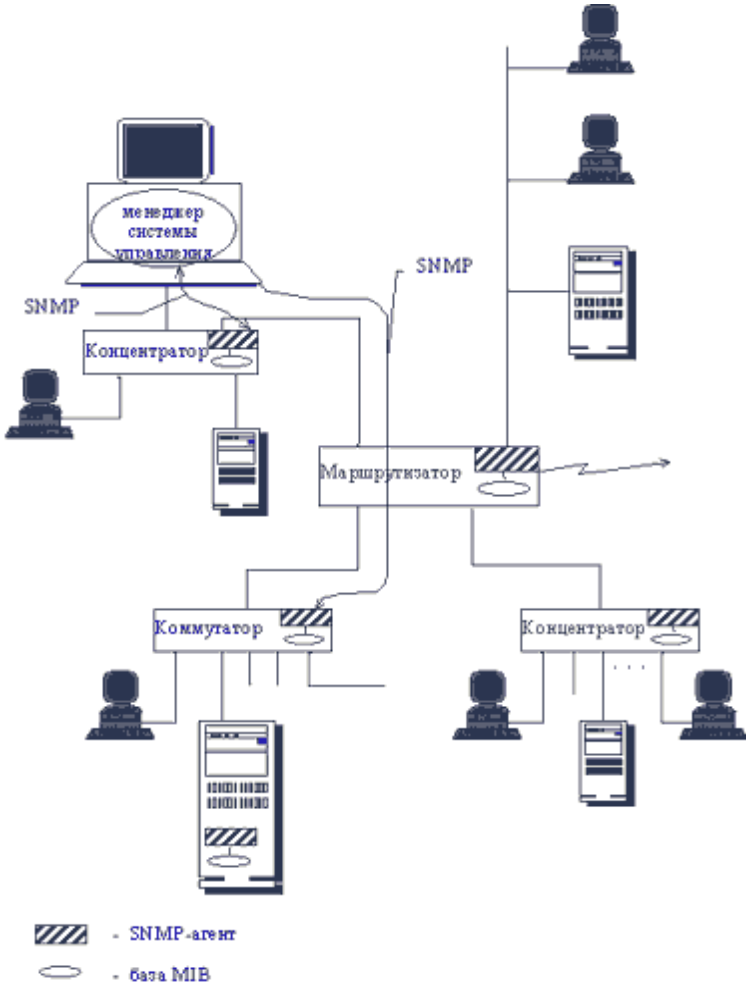

Рис. 5. Типичная структура системы управления сетью

Основные операции по управлению вынесены в менеджер, а агент SNMP выполняет чаще всего пассивную роль, передавая в менеджер по его запросу значения накопленных статистических переменных. При этом устройство работает с минимальными издержками на поддержание управляющего протокола. Оно использует почти всю свою вычислительную мощность для выполнения своих основных функций маршрутизатора, моста или концентратора, а агент занимается сбором статистики и значений переменных состояния устройства и передачей их менеджеру системы управления.

3.2. Команды протокола SNMP

SNMP – это протокол типа «запрос-ответ», т.е. на каждый запрос, поступивший от менеджера, агент должен передать ответ. Особенностью протокола является его чрезвычайная простота – он включает в себя всего несколько команд.

Команда Get-request используется менеджером для получения от агента значения какого-либо объекта по его имени.

Команда GetNext-request используется менеджером для извлечения значения следующего объекта (без указания его имени) при последовательном просмотре таблицы объектов.

С помощью команды Get-response агент SNMP передает менеджеру ответ на команды Get-request или GetNext-request.

Команда Set используется менеджером для изменения значения какого-либо объекта. С помощью команды Set происходит собственно управление устройством. Агент должен понимать смысл значений объекта, который используется для управления устройством, и на основании этих значений выполнять реальное управляющее воздействие – отключить порт, приписать порт определенной VLAN и т.п. Команда Set пригодна также для установки условия, при выполнении которого агент SNMP должен послать менеджеру соответствующее сообщение. Может быть определена реакция на такие события, как инициализация агента, рестарт агента, обрыв связи, восстановление связи, неверная аутентификация и потеря ближайшего маршрутизатора. Если происходит любое из этих событий, то агент инициализирует прерывание.

Команда Trap используется агентом для сообщения менеджеру о возникновении особой ситуации.

Версия SNMP v.2 добавляет к этому набору команду GetBulk, которая позволяет менеджеру получить несколько значений переменных за один запрос.

3.3. Структура SNMP MIB

На сегодня существует несколько стандартов на базы данных управляющей информации для протокола SNMP. Основными являются стандарты MIB-I и MIB-II, а также версия базы данных для удаленного управления RMON MIB. Кроме этого существуют стандарты для специальных устройств MIB конкретного типа (например, MIB для концентраторов или MIB для модемов), а также частные MIB конкретных фирм-производителей оборудования.

Первоначальная спецификация MIB-I определяла только операции чтения значений переменных. Операции изменения или установки значений объекта являются частью спецификаций MIB-II.

Версия MIB-I (RFC 1156) определяет 114 объектов, которые подразделяются на восемь групп:

System – общие данные об устройстве (например, идентификатор поставщика, время последней инициализации системы).

Interfaces – параметры сетевых интерфейсов устройства (например, их количество, типы, скорости обмена, максимальный размер пакета).

Address Translation Table – описание соответствия между сетевыми и физическими адресами (например, по протоколу ARP).

Internet Protocol – данные, относящиеся к протоколу IP (адреса IP-шлюзов, хостов, статистика о IP-пакетах).

ICMP – данные, относящиеся к протоколу обмена управляющими сообщениями ICMP.

TCP – данные, относящиеся к протоколу TCP (например, о TCP-соединениях).

UDP – данные, относящиеся к протоколу UDP (число переданных, принятых и ошибочных UPD-дейтаграмм).

EGP – данные, относящиеся к протоколу обмена маршрутной информацией Exterior Gateway Protocol, используемому в Internet (число принятых с ошибками и без ошибок сообщений).

Из этого перечня групп переменных видно, что стандарт MIB-I разрабатывался с жесткой ориентацией на управление маршрутизаторами, поддерживающими протоколы стека TCP/IP.

В версии MIB-II (RFC 1213), принятой в 1992 г., был существенно (до 185) расширен набор стандартных объектов, а число групп увеличилось до 10. На рисунке 6 приведен пример древовидной структуры базы объектов MIB-II. На нем показаны две из 10 возможных групп объектов – System (имена объектов начинаются с префикса Sys) и Interfaces (префикс if). Объект SysUpTime содержит значение продолжительности времени работы системы с момента последней перезагрузки, объект SysObjectID – идентификатор устройства (например, маршрутизатора).

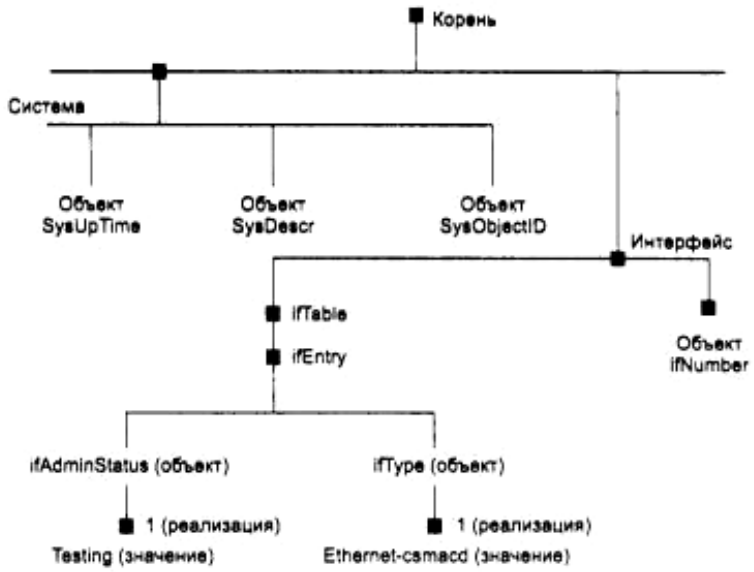

Рис. 6. Стандартное дерево MIB-II (фрагмент)

Объект ifNumber определяет количество сетевых интерфейсов устройства, а объект ifEntry является вершиной поддерева, описывающего один из конкретных интерфейсов устройства. Входящие в это поддерево объекты ifType и ifAdminStatus определяют, соответственно, тип и состояние одного из интерфейсов, в данном случае интерфейса Ethernet.

В число объектов, описывающих каждый конкретный интерфейс устройства, включены следующие:

ifType – тип протокола, который поддерживает интерфейс. Этот объект принимает значения всех стандартных протоколов канального уровня, например rfc877-x25, ethemet-csmacd, iso88023-csmacd, iso88024-tokenBus, iso88025-tokenRlng и т.д.

ifMtu – максимальный размер пакета сетевого уровня, который можно послать через этот интерфейс.

ifSpeed – пропускная способность интерфейса в битах в секунду (100 для Fast Ethernet).

ifPhysAddress – физический адрес порта, для Fast Ethernet им будет MAC-адрес.

ifAdminStatus – желаемый статус порта.

up – готов передавать пакеты.

down – не готов передавать пакеты.

testing – находится в тестовом режиме.

ifOperStatus – фактический текущий статус порта, имеет те же значения, что и ifAdminStatus.

ifInOctets – общее количество байт, принятое данным портом, включая служебные, с момента последней инициализации SNMP-агента.

iflnUcastPkts – количество пакетов с индивидуальным адресом интерфейса, доставленных протоколу верхнего уровня.

IflnNUcastPkts – количество пакетов с широковещательным или мультивещательным адресом интерфейса, доставленных протоколу верхнего уровня.

ifInDiscards – количество пакетов, которые были приняты интерфейсом, оказались корректными, но не были доставлены протоколу верхнего уровня, скорее всего, из-за переполнения буфера пакетов или же по иной причине.

ifin Errors – количество пришедших пакетов, которые не были переданы протоколу верхнего уровня из-за обнаружения в них ошибок.

Кроме объектов, описывающих статистику по входным пакетам, имеются аналогичные объекты, но относящиеся к выходным пакетам.

Как видно из описания объектов MIB-II, эта база данных не дает детальной статистики по характерным ошибкам кадров Ethernet, кроме этого, она не отражает изменение характеристик во времени, что часто интересует сетевого администратора.

Эти ограничения были впоследствии сняты новым стандартом на MIB-RMON MIB, который специально ориентирован на сбор детальной статистики по протоколу Ethernet, к тому же с поддержкой такой важной функции, как построение агентом зависимостей статистических характеристик от времени.

3.4. Протокол RMON

Стандарт на RMON появился в ноябре 1991 г., когда Internet Engineering Task Force выпустил документ RFC 1271 под названием Remote Network Monitoring Management Information Base (Информационная база дистанционного мониторинга сетей). Данный документ содержал описание RMON для сетей Ethernet. В сентябре 1993 г. к нему добавился документ RFC 1513, определяющий RMON для сетей Token Ring. Наконец, в феврале 1995 г. был выпущен документ RFC 1757, представляющий собой новую версию RFC 1271.

RMON – это расширение SNMP, в основе которого, как и в основе SNMP, лежит сбор и анализ информации о характере информации, передаваемой по сети. Как и в SNMP, сбор информации осуществляется аппаратно-программными агентами, данные от которых поступают на компьютер, где установлено приложение управления сетью. Отличие RMON от своего предшественника состоит, в первую очередь, в характере собираемой информации – если в SNMP эта информация характеризует только события, происходящие на том устройстве, где установлен агент, то RMON требует, чтобы получаемые данные характеризовали трафик между сетевыми устройствами, а ведь именно это, как правило, и интересует администратора сети более всего.

Передача информации от агентов SNMP приложению управления осуществляется по следующей схеме: приложение управления опрашивает агентов, а они в ответ высылают необходимые данные. Предусмотрено и нечто вроде механизма прерываний – агент может послать приложению запрос на обслуживание (например, при возникновении какого-либо отказа), однако этот механизм в SNMP несовершенен и применяется редко. Сами агенты анализом данных о работе сети не занимаются – это целиком и полностью оставлено в компетенции приложений управления. Ясно, что такая схема обмена информацией сильно перегружает сеть и потому является неприемлемой для сетей глобального масштаба, где стоимость трафика чрезвычайно высока. В отличие от агентов SNMP, агенты RMON самостоятельно выполняют анализ данных и посылают на приложение управления уже частично обработанные данные. Помимо этого, сами агенты RMON могут выполнять простейшие функции по управлению сетью, в частности, осуществлять фильтрацию пакетов.

Интеллект агентов RMON позволяет им выполнять также простые действия по диагностике неисправностей и предупреждению о возможных отказах – например, в рамках технологии RMON можно собрать данные о нормальном функционировании сети (т.е. выполнить так называемый baselining), а потом выставлять предупреждающие сигналы, когда режим работы сети отклонится от baseline – это может свидетельствовать, в частности, о неполной исправности оборудования. Собрав воедино информацию, по-

лучаемую от агентов RMON, приложение управления может помочь администратору сети (находящемуся, например, за тысячи километров от анализируемого сегмента сети) локализовать неисправность и выработать оптимальный план действий для ее устранения.

Сбор информации RMON осуществляется аппаратно-программными зондами, подключаемыми непосредственно к сети. Чтобы выполнить задачу сбора и первичного анализа данных, зонд должен обладать достаточными вычислительными ресурсами и объемом оперативной памяти. В настоящее время на рынке имеются зонды трех типов: встроенные, зонды на базе компьютера и автономные. Продукт считается поддерживающим RMON, если в нем реализована хотя бы одна группа RMON. Разумеется, чем больше групп данных RMON реализовано в данном продукте, тем он, с одной стороны, дороже, а с другой – тем более полную информацию о работе сети он предоставляет.

Встроенные зонды представляют собой модули расширения для сетевых устройств. Такие модули выпускаются многими производителями, в частности, такими крупными компаниями, как 3Com, Cabletron, Bay Networks и Cisco. Наиболее естественным выглядит решение встраивать модули RMON в концентраторы, ведь именно из наблюдения за этими устройствами можно составить себе представление о работе сегмента. Достоинство таких зондов очевидно: они позволяют получать информацию по всем основным группам данных RMON при относительно невысокой цене. Недостатком в первую очередь является не слишком высокая производительность, что проявляется, в частности, в том, что встроенные зонды часто поддерживают далеко не все группы данных RMON. Не так давно 3Com объявила о намерении выпустить поддерживающие RMON драйверы для сетевых адаптеров Etherlink III и Fast Ethernet. В результате окажется возможным собирать и анализировать данные RMON непосредственно на рабочих станциях в сети.

Зонды на базе компьютера – это просто подключенные к сети компьютеры с установленным на них программным агентом RMON. Такие зонды (к числу которых относится, например, продукт Cornerstone Agent 2.5 компании Network General) обладают более высокой производительностью, чем встроенные зонды, и поддерживают, как правило, все группы данных RMON. Они более дороги, чем встроенные зонды, но гораздо дешевле автономных зондов. Помимо этого, зонды на базе компьютера имеют довольно большой размер, что может иногда ограничивать возможности их применения.

Автономные зонды обладают наивысшей производительностью; как легко понять, это одновременно и наиболее дорогие продукты из всех описанных. Как правило, автономный зонд – это процессор (класса Pentium или RISC-процессор), оснащенный достаточным объемом оперативной памяти и сетевым адаптером. Лидерами в этом секторе рынка являются

компании Frontier и Hewlett-Packard. Зонды этого типа невелики по размеру и весьма мобильны – их очень легко подключать к сети и отключать от нее. При решении задачи управления сетью глобального масштаба это, конечно, не слишком важное свойство, однако если средства RMON применяются для анализа работы корпоративной сети средних размеров, то (учитывая высокую стоимость устройств) мобильность зондов может сыграть весьма положительную роль. Существуют компании, предоставляющие зонды в аренду, а также оказывающие комплексные услуги по диагностике сети – приходят, подключают зонды, наблюдают за работой сети, а потом выдают рекомендации администраторам.

Информацию, собираемую агентами, надо обобщать и представлять в удобном для пользователя виде. Этим занимаются приложения управления, представляющие собой весьма сложные программы, обеспечивающие просмотр статистики в целом по сети, выявление наиболее загруженных участков, обнаружение основных источников перегрузок (при этом удается выявить наиболее активные приложения), а также позволяющие выполнять анализ протоколов. Среди производителей наиболее продвинутого программного обеспечения надо упомянуть ARMON, Frontier Software, Hewlett-Packard и Novell.

3.5. Спецификация RMON MIB

Новейшим добавлением к функциональным возможностям SNMP является спецификация RMON, которая обеспечивает удаленное взаимодействие с базой MIB. До появления RMON протокол SNMP не мог использоваться удаленным образом, он допускал только локальное управление устройствами. База RMON MIB обладает улучшенным набором свойств для удаленного управления, так как содержит агрегированную информацию об устройстве, не требующую передачи по сети больших объемов информации. Объекты RMON MIB включают дополнительные счетчики ошибок в пакетах, более гибкие средства анализа трендов и статистики, более мощные средства фильтрации для захвата и анализа отдельных пакетов, а также более сложные условия установления сигналов предупреждения. Агенты RMON MIB более интеллектуальны по сравнению с агентами MIB-I или MIB-II и выполняют значительную часть работы по обработке информации об устройстве, которую раньше выполняли менеджеры. Эти агенты могут располагаться внутри различных коммуникационных устройств, а также быть выполнены в виде отдельных программных модулей, работающих на универсальных персональных компьютерах и ноутбуках.

В соответствии с документом RFC 1271, информационная база управления RMON состоит из десяти групп данных.

Первая группа носит название группы статистики (statistics). В ней собирается общая информация о трафике в данном сегменте и степени использования пропускной способности сети – количестве переданных байтов и сетевых пакетов, числе ошибок и коллизий и т.д.

Группа предыстории (history) отвечает за сбор информации, определенной в группе статистики, в течение определенного времени (от одной секунды до одного часа). В результате оказывается возможным проанализировать текущие тенденции в работе сети и сравнить текущее состояние с базовым – это позволит выявить нежелательные явления в работе сети раньше, чем они превратятся в серьезную проблему (например, пока сбои в работе оборудования не привели к его полному отказу).

Группа аварийных сигналов (alarms) позволяет пользователю определить ряд пороговых уровней (эти пороги могут относиться к самым разным вещам – любому параметру из группы статистики, амплитуде или скорости его изменения и многому другому), по превышении которых генерируется аварийный сигнал. Пользователь может также определить, при каких условиях превышение порогового значения должно сопровождаться аварийным сигналом – это позволит избежать генерации сигнала по пустякам, что плохо, во-первых, потому, что на постоянно горящую красную лампочку никто не обращает внимания, а во-вторых, потому, что передача ненужных аварийных сигналов по сети приводит к излишней загрузке линий связи. Аварийный сигнал, как правило, передается в группу событий, где и определяется, что с ним делать дальше.

Четвертая группа информационной базы управления RMON – группа хостов (hosts). В ней регистрируются все хост-машины и прочие сетевые устройства, работающие в данном сегменте сети, и осуществляется сбор основной статистики для этих устройств.

Таблица N главных хостов (HostTopN) содержит список N первых хостов, характеризующихся максимальным значением заданного статистического параметра для заданного интервала. Например, можно затребовать список 10 хостов, для которых наблюдалось максимальное количество ошибок в течение последних 24 часов. Список этот будет составлен самим агентом, а приложение управления получит только адреса этих хостов и значения соответствующих статистических параметров. Отчетливо видно, до какой степени такой подход экономит сетевые ресурсы.

Шестая группа данных информационной базы – матрица трафика (traffic matrix). Строки этой матрицы пронумерованы в соответствии с MAC-адресами станций-источников сообщений, а столбцы – в соответствии с адресами станций-получателей. Матричные элементы характеризуют интенсивность трафика между соответствующими станциями и количество ошибок. Проанализировав такую матрицу, пользователь легко может выяснить, какие пары станций генерируют наиболее интенсивный трафик.

Эта матрица опять-таки формируется самим агентом, поэтому отпадает необходимость в передаче больших объемов данных на центральный компьютер, отвечающий за управление сетью.

Группа фильтров (filters), как можно понять из самого ее названия, используется для фильтрации пакетов. Признаки, по которым фильтруются пакеты, могут быть самыми разнообразными – например, можно потребовать отфильтровывать как ошибочные все пакеты, длина которых оказывается меньше некоторого заданного значения. Можно сказать, что установка фильтра соответствует как бы организации канала для передачи пакета. Куда ведет этот канал – определяет пользователь. Например, все ошибочные пакеты могут перехватываться и направляться в соответствующий буфер. Кроме того, появление пакета, соответствующего установленному фильтру, может рассматриваться как событие (event), на которое система должна реагировать заранее оговоренным образом.

В состав группы перехвата пакетов (packet capture) входят буфера для захвата, куда направляются пакеты, чьи признаки удовлетворяют условиям, сформулированным в группе фильтров. При этом захватываться может не пакет целиком, а, скажем, только первые несколько десятков байт пакета. Содержимое буферов перехвата можно впоследствии анализировать при помощи различных программных средств, выясняя целый ряд весьма полезных характеристик работы сети. Перестраивая фильтры на те или иные признаки, можно характеризовать разные параметры работы сети.

В группе событий (events) определяется, когда следует отправлять аварийный сигнал приложению управления, когда – перехватывать пакеты, и вообще – как реагировать на те или иные события, происходящие в сети, например, на превышение заданных в группе alarms пороговых значений: следует ли ставить в известность приложение управления, или надо просто запротоколировать данное событие и продолжать работать. События могут и не быть связаны с передачей аварийных сигналов – например, направление пакета в буфер перехвата тоже представляет собой событие.

Десятая группа данных важна только для сетей Token Ring, поэтому мы на ней подробно останавливаться не станем. Здесь, в частности, определяется порядок следования станций в кольце.

Как видно, все группы данных информационной базы управления RMON описывают обмен данными в пределах одного сегмента локальной сети. Приложения управления могут собрать из этих фрагментов картину обмена данными в масштабах всей сети. Задача эта очень сложна, и, соответственно, программы для ее решения немногочисленны и весьма дороги. Естественным образом возникает вопрос, нельзя ли часть сборки переложить на плечи распределенных по сети агентов – так же, как в свое время был совершен переход от SNMP к RMON. Именно эту задачу и призван решить новый стандарт RMON 2, который сначала вроде бы должен был появиться в ноябре 1995 г., потом это событие было перенесено на конец лета 1996 г., но до сих пор о нем что-то ничего не слышно.

В RMON 2 будет описан сбор данных, описывающих работу сети на сетевом уровне и уровне приложений. О своей готовности реализовать RMON 2 объявили уже многие производители сетевого оборудования, работающего под RMON.

Всего стандарт RMON MIB определяет около 200 объектов в 10 группах, зафиксированных в двух документах – RFC 1271 для сетей Ethernet и RFC 1513 для сетей Token Ring.

Отличительной чертой стандарта RMON MIB является его независимость от протокола сетевого уровня (в отличие от стандартов MIB-I и MIB-II, ориентированных на протоколы TCP/IP). Поэтому он удобен для гетерогенных сред, использующих различные протоколы сетевого уровня.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Основная литература

1. Microsoft Windows 2003 Server: Учебный курс MCSE [Текст] : учеб. пособие. – М. : Русская редакция, 2003. – 664 с.
2. Администрирование сетей на основе Microsoft Windows 2003: Учебный курс MCSE [Текст] : учеб. пособие. – М. : Русская редакция, 2003. – 537 с.
3. Администрирование SQL Server 2000. Учебный курс MCSE [Текст] : учеб. пособие. – М. : Русская редакция, 2003. – 459 с.
4. Суздалев, А.В. Передача данных в локальных сетях связи [Текст] : учебник / А.В. Суздалев, О.С. Чугреев. – М. : Радио и связь, 2005. – 168 с.
5. Зелигер, Н.Б. Проектирование сетей и систем передачи дискретных сообщений [Текст] : учеб. пособие / Н.Б. Зелигер, О.С. Чугреев, Г.Г. Яновский. – М. : Радио и связь, 2004. – 176 с.
6. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы [Текст] : учеб. пособие / В.Г. Олифер, Н.А. Олифер. – СПб. : Питер, 2003. – 672 с.
7. Джонс, А. Руководство системного администратора Windows: для профессионалов [Текст] : учеб. пособие / А. Джонс. – СПб. : Питер, 2003. – 368 с.
8. Робишо, П. MCSE: Администрирование инфраструктуры сети Windows 2003 [Текст] : учеб. пособие / П. Робишо. – М. : Лори, 2004. – 590 с.

Дополнительная литература

9. Microsoft Systems Management Server 2.0. Учебный курс [Текст] : учеб. пособие. – М. : Русская редакция, 2004. – 437 с.
10. Мизин, И.А. Протоколы информационно-вычислительных сетей [Текст] : справочник / И.А. Мизин, А.П. Кулешов. – М. : Радио и связь, 2006. – 504 с.
11. Щербо, В.К. Стандарты по локальным вычислительным сетям [Текст] : учеб. пособие / В.К. Щербо, В.М. Киреичев. – М. : Радио и связь, 2005. – 304 с.
12. Мафтик, С. Механизмы защиты в сетях ЭВМ [Текст] : учеб. пособие / С. Мафтик. – М. : Мир, 2003. – 216 с.
13. Шибанов, В.С. Средства автоматизации управления в системах связи [Текст] : учеб. пособие / В.С. Шибанов, Н.И. Лычагин. – М. : Радио и связь, 2005. – 232 с.
14. Реймер, С. Active Directory для Windows Server 2003. Справочник администратора [Текст] : учеб. пособие / С. Реймер, М. Малкер. – М. : СП ЭКОМ, 2004. – 512 с.
15. Ханикат, Дж. Знакомство с Microsoft Windows Server 2003 [Текст] : учеб. пособие / Дж. Ханикат. – М. : Русская редакция, 2004. – 464 с.

Учебное издание

АДМИНИСТРИРОВАНИЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Учебно-методическое пособие

Составители: НИКУЛИЧЕВ Николай Николаевич
СЕМЁНОВ Владимир Владимирович МАНЖУЛА
Владимир Гаврилович
ПОПОВ Алексей Эдуардович

Ответственный за выпуск Н.В. Ковбасюк
Редактор В.В. Крайнова
Компьютерная верстка: Н.А. Алтаева

ИД № 06457 от 19.12.01 г. Издательство ЮРГУЭС.
Подписано в печать 28.04.08 г.
Формат бумаги 60х84/16. Усл. печ. л. 2,8. Тираж 116 экз. Заказ № 163.

ПЛД № 65-175 от 05.11.99 г.
Типография Издательства ЮРГУЭС.
346500, г. Шахты, Ростовская обл., ул. Шевченко, 147