Министерство образования и науки Российской Федерации
Белгородский государственный технологический университет
им. В. Г. Шухова

В. В. Михайлов

АДМИНИСТРИРОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ

Конспект лекций

Белгород
2017

Министерство образования и науки Российской Федерации
Белгородский государственный технологический университет
им. В. Г. Шухова

В. В. Михайлов

АДМИНИСТРИРОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ

Конспект лекций

Утверждено ученым советом университета в качестве учебного пособия для студентов очной и заочной форм обучения направлений 09.03.02 - Информационные системы и технологии, 09.03.03 - Прикладная информатика

Белгород
2017

УДК 004.7(07)
ББК 32.97я7
М 69

Рецензенты:

Кандидат технических наук, доцент Белгородского государственного технологического университета им. В. Г. Шухова *Д. Н. Старченко*

Кандидат технических наук, доцент Белгородского государственного аграрного университета им. В. Я. Горина *В. А. Игнатенко*

Михайлов, В. В.

М 69 Администрирование информационных систем: конспект лекций: учебное пособие / В. В. Михайлов. – Белгород: Изд-во БГТУ, 2017. – 112 с.

В учебном пособии рассмотрены основные теоретические и практические вопросы, касающиеся администрирования информационных систем (ИС). Основное внимание уделено подходам к моделированию и проектированию ИС, учитывая доменные структуры, их функционал и безопасность. Также рассматриваются среды и технологии виртуализации серверного парка, процесс конфигурации и администрирования ошибок в ИС.

Учебное пособие предназначено для студентов очной и заочной форм обучения направлений 09.03.02 - Информационные системы и технологии, 09.03.03 - Прикладная информатика.

Данное издание публикуется в авторской редакции.

УДК 004.7(07)
ББК 32.97я7

ОГЛАВЛЕНИЕ

Введение

Сегодня обилие средств вычислительной техники и все более широкое использование информационных систем (ИС) в жизни и деятельности человека привело к необходимости в специалистах, которые умеют создавать и администрировать системы такого класса. При этом потребность в них возрастает, а область их деятельности постоянно расширяется с увеличением размеров и сложности информационных систем.

В данном курсе лекций рассматриваются основные темы из области администрирования информационных систем. Уделено внимание стандартизации администрирования, моделированию ИС, настройке системных и программных средств. Более подробно освещаются вопросы практического проектирования и создания доменных структур и средствам управления доменными ресурсами: объектам, структурам и службам управления доменами. Также уделено внимание сетевому администрированию и управлению сетевыми потоками информации. Рассмотрены основные технологии и программные средства и системы виртуализации компьютерного парка. Уделено внимание администрированию процесса конфигурации и поиска и диагностики ошибок при создании и сопровождении ИС.

Дисциплина «Администрирование информационных систем» является завершающей для обучающегося по направлениям 09.03.02 – Информационные системы и технологии и 09.03.03 – Прикладная информатика. В виду этого в данном курсе лекций излагаются вопросы, касающиеся общих методов администрирования ИС. Более конкретные аспекты конфигурирования программных и аппаратных средств, программирования ИС и управления ими рассматриваются в предшествующих этому курсу дисциплинах.

1. АДМИНИСТРИРОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ (ИС). ВВОДНЫЕ ПОЛОЖЕНИЯ

В данной теме рассматриваются вводные положения по администрированию ИС, функции администратора системы (АС), состав служб администратора системы и их функции. С учетом многообразия и сложности выполнения ряда функций администратором системы и службами администратора системы также излагаются требования к специалистам, работающим в службах администрирования информационных систем. На основе общих положений по организации и построению открытых и гетерогенных систем (к которым относится большинство информационных систем) делается вывод о необходимости рассмотрения стандартов работы ИС и стандартизирующих организаций.

1.1. Функции и состав служб администратора системы

Администратор системы (системный администратор) — это человек или группа людей, которые создают и затем эксплуатируют информационную систему предприятия. Он или они могут быть сотрудниками служб информационных технологий компании и выполняют широкий набор функций, в который входят:

- установка и сопровождение компьютерных сетевых и информационных систем;
- определение и согласование с фирмами-поставщиками «сей аппаратно-программной и организационной части по реализации системы;
- планирование развития информационных систем и внедрения сервисов;
- решение вопросов ведения проектов;
- обучение технического персонала и пользователей;
- консультирование по компьютерным проблемам персонала предприятия и технических служб;
- решение проблем сбора статистики, мониторинга, диагностики, восстановления и сохранения системы, а также всех вопросов организации, соответствующих программных и аппаратных продуктов для этой деятельности;
- разработка программных продуктов на языках управления заданиями (например, скриптах) с целью создания технологии работы компании и синхронизации работы компонентов информационной системы;
- определение ошибок в работе прикладных, системных и аппаратных средств, используемых предприятием, и решение вопросов по их устранению.

Раньше выполнение этих функций входило в обязанности сотрудников отделов системного программирования вычислительных центров предприятий. В настоящее время эти функции, как правило, выполняются совокупностью информационных служб предприятия, а именно:

- службами управления: конфигурацией, контролем характеристик, ошибочными ситуациями, безопасностью, производительностью;
- службами планирования и развития;
- службами эксплуатации и сопровождения;
- службами общего управления.

Службы управления конфигурацией занимаются вопросами задания параметров запуска (инсталляции) операционных систем (ОС) и СУБД, заданием параметров запуска приложений. Они же выполняют функции изменения этих параметров при модификации информационной системы, следя за согласованностью и совместимостью этих параметров.

Службы управления по контролю характеристик и ошибочными ситуациями осуществляют мониторинг и сбор статистики параметров информационной системы при помощи специальных программно-аппаратных комплексов, устанавливают критерии определения опасных и тревожных ситуаций, следят за их обнаружением и устранением, используют специальные методы и средства диагностики ошибок.

Службы управления безопасностью (иногда их называют службами защиты от несанкционированного доступа — НСД) осуществляют комплекс мероприятий по противодействию различным угрозам несанкционированного доступа, настраивают работу различных ОС, СУБД и прикладных продуктов, внедряя их собственные средства защиты от НСД. Эти службы управляют всеми имеющимися в организации компьютерными средствами защиты, например, программируют кодовые замки и системы контроля доступа в помещение. Они же при помощи средств ОС, СУБД, прикладных продуктов или специальных управляющих программных продуктов ведут учет использования ресурсов в системе и контроль (аудит) за их разрешенным (санкционированным) использованием пользователями системы.

Службы управления производительностью обычно работают в тесном взаимодействии со службами управления по контролю характеристик и ошибочными ситуациями. При помощи аппаратно-программных комплексов они анализируют работу информационной системы и следят за такими параметрами, как время работы приложения, время от-

клика приложения, время обращения к дисковой подсистеме ввода-вывода, задержка передачи данных и др. Анализируя результаты совместно с другими службами, они определяют причины изменения параметров работы системы и способы предотвращения или коррекции ухудшений значений параметров.

Службы планирования и развития определяют техническую и экономическую эффективность от внедрения различного вида информационных услуг или сервисов компании, следят за появлением новых компьютерных технологий и оценивают целесообразность их использования, ведут внедряемые проекты и планируют работы других служб и компаний-поставщиков и инсталляторов по их реализации. Контролируют выполнение подрядными организациями работ по внедрению частей информационной системы или их модернизации.

Службы эксплуатации и сопровождения осуществляют архивирование (копирование) и восстановление информационной системы. Эти службы определяют режимы копирования (копируется вся система или ее часть), расписание копирования (например, еженедельное с затиранием предыдущей копии), ведут базу данных копий при помощи программно-аппаратных средств, проводят проверки целостности данных (их непротиворечивости) средствами информационной системы (например, при помощи утилит СУБД), определяют стратегию восстановления информационной системы (например, режим автооткатов ОС). Они же занимаются сопровождением аппаратных средств (например, заменой картриджа принтера), подключением новых пользователей (например, организацией для них рабочего места), организацией электропитания, выполнением профилактических работ (например, уходом за оборудованием при помощи составов, препятствующих накоплению электростатики компьютеров).

Службы общего управления занимаются управлением работы всех информационных служб, согласованием их действий, выработкой корпоративных стандартов (например, на формат документов), разработкой инструкций для пользователей, их обучением и консультацией, ведением нормативно справочной документации необходимой в организации.

1.2. Требования к специалистам служб администрирования ИС

Профессиональные навыки специалистов, работающих в службах администрирования ИС должны быть достаточно высоки и разнообразны. Так, с учетом функций по администрированию ИС, системные

администраторы должны обладать знаниями в нескольких предметных областях:

- теории операционных систем (ОС) и практики их установки;
- теории баз данных и вопросов администрации СУБД, вопросов поддержки целостности данных;
- сетевых технологий, сетевого оборудования (конфигурации и применения коммутаторов и маршрутизаторов), вопросов диагностики сетевых проблем;
- электротехники и реализации кабельных систем для целей передачи данных;
- реализации веб-приложений и организации доступа к web-сайтам;
- защиты информации от несанкционированного доступа, включая администрирование специальных устройств (firewall) и консультации пользователей по вопросам защиты их информации;
- вычислительной техники, начиная с простейших операций и заканчивая архитектурой центров обработки данных (ЦОД);
- основ проектирования информационных систем, прикладного программирования;
- способов восстановления информации и реализации подсистем ввода-вывода, файловых подсистем;
- языков программирования;
- методов управления в информационных системах и соответствующих аппаратно-программных комплексов.

Область деятельности системных администраторов должна охватывать все компоненты информационной системы.

Под **информационной системой** будем понимать материальную систему, организующую, хранящую, преобразующую, обрабатывающую, передающую и предоставляющую информацию.

Рассмотрим компоненты ИС.

Технические средства ИС включают в свой состав вычислительные комплексы, средства передачи данных (сетевую аппаратуру), кабельные системы или средства передачи данных в эфирной (неограниченной) среде.

Программные и технологические средства ИС (процедуры обработки информации). Здесь обычно выделяют системные средства, позволяющие управлять аппаратной частью и данными (ОС и СУБД), и процедуры управления специализированной функциональной обработки согласно требованиям предметной области (прикладное программное обеспечение).

Информационный фонд подразумевает саму информацию, способы ее организации (модель данных) и языки представления и управления информацией (лингвистическое обеспечение).

Структура большинства ИС разбивается на функционально важные подсистемы (см. рис. 1).

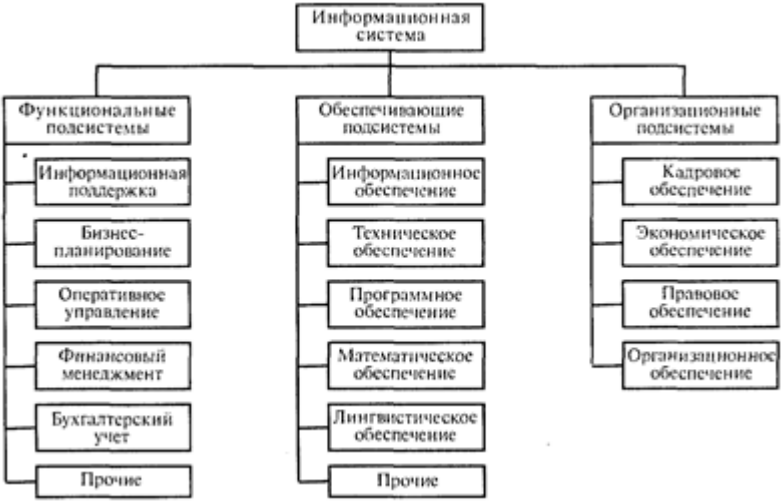

Рис. 1. Функциональный состав ИС

Функциональные подсистемы реализуют и сопровождают модели, методы и алгоритмы обработки информации и формирования управляющих воздействий в рамках задач предметной области.

Состав **обеспечивающих подсистем** достаточно стабилен, мало зависит от предметной области и наряду с информационным, программным и техническим обеспечением включает математическое обеспечение (совокупность методов, моделей и алгоритмов обработки данных) и лингвистическое обеспечение (совокупность языковых средств представления и обработки информации).

Организационные подсистемы направлены на обеспечение эффективной работы персонала и реализацию организационных процедур.

Управление (администрирование) ИС — это совокупность действий, осуществляемых администратором системы средствами самой ИС, обеспечивающих сохранение и/или развитие ее свойств в заданном направлении. В полном объеме управлять всеми компонентами ИС и

всеми ее функциональными подсистемами может только непосредственно руководство предприятия. АС обычно выполняет задачи управления обеспечивающих подсистем и частично задачи управления функциональных и организационных подсистем в рамках, переданных ему руководством предприятия полномочий. Обычно администрирование обеспечивающих подсистем подразделяют на следующие группы задач:

- администрирование кабельных систем зданий и кампусов;
- администрирование ОС и СУБД;
- администрирование компьютерной сети и средств подключения к операторам связи;
- администрирование данных.

При этом администраторы систем должны обладать специальным складом мышления, нацеленным на поиск решения проблемы (чаще всего ошибки или недостаточной скорости работы системы) в условиях ограниченного времени и общение с весьма нервным пользователем. Сложность заключается в том, что информационные технологии развиваются чрезвычайно быстро и еще быстрее устаревают. Поэтому помимо университетских знаний в области компьютерных наук, защиты информации, сетевых технологий, архитектуры ЭВМ, языков программирования и даже экономических дисциплин необходимо постоянное дополнительное изучение отдельных продуктов и технологий. Полезно также иметь сертификаты о прохождении обучения в промышленных компаниях по вопросам ОС, коммуникационных технологий, RAID-технологий, кабельных систем, такие как: Novell CAN, CNE, CISCO CCNA, Sun Certified SCNA, Microsoft MSCA, MCSE и аналогичные.

К сожалению, в небольших организациях вместо совокупности служб администрирования организуется группа администрирования систем, а в ряде случаев только один специалист выделяется для выполнения всех разнообразных функций, и это, безусловно, сказывается на качестве работ.

1.3. Общие понятия об открытых и гетерогенных системах

В настоящее время администрирование ИС чаще всего осуществляется в условиях, когда эти системы являются открытыми и гетерогенными. Но предварительно остановимся на понятиях корпоративной и глобальной информационных систем.

Корпоративной ИС называется информационная система, виртуально объединяющая (в информационном плане) все части одной организации, которые могут находиться в разных городах, частях страны

или земного шара. Доступ пользователей в корпоративную систему возможен только для членов компании, ее клиентов или ее контрагентов. В то же время множество информационных систем сегодня пересекают национальные, коммерческие и континентальные границы для обеспечения глобального взаимодействия большого числа организаций и физических лиц. Такие ИС называются глобальными. К глобальной системе имеет доступ любой пользователь в соответствии с определенными правилами, выработанными самоорганизованным комитетом пользователей и разработчиков такой системы. Примером системы является сеть Интернет с комитетом IETF (Internet Engineering Task Force).

С появлением больших корпоративных и глобальных ИС возникла необходимость взаимодействия друг с другом различных производителей программных и аппаратных средств. В результате появилось понятие открытой системы.

В широком смысле открытой системой может быть названа любая система (компьютер, вычислительная сеть, операционная система, программный продукт), которая построена в соответствии с открытыми спецификациями для интерфейсов, служб и форматов.

Напомним, что под термином **«спецификация»** (в вычислительной технике) понимают формализованное описание аппаратных или программных компонентов, способов их функционирования, взаимодействия с другими компонентами, условий эксплуатации, ограничений и особых характеристик.

Такую спецификацию еще называют протоколом. Под **открытыми** спецификациями понимают опубликованные, общедоступные спецификации стандартизирующих организаций или компаний-разработчиков аппаратных и программных средств.

Использование при разработке систем открытых спецификаций позволяет третьим сторонам разрабатывать для этих систем различные аппаратные или программные средства расширения и модификации, а также создавать программно-аппаратные комплексы из продуктов разных производителей.

Для реальных систем полная открытость — недостижимая цель. Как правило, даже в системах, называемых открытыми, этому определению соответствуют лишь некоторые ее части, поддерживающие внешние интерфейсы. Но при администрировании систем в общем случае следует стремиться к тому, чтобы система создавалась и работала с помощью открытых спецификаций. Только тогда можно обеспечить ее быстрое и своевременное развитие, технологичную поддержку и модифика-

цию. Исключением могут быть специализированные системы, например, применяемые в военно-промышленном комплексе, или отдельные части информационной системы, требующие сугубо корпоративных правил.

Если информационная система построена с соблюдением принципов открытости, то это дает следующие преимущества:

- возможность построения системы из аппаратных и программных средств различных производителей, придерживающихся одного и того же стандарта;
- перенос созданного программного обеспечения с минимальными изменениями в широком диапазоне систем, полученных от одного или нескольких поставщиков;
- возможность безболезненной замены отдельных компонентов системы другими, более совершенными, что позволяет ей развиваться с минимальными затратами;
- возможность легкого сопряжения с другими информационными системами;
- простоту освоения, обслуживания и введения нового персонала для поддержки системы.

Одним из первых примеров открытых систем является ЭВМ IBM/360, открытые спецификации которой позволили различным производителям программного обеспечения разрабатывать прикладные продукты под управлением ее операционной системы OS/360. Примером открытой системы является и международная сеть Интернет, развивавшаяся в полном соответствии с требованиями, предъявляемыми к открытым системам. В результате сеть Интернет объединила в себе самое разнообразное оборудование и программное обеспечение огромного числа различных сетей.

Как уже отмечалось, в современных ИС информация передается между компьютерами различных производителей. При этом используются различные интерфейсы и средства передачи данных, различное программное обеспечение и различная архитектура ЭВМ. Таким образом, практически любая система является разнородной или **гетерогенной**, включающей в себя оборудование и программное обеспечение нескольких производителей, т. е. современные ИС в своем подавляющем большинстве являются открытыми гетерогенными системами (рис. 2).

Особую роль при создании таких систем играют стандарты. Без стандартизации работоспособность этих систем невозможна, поскольку программное обеспечение одного производителя «не поймет» программное обеспечение другого.

Рис. 2. Гетерогенная система

Знание стандартов, их понимание и соблюдение абсолютно необходимо для реализации и сопровождения информационных систем. Существует ряд международных и национальных стандартизирующих организаций, например, ISO (Международная организация по стандартизации) или ANSI (Американский национальный институт стандартов) и целый ряд международных форумов, добровольных самоорганизованных сообществ профессионалов, например, MEF (Metro Ethernet Forum), которые занимаются разработкой стандартов во всех областях информационных технологий. Помимо стандартизирующих организаций свои разработки в области информационных технологий и их стандартизации постоянно ведут крупнейшие мировые производители. Это компании IBM, Lucent Technologies (в настоящее время Alcatel-Lucent), Unisys, Sun Microsystems, Adaptec, Cisco, Nortel, Novell, Microsoft, HP, SAP, Oracle и множество других. Все это требует от администраторов систем постоянного изучения документов, имеющихся в открытом доступе. Такие документы публикуются на официальных сайтах стандартизирующих организаций и форумов и официальных сайтах ведущих компаний-разработчиков аппаратных и программных средств.

1.4. Стандарты работы ИС и стандартизирующие организации

Стандарт — это вариант реализации протокола в аппаратуре или программном обеспечении, который отражается в документе, согласованном и принятом аккредитованной организацией, разрабатывающей стандарты. Стандарт содержит правила, руководства или характеристики для работ или их результатов в целях достижения оптимальной степени упорядочения и согласованности в заданном контексте.

Стандарты могут разрабатываться как стандартизирующими организациями, так и отдельными производственными компаниями. При этом бывают стандарты юридические и фактические (промышленные).

Юридические стандарты подтверждаются законами, которые приняты государством. Государственное управление деятельностью по стандартизации в Российской Федерации осуществляет Федеральное агентство по техническому регулированию и метрологии (Ростехрегулирование, www.gost.ru), на которое возложены функции Национального органа по стандартизации в соответствии с Федеральным законом «О техническом регулировании». Другие органы государственного управления организуют деятельность по стандартизации в пределах их компетенции.

Фактические стандарты существуют, но их использование не определено законами или нормативами.

С точки зрения авторства стандарт может быть частным (корпоративным) или созданным стандартизирующей организацией.

Корпоративные стандарты разрабатываются и внедряются частными коммерческими компаниями для своих продуктов.

Стандарты стандартизирующих организаций создаются специализированными организациями или самоорганизующимися комитетами и форумами.

ITU (International Telecommunications Union) — Международный союз электросвязи; является структурным подразделением ООН.

ISO (The International Organization for Standardization, а так же International Standards Organization) — Международная организация по стандартизации.

IEEE (произносится «ай-трипл-и», Institute of Electrical and Electronics Engineers, Inc.) — Институт инженеров по электротехнике и электронике (США).

EIA (Electronics Industries Alliance) — Ассоциация предприятий электронной промышленности США, альянс EIA.

TIA (Telecommunication Industry Association) — Ассоциация телекоммуникационной промышленности США, ассоциация TIA. Ассоциация изготовителей средств связи, которая разрабатывает стандарты на кабельные системы.

2. ОБЪЕКТЫ АДМИНИСТРИРОВАНИЯ И МОДЕЛИ УПРАВЛЕНИЯ

С точки зрения состава ИС администратор системы сталкивается с необходимостью сопровождать и поддерживать при помощи специальных средств различные компоненты обеспечивающих подсистем и частично функциональных и организационных подсистем.

Для успешного администрирования администратор системы должен знать, что является объектами администрирования ИС и какие наборы функций (модели) используются для управления техническим обеспечением, организационной и функциональной подсистемами.

Рассмотрим объекты администрирования в информационных системах, а затем изложим сущность ряда моделей и соответствующих им протоколов (спецификаций) и технологий. При этом особое внимание обращаем на модели ISO FCAPS, RPC и OGC ITIL, поскольку они наиболее часто используются при администрировании ИС в настоящее время.

2.1. Объекты администрирования в информационных системах

При администрировании информационных систем **объектами администрирования** являются отдельные ее подсистемы, которые часто называют просто системами (например, администрирование кабельной системы). Объектами администрирования также могут быть прикладные или системные процессы обработки данных, существующие в ИС и затрагивающие несколько подсистем (например, администрирование электронной почты или администрирование конфигурации ИС. Т. е. объектами администрирования могут быть как отдельные подсистемы, так и информационные процессы, существующие в нескольких подсистемах.

К задачам администрирования подсистем относятся:

- администрирование кабельной системы;
- поддержка и сопровождение аппаратной части;
- администрирование сетевой системы;
- администрирование прикладной системы;
- администрирование операционной системы;
- Web-администрирование;
- управление информационными службами;
- администрирование СУБД.

Каждая из перечисленных подсистем имеет свои способы, технологии и средства администрирования, которые будут рассмотрены в последующих главах.

Международная организация по стандартизации (ISO) рассматривает в качестве объектов управления не подсистемы ИС, а процессы ИС, например, процесс передачи данных между элементами системы. А организация TMF как объект управления рассматривает совокупность прикладных процессов оператора связи.

В процессе администрирования ИС администратор системы должен руководствоваться моделью администрирования.

Модель администрирования (управления) в ИС - это набор функций по управлению подсистемой или информационным процессом.

Различные стандартизирующие организации предлагают разные наборы функций (различные модели) по управлению техническим обеспечением, организационной и функциональной подсистемами. Это модели ISO OSI, ISO FCAPS, OGC ITIL, ITU TMN, TMF eTOM. Рассмотрим некоторые из них.

2.2. Модель сетевого управления ISO OSI

Модель сетевого управления ISO OSI Management Framework — определена в документе ISO/IEC 7498-4: Basic Reference Model, Part 4, Management Framework. Она является развитием общей семиуровневой модели взаимодействия открытых систем для случая, когда одна система управляет другой.

Документ ISO/IEC 7498-4 состоит из пяти основных разделов:

- термины и общие концепции;
- модель управления системами;
- информационная модель;
- функциональные области управления системами;
- структура стандартов управления системами.

Стандарты ISO в области управления используют специальную терминологию, которой в свою очередь воспользовались создатели Internet в протоколе SNMP (Simple Network Management Protocol — простой протокол управления сетью).

Эта терминология вследствие фактического применения всеми пользователями такой глобальной и открытой системы передачи информации стала фактическим стандартом.

Согласно документам OSI (см. рис. 3) обмен управляющей информацией с помощью протокола управления (Management Protocol) происходит между субъектами приложений управления системами (Systems

Management Application Entities, SMAE). Субъекты SMAE расположены на прикладном уровне семиуровневой модели OSI и являются элементами службы управления. Под субъектом в модели OSI понимается активный в данный момент процесс (протокол) какого-либо уровня, участвующий во взаимодействии. Примерами SMAE являются агенты и менеджеры систем управления ИС.

Сообщения, которые агент посылает менеджеру по своей инициативе, называются уведомлениями (notifications). Элемент X, который является для системы управления управляемым объектом (managed object), может послать уведомление агенту. Элемент X может находиться в той же управляемой системе, что и агент, или в другой системе. В свою очередь агент посылает уведомление менеджеру о том, что элемент X произвёл какое-то действие (например, происходит отказ в работе порта оборудования). В соответствии с этим уведомлением менеджер обновляет базу данных конфигурации системы, которую он сопровождает.

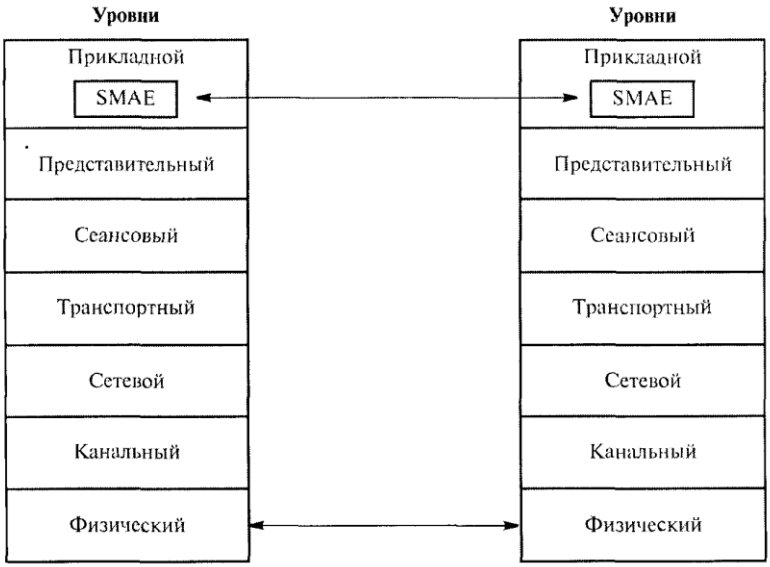

Рис. 3. Концепция SMAE в модели OSI

Менеджер не только собирает и сопоставляет данные, получаемые от агентов, на основе этих данных он может также выполнять административные функции, управляя операциями удаленных агентов.

В модели OSI границы между менеджерами и агентами не очень четкие. Субъект SMAE, выполняющий в одном взаимодействии роль менеджера, в другом взаимодействии может иметь роль агента, и наоборот. Модель OSI не определяет способы взаимодействия агента с управляемыми объектами.

В модели OSI также не говорится о том, как агент взаимодействует с управляемыми объектами, которые находятся за пределами управляемой системы, т. е. объектами, с которыми нужно взаимодействовать через сеть. В таких случаях может потребоваться, например, чтобы один агент запросил данные о некотором объекте от другого агента. Порядок такого рода взаимодействия также не определяется моделью OSI.

Прикладной уровень модели OSI включает в себя несколько вспомогательных служб общего назначения, которые используются прикладными протоколами и пользовательскими приложениями (в том числе и приложениями управления) для автоматизации наиболее часто выполняемых действий.

ACSE (Association Control Service Element). Эта служба отвечает за установление соединений между приложениями различных систем. Соединение (сессия, сеанс) на прикладном уровне OSI носит название ассоциации. Ассоциации бывают индивидуальными и групповыми (shared).

RTSE (Reliable Transfer Service Element). Служба осуществляет поддержку восстановления диалога, вызванного разрывом нижележащих коммуникационных служб, в рамках ассоциации.

ROSE (Remote Operations Service Element). Организует выполнение программных функций на удаленных машинах. Является аналогом службы RPC (Remote Procedure Call — вызов удаленных процедур).

Основная модель управления OSI включает:

- управление системами;
- управление N-уровнем;
- операции N-уровня.

Это разбиение на три области сделано для того, чтобы учесть всё возможные ситуации, возникающие при управлении.

Управление системами имеет дело с управляемыми объектами на всех семи уровнях OSI, включая прикладной уровень. Оно основано на надежной передаче с установлением соединения управляющей информации между конечными системами. Необходимо подчеркнуть, что модель управления OSI не разрешает использовать службы без установления соединения.

Управление N-уровнем ограничено управляемыми объектами какого-то определенного уровня семиуровневой модели. Протокол управления использует при этом коммуникационные протоколы нижележащих уровней. Управление N-уровнем полезно, когда нет возможности использовать все семь уровней OSI. В этом случае допускается пользоваться протоколом управления N-уровня, который строго предназначен для данного уровня.

Операции N-уровня сводятся к мониторингу и управлению на основе управляющей информации, содержащейся в коммуникационных протоколах только данного уровня. Например, данные мониторинга сети, содержащиеся во фреймах STM-n (Synchronous Transport Module — синхронный транспортный модуль), технологии SDH (Synchronous Digital Hierarchy — синхронная цифровая иерархия), относятся к операциям N-уровня, а именно физического уровня. Стандарты на управление N-уровнем и операции N-уровня не входят в набор протоколов управления OSI. Протоколы OSI рассматривают управление системами с помощью полного семиуровневого стека.

2.3. Модель управления ITU TMN

Архитектура и принципы построения TMN обеспечивают реализацию задач по управлению, оперативному контролю и эксплуатации разнородного телекоммуникационного оборудования и систем электросвязи, которые изготовлены различными фирмами-производителями (см. рис. 4).

TMN предназначена для управления услугами сетей связи, для эксплуатации и технического обслуживания оборудования, для оперативно-технического контроля и администрирования сетевых устройств с целью обеспечить нормативное качество оказания услуг связи.

Объектами управления TMN являются телекоммуникационные ресурсы. Телекоммуникационные ресурсы управления физически представляют собой реальное оборудование связи — стойки, функциональные блоки, модули, на определенные свойства которых можно осуществлять целенаправленное управляющее воздействие.

Обмен командами управления и иной информацией между TMN и оборудованием связи осуществляется через опорные точки, которые реализуются в виде стандартизованных или нестандартизованных интерфейсов TMN.

Функции прикладного уровня TMN реализуются с помощью одной или нескольких операционных систем (Operations Systems).

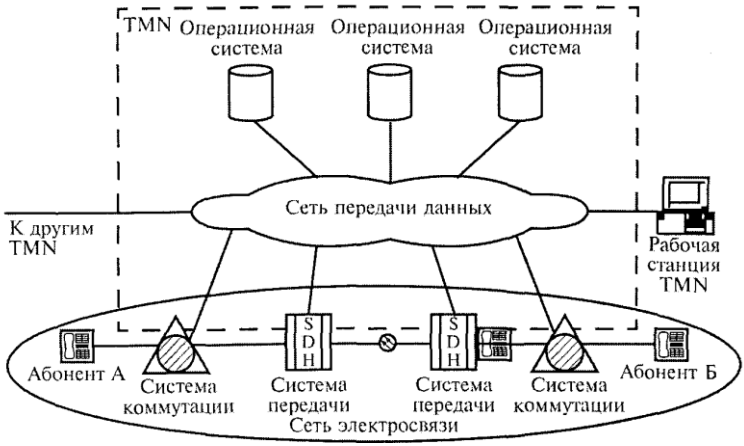

Рис. 4. TMN и сеть электросвязи

Операционные системы выполняют следующие задачи:

• обеспечивают обработку данных (поступающих от управляемой сети электросвязи) в целях мониторинга и контроля функционирования телекоммуникационного оборудования, а также для обеспечения работы собственно TMN;

• поддерживают информационную модель сети электросвязи, которая представляет собой описание физических объектов электросвязи с использованием принятой информационной технологии и специальных программных средств, например, СУБД;

• обеспечивают работу прикладных программных средств управления (приложение управления), которые реализуют большинство услуг и функций управления системами.

• С учетом характеристик управления открытыми системами TMN функционально должна обеспечивать:

• обмен информацией управления между сетями электросвязи и сетью TMN;

• преобразование информации управления для различных систем связи в единый формат в целях обеспечения совместимости и согласованности данных в TMN;

• перенос информации управления между различными компонентами в TMN;

• анализ и соответствующую реакцию на информацию управления;

• преобразование информации управления в форму, которая понятна пользователю системы управления — оператору или администратору; в результате повышается качество услуг управления и обеспечивается дружественное взаимодействие с пользователями посредством общепринятых стандартов графического отображения информации;

• защищенный доступ к информации по управлению для пользователей TMN;

• контроль крупных и сложных объектов управления.

С точки зрения оператора связи можно сформулировать следующие цели, которые должны быть достигнуты при внедрении TMN:

• минимальное время реакции системы управления на существенные сетевые события;

• минимизация нагрузки, создаваемой системой управления; это особенно важно в случае, когда для передачи информации управления используются ресурсы сети электросвязи общего пользования, а не выделенные каналы связи;

• реализация процедур для изоляции мест повреждения (неисправностей) в реальном времени, возможность дистанционного вызова и запуска процедур восстановления повреждений;

• учет различных схем организации сетей связи при реализации функций управления.

Функциональные возможности сети TMN определяются пятью уровнями управления (рис. 5):

• уровень управления бизнесом (Business Management Layer — BML);

• уровень управления услугами (Service Management Layer — SML);

• уровень управления сетью (Network Management Layer — NML);

• уровень управления элементом (Element Management Layer — EML);

• уровень элемента сети (Network Element Layer — NEL).

Реализации TMN могут включать в себя бизнес-функции (Business Operation System Function — B-OSF), которые имеют отношение ко всем управляемым сетям/системам связи и осуществляют общую координацию делового управления оператора связи. Сервисные функции (S-OSF) на уровне управления услугами имеют отношение к услугам связи, предоставляемым с помощью технических средств одной или несколькими сетями электросвязи, и обеспечивают интерфейс с абонентом или клиентом.

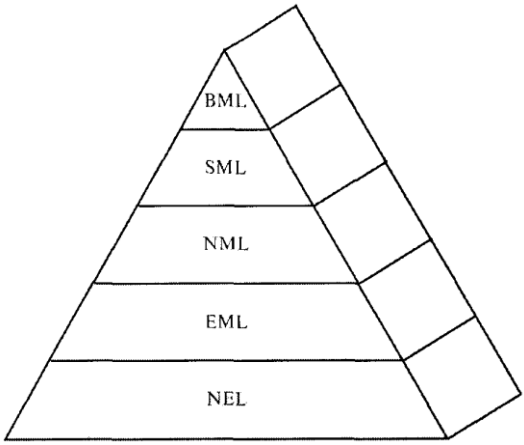

Рис. 5. Модель TMN и ее уровни управления

2.4. Модель управления ISO FCAPS

FCAPS (Fault Configuration Account Performance Security) – модель Международной организации по стандартизации, в которой отражены ключевые функции администрирования и управления сетями (обеспечивающей подсистемы ИС) и не рассматриваются вопросы администрирования функциональной или организационной подсистем. Модель учитывает то, что современные ИС - это системы передачи цифровой информации и предназначены для описания функций администрирования только таких систем. Согласно модели FCAPS, все аспекты администрирования сети ИС можно описать при помощи пяти видов функций. Соотношение моделей FCAPS и TMN, которая будет кратко рассмотрена далее, отражено на рис. 6.

В рекомендациях ITU-T X.700 и в стандарте ISO 7498-4 описаны пять функциональных групп модели FCAPS:

(F) Fault Management (управление отказами) - обнаружение отказов в устройствах сети, сопоставление аварийной информации от различных устройств, локализация отказов и инициирование корректирующих действий;

(C) Configuration Management (управление конфигурированием) - возможность отслеживания изменений, конфигурирования, передачи и установки программного обеспечения на всех устройствах сети;

(A) Accounting Management (управление учетом) - возможность сбора и передачи учетной информации для генерации отчетов об использовании сетевых ресурсов;

(P) Performance Management (управление производительностью) - непрерывный источник информации для мониторинга показателей работы сети (QoS (Quality of Service, Качество обслуживания), ToS (Terms of Service, Тип обслуживания)) и распределения сетевых ресурсов;

(S) Security Management (Управление безопасностью) - возможность управления доступом к сетевым ресурсам и защитой от угроз.

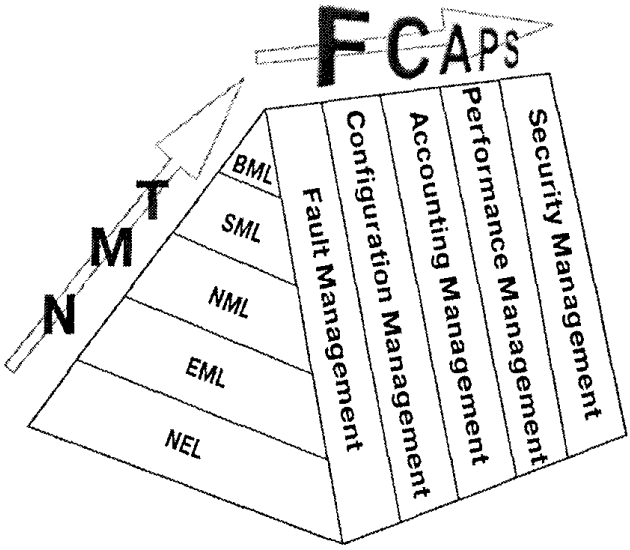

Рис. 6. Соотношение FCAPS и TMN

Управление отказами

Эта группа задач включает в себя 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 и анализ. Фильтрация позволяет выделить из весьма интенсивного потока сообщений об ошибках, только важные сообщения; маршрутизация обеспечивает их доставку нужному элементу системы управления, а анализ позволяет найти причину, породившую поток сообщений.

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

Управление конфигурированием

Эти задачи заключаются в конфигурировании параметров как элементов сети, так и сети в целом. В современных устройствах все управление осуществляется с помощью программного обеспечения, так как конфигурирование даже средней системы представляется весьма трудоемкой задачей. При этом считается, что система размером до 50 портов (пользователей) — маленькая система, до 800 портов — средняя система и более 800 портов — большая система. Для элементов сети, таких как маршрутизаторы, мультиплексоры и пр., с помощью этой группы задач устанавливаются сетевые адреса, идентификаторы (имена), географическое положение и другие базовые параметры.

Для сети в целом управление конфигурацией обычно начинается с анализа функциональной схемы сети, отображающей связи между элементами сети (аппаратными и программными модулями), создаваемой при проектировании ИС и предоставляемой администратору системы компанией-разработчиком.

Средствами конфигурации ИС все производимые при этом процессе изменения должны отражаться в базе данных коммутации и маршрутизации устройств и на функциональных схемах сети.

Задание параметров запуска программного обеспечения или аппаратуры системы должно проводиться администратором системы вручную с документированием полученных результатов и обязательным фиксированием значений параметров, заданных по умолчанию (defaults). Схема сети корректируется автоматически при помощи опроса специализированных программных средств (агентов), запущенных на устройствах сети специальными программными продуктами (менеджерами). Обычно такие программные средства используют протокол управления SNMP.

Настройка параметров запуска или эксплуатации операционных систем коммутаторов, маршрутизаторов, различных серверов является достаточно сложной задачей, требующей подготовленных специалистов - администраторов систем служб управления конфигурацией.

Управление учетом

Задачи этой группы составляют регистрацию права доступа и времени использования различных ресурсов системы — устройств, каналов, подсистем ввода-вывода, дискового пространства, транспортных служб. Помимо регистрации прав и времени работы эти задачи включают в себя различного вида отчетность об используемых ресурсах. Кроме того, функции учета имеют дело с таким понятием, как плата за ресурсы. Вопросы оплаты сервисов и информационных услуг, предоставляемых предприятием, из-за их специфического характера у различных предприятий и различных форм соглашения об уровне услуг не включаются в коммерческие системы управления типа HP Open View, а реализуются в специализированных системах (например, системах биллинга операторов связи).

Эксплуатация таких систем обычно выделяется в отдельную задачу и не входит в компетенцию общих служб эксплуатации администратора системы.

Управление производительностью

Задачи этой группы связаны со сбором статистики, мониторингом, оптимизацией, метриками измерения производительности системы. Главное для администратора системы — понять, по каким именно метрикам (параметрам или критериям) следует рассчитать производительность системы. Ими могут быть время реакции системы, пропускная способность реального или виртуального канала связи между двумя объектами ИС, 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.

Управление безопасностью

Задачи этой группы составляют 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 авторизации, аутентификации, а также аудита пользователей (средства AAA или ЗА). Функции этой группы не только включаются в системы управления сетями, но и всегда реализованы в составе операционных систем, СУБД и системных приложений.

На сегодняшний день модель FCAPS — это основная модель администрирования не только сетевых систем, но и любых ИС как систем передачи данных. Она наиболее распространена и после ее создания ISO была включена ITU в модель TMN.

3. СРЕДСТВА АДМИНИСТРИРОВАНИЯ ОПЕРАЦИОННЫХ СИСТЕМ (ОС)

Основной функцией операционной системы (ОС) является функция управления ресурсами компьютера, включая управление оперативной и дисковой памятью, управление периферийными устройствами и процессором. ОС должна:

- обеспечивать загрузку прикладных программ в оперативную память и их выполнение;
- обеспечивать распределение памяти между различными прикладными процессами и самой ОС;
- обеспечивать работу дисковых подсистем ввода-вывода, магнитных лент, флэш-памяти, управлять распределением дискового пространства на этих носителях и хранить данные на них в виде файловых систем;
- обеспечивать параллельное (или псевдопараллельное, если компьютер имеет только один процессор) исполнение задач, защиту системных ресурсов от ошибочных действий или аварийных ситуаций;
- управлять работой и разделением пользователями различных периферийных устройств (терминалов, принтеров, модемов и т.д.);
- выполнять аутентификацию и авторизацию пользователей;
- реализовывать организацию взаимодействия задач друг с другом и их приоритезацию для исполнения;
- реализовывать средства обеспечения безопасности;
- диагностировать систему и собирать статистику по ее работе.

Управление всеми этими функциями операционной системы осуществляется с помощью параметров ядра ОС и специальных средств (утилит) ОС, входящих в ее состав. Параметры ядра ОС задаются администратором системы (АС) при инсталляции ОС. После установки ОС администратор системы задает атрибуты пользователей в системе и осуществляет оперативное управление ОС. В процессе авторизации пользователей АС может задать ряд параметров их работы: права доступа, максимальный объем дискового пространства, пароль пользователя и т.д. Средства учета ресурсов ОС позволяют администратору системы накапливать для дальнейшего анализа информацию об использовании отдельными пользователями таких ресурсов, как число блоков, считанных/записанных с диска сервера, число блоков, записанных за день, продолжительность работы приложения и т.д. Утилиты работы с консолью сервера позволяют администратору системы контролировать функционирование рабочих станций, останавливать или запускать принтер,

управлять очередями заданий к принтерам, посылать сообщения пользователям ИС. Операционные системы имеют похожие, но все же отличающиеся средства оперативного управления, которые описываются в технической документации по конкретной ОС.

3.1. Параметры ядра ОС и ее инсталляция

Инсталляция (установка) ОС, как и любая инсталляция ИС или ее подсистемы, очень ответственный для АС процесс. Он включает в себя подготовку площадки и оборудования, инсталляцию файл-сервера и инсталляцию программного обеспечения рабочих станций, планирование структур каталогов (директорий), планирование пользователей и групп пользователей, планирование защиты, планирование процедур регистрации, настройку параметров. При некорректной первоначальной инсталляции ОС и неправильно заданных параметрах дальнейшая эксплуатация ИС может быть неэффективной, а в некоторых случаях - невозможной. Процессу инсталляции должен предшествовать ряд подготовительных действий.

Прежде всего администратор системы должен проверить условия эксплуатации и выполнение требований по электропитанию оборудования. В «Руководстве по эксплуатации ОС» или в документации с аналогичным названием определены конкретные требования по следующим вопросам:

- температура/влажность;
- максимальная высота, глубина, ширина оборудования;
- требования электропитания - частота тока, потребляемая мощность, рассеиваемая мощность.

Далее все аппаратные средства следует подключить к специализированным линиям питания, выделенным только для работы компьютерного оборудования. Все розетки должны быть трехпроводными заземленными, соединенными непосредственно с землей, оборудование должно быть правильно подключено к сигнальным и силовым линиям.

Далее администратору системы необходимо создать рабочие копии **дистрибутива** (поставляемой производителем ОС копии продукта). Оригинальный дистрибутив должен храниться в сейфе. При инсталляции АС должен использовать рабочие копии.

АС должен решить, делает ли он обновление существующей версии ОС (upgrade) или первичную инсталляцию. Следует внимательно просмотреть инструкции по ОС для каждой из этих операций, так как действия при их осуществлении обычно различны, зависят от конкретной ОС и может существовать не один метод обновления.

АС должен записать в рабочую таблицу (worksheet) информацию по устанавливаемому серверу. Таблица содержит следующую информацию:

- имя, марку, модель файл-сервера;
- размер памяти;
- несетевые платы - тип и настройка;
- сетевые платы - соответствующие драйверы, адрес сети, номер сети, адрес памяти, прерывание;
- плата процессора - модель, скорость работы;
- дисковые подсистемы - тип контроллера, драйверы, емкость, модель, производитель, число каналов ввода-вывода.

АС должен подготовить для работы ОС подсистемы ввода-вывода на жесткие диски.

После всех предварительных мероприятий осуществляется непосредственно процесс инсталляции с помощью утилит, предлагаемых производителем ОС (например, командой Install или Setup).

Процесс инсталляции ОС состоит в следующем: системные файлы помещаются на диск в специальную область. Загружаются дисковые, сетевые драйверы и драйверы периферийных устройств. Задаются параметры их работы. Это может выполняться либо администратором системы, например, отдельной командой Load, либо автоматически самой ОС.

После этого администратор системы загружает ядро ОС с помощью вызова команды, предлагаемой производителем, например, Server.exe, и задает основные параметры работы ядра. К этим параметрам относятся:

- имя сервера;
- имя администратора и его пароль;
- список сетевых протоколов и их настройки (например, TCP/IP);
- параметр блокирования консоли сервера;
- опция шифрования паролей в системе;
- номера очередей печати;
- команды трассировки действий ядра (например, Track On) и т. д.

Конкретный список таких параметров приводится в документации по конкретной операционной системе.

Затем администратору системы следует установить ОС на рабочих станциях ИС аналогично установке сервера.

Далее АС должен сконфигурировать (иногда и установить) сетевые платы и загрузить драйвер сетевого адаптера с указанием параметров

адреса памяти и прерывания, по которым он работает и специальную оболочку (Shell), определяющую, является обращение прикладной программы обращением к локальной ОС или к сетевой.

При инсталляции ОС создаются оглавления томов и обычно по умолчанию директории для записи файлов.

После инсталляции администратор системы должен спланировать дополнительные директории, например, прикладные директории для программ приложений ИС или директории общего пользования для промежуточного копирования файлов, группы пользователей с их правами доступа (возможно выделение для группы своей директории или тома) и создать пользователей в системе, приписав их к определенным группам. Для пользователей и групп необходимо спланировать права доступа. Для директорий и файлов АС должен спланировать атрибутную защиту.

Атрибутная защита в ОС означает присвоение определенных свойств отдельным файлам и директориям. Каждый атрибут представляется обычно по первой букве его английского названия. В различных ОС системы атрибутной защиты несколько различаются.

Далее АС должен спланировать процедуру регистрации пользователя на сервере. Фактически выполняются всегда две процедуры - сначала системная (для настройки рабочей среды всех пользователей), а затем пользовательская (для настройки среды конкретного пользователя). В системную процедуру могут входить общие приветствия всех пользователей, назначения имен (буквы английского алфавита) сетевым дискам (tap), подключение групп пользователей к различным серверам (attach). В процедурах пользовательской регистрации инициализируются параметры среды каждого пользователя, например, доступ к данному серверу только данного пользователя. Конкретные возможности процедур регистрации зависят от реализации ОС.

3.2. Дисковая подсистема и способы ее организации

Поддержка дисковой подсистемы - одна из основных задач ОС, а сама дисковая подсистема является источником проблем для администратора системы. АС может воспользоваться рядом процедур и программных продуктов для повышения производительности, и восстановления в случае сбоев дисковой подсистемы.

Современная дисковая подсистема ввода-вывода состоит из адаптеров на материнской плате HBA (Host Bus Adapter), шины (интерфейс), дискового контроллера и непосредственно жестких дисков. Совокуп-

ность этих устройств называют каналом ввода-вывода. ОС может одновременно поддерживать несколько каналов ввода-вывода, и эта опция может быть различной для разных версий ОС.

Способ кодирования, способ передачи данных по шине, ширина шины существенно влияют на скорость записи на диск.

Так как обычно операционная система может поддерживать более одного канала ввода-вывода, АС должен изучить особенности работы конкретной ОС. С увеличением числа каналов ввода-вывода обычно резко растет производительность системы.

Кроме того, производительность дисковой подсистемы зависит от типа интерфейса. Кратко рассмотрим наиболее распространенные типы интерфейсов.

IDE: контроллер располагается непосредственно на диске, благодаря чему скорость возрастает до 12 Мбит/с. Используется RLL- кодирование и сняты ограничения на объем дисковой памяти.

EIDE - Enhanced (расширенный) IDE: добавляет специальную систему адресации для дисков системы адресации AT Attachment (ATA). Система адресации ATA - это промышленный стандарт, который описывает способ адресации диска емкостью свыше 528 Мбайт с помощью BIOS компьютера. Скорость интерфейса составляет до 13,3 Мбит/с, а адаптеры на материнской плате компьютера для подключения контроллеров дисков Host Bus Adapters (HBA) позволяют подключать до 4 дисков и различные периферийные устройства.

SCSI (Small Computer Systems Interface) - это высокоскоростной параллельный интерфейс, стандартизированный ANSI. Он позволяет подключать к одной шине множество устройств, вытягивая их в цепочку. К каждому дисковому контроллеру SCSI можно присоединить до семи устройств. В настоящее время SCSI широко применяется на серверах, высокопроизводительных рабочих станциях. Скорость записи на диск достигает 600 Мбит/с.

SATA - Serial ATA - высокоскоростной последовательный интерфейс обмена данными с накопителями информации (как правило, с жесткими дисками). SATA является развитием интерфейса ATA, который после появления SATA был переименован в PATA (Parallel ATA). Обеспечивает скорость до 600 Мбит/с. SATA предполагает отказ от плоских параллельных кабелей с разъемами для двух дисков и переход к последовательной передаче данных по витой паре. Но к каждому контроллеру подключается только один диск одним кабелем. При этом переход к последовательной шине значительно упростил разводку про-

водников на материнской плате и разводку кабелей внутри корпуса компьютера. Администратору системы надо учесть, что при этом сохраняется совместимость с контроллерами ATA по регистрам и командам.

Особенностью стандарта SATA по сравнению с PATA является использование встроенной очереди команд NCQ (Native Command Queuing). NCQ позволяет устройству накапливать запросы и оптимизировать порядок их выполнения с учетом внутренней архитектуры устройства (минимизация количества перемещений головок, простоя в ожидании нужного сектора на треке). NCQ повышает производительность решения задач, связанных с произвольным чтением, обработкой данных от двух и более источников, одновременную работу нескольких программ. Также благодаря NCQ стандарт SATA предусматривает горячую замену устройств. Еще одна интересная перспектива для администратора системы - это конвергенция конкурирующих стандартов SATA и SCSI с помощью стандарта SAS (Serially Attached SCSI). Заметим, что диски SAS могут подключаться к интерфейсу SATA (но не наоборот).

Администратор системы должен изучить конкретную техническую документацию производителя по дисковой подсистеме для правильной инициализации дисковых адаптеров и контроллеров, выставления нужных адресов и прерываний, установки переключателей на платах, подсоединению шин и установке параметров CMOS компьютера.

3.3. Подготовка дисковой подсистемы, технология RAID

Любая дисковая подсистема требует подготовки для работы с ней конкретной ОС. Часто часть этой подготовки производится на заводах-производителях или компаниями-поставщиками оборудования. Подготовка дисковой подсистемы содержит три этапа: форматирование низкого уровня, организация разделов, форматирование высокого уровня.

Форматирование низкого уровня (Low level format) - это форматирование, необходимое контроллеру диска, чтобы читать его по секторам. Обычно оно выполняется на заводе-производителе дисков, и соответствующая утилита прилагается к дисковой подсистеме для случая проведения этой процедуры администратором системы. При форматировании низкого уровня обычно выполняются следующие действия:

- проводится анализ дискового пространства на наличие ошибок;
- сектора диска разбиваются на треки (дорожки) и присваиваются идентификаторы секторов;
- помечаются испорченные сектора (bad-сектора);

• устанавливается чередование секторов (interleave), когда номера секторов не совпадают с их физической последовательностью.

Чередование секторов необходимо, чтобы синхронизировать работу процессора (обработку данных) и контроллера (считывание с диска). От этого зависит скорость работы подсистемы ввода-вывода. Параметр interleave определяется ОС и дисковой подсистемой.

Администратор системы должен проводить форматирование низкого уровня в случаях, когда:

• ставятся новые дисковые подсистемы (если это не сделано производителем);

• обнаружено большое число дисковых ошибок (если средства ОС не помогают их устранить);

• необходимо поменять параметр interleave (но это опасная операция, при которой следует очень хорошо понимать, как именно обрабатываются данные контроллером и ОС и зачем нужно что-то менять);

• возникает необходимость переразметить bad-сектора.

При этом АС должен помнить, что современные дисковые контроллеры предоставляют логику опережающего считывания и отложенной записи, которые снижают потребность в оптимизации производительности методом изменения interleave.

Организация разделов - это процесс разбиения жесткого диска на логические части - партиции (partitions). Необходимость организации разделов обусловлена тем, что с данным дисковым пространством на одном компьютере может работать несколько ОС. Для каждой из них нужно свое дополнительное форматирование. Обычно при загрузке компьютера одна ОС загружается первой. Ее партиция называется первичной (primary partition). Остальная часть диска может быть использована для работы других ОС.

В начале каждого диска на нулевом треке располагается специальная таблица (partition table). В ней находится информация о том, как будет использоваться дисковое пространство согласно различным партициям. Ее потеря означает для администратора системы потерю всей информации в системе.

Форматирование высокого уровня (High level format) осуществляется средствами той ОС, которая работает в этой партиции. Во время этого форматирования создается оглавление диска и его подготовка для конкретной ОС. В различных ОС при этом выполняются различные функции.

Администратор системы должен выполнять форматирование высокого уровня, если требуется установить новый диск под управлением ОС либо есть необходимость полностью стереть информацию на диске.

АС следует помнить, что информацию после низкоуровневого форматирования восстановить нельзя! После высокоуровневого форматирования информацию восстановить можно при условии, что после его завершения не велась запись на диск.

Разбиение на тома осуществляет администратор системы средствами ОС, работающей в данной партиции, чтобы выделить логически единые части информации. Том может быть частью партиции, состоять из одной целой партиции или из нескольких партиций.

В начале каждого тома хранится специальная таблица **VDT** (Volume Definition Table). Обычно она дублируется, располагаясь в нескольких местах. В VDT находится информация о том, какие треки используются для этого тома в партиции.

Зеркалирование. Обычно в операционных системах существует поддерживаемый ими режим дублирования дисков или каналов ввода-вывода.

В режиме дублирования дисков (Disk Mirroring) на материнской плате устанавливается один адаптер HBA с подсоединенным контроллером и двумя дисками (primary и secondary). Диски полностью «зеркалируются», т. е. драйверами ОС ведется параллельная запись информации на оба диска с полным ее дублированием. Если один диск отказывает, система работает со вторым.

Средства организации зеркалирования могут быть как программными (драйверы ОС), так и аппаратными (специальные контроллеры, которые могут писать одновременно на два диска, что всегда быстрее).

Кроме того, лучше, чтобы партиции на mirror-дисках имели одинаковые размеры.

В режиме дублирования каналов ввода-вывода (Disk duplexing) дублируется весь дисковый канал ввода-вывода, т. е. устанавливаются два адаптера HBA, два диска. Это увеличивает надежность в случае отказа одного из каналов ввода-вывода.

Технология RAID

Термин RAID (Redundant Array of Independent/Inexpensive Disks) определяет любую дисковую подсистему, которая объединяет два или более стандартных физических диска в единый логический диск (дисковый массив). Такие дисковые массивы служат для повышения надеж-

ности хранения данных и для повышения скорости чтения/записи информации. Они также упрощают сопровождение дисковой подсистемы, так как АС вместо нескольких дисков обслуживает как бы один. Обычно объединение в логический диск осуществляется программно средствами ОС на базе подсистемы ввода-вывода SCSI (для небольших систем на базе SATA). Различают шесть типов (уровней) технологии RAID в зависимости от метода записи на диски: RAID 0, RAID 1 и т. д.

Драйверы для использования RAID-массивов входят в состав любой современной ОС. Windows 10 поддерживает массивы RAID 0 и RAID 1, а Windows Server 2012 - 0, 1 и 5. В состав ОС семейства Linux входит расширенный драйвер дисковых устройств, позволяющий работать с массивами RAID 0, RAID 1, RAID 4 и RAID 5. Непосредственное управление RAID-массивами происходит на уровне драйвера с помощь вызова системных функций. В зависимости от типа интерфейса, к которому подключены жесткие диски, для управления контроллером драйвер использует соответственно команды SATA или SCSI.

Существуют и аппаратные контроллеры RAID, имеющие в дополнение к контроллерам SCSI собственные процессор и память. При аппаратной реализации технологии RAID команды драйвера исполняет процессор ввода-вывода (IOP, Input/ Output Processor). IOP является центром системы RAID. IOP не только исполняет команды драйвера, но и управляет виртуализацией дисков, обработкой кэша и конфигурированием логических томов. IOP освобождает главный процессор от постоянной обработки прерываний, генерируемых при обращении к дискам, входящим в RAID-массив.

Обычно IOP – это единственный компонент подсистемы RAID, о котором знает ОС. Работа всех остальных компонентов скрыта от нее и управление ими осуществляет IOP.

Администратор системы, при возможности выбирать, должен использовать аппаратные решения для RAID-массивов.

Рассмотрим особенности наиболее часто используемых уровней RAID-массивов и укажем их недостатки и достоинства.

RAID 0 - разделение данных между дисками и чередование блоков. Система пишет блоки данных на каждый диск массива подряд (рис. 7).

Преимущества: улучшенная производительность и увеличение объема логических томов; разделение данных между дисками позволяет предотвратить ситуации, в которых происходит постоянное обращение к одному диску, в то время как другие диски простаивают.

Недостатки: отсутствие избыточности; поскольку весь массив дисков представляет собой один логический том, то при выходе из строя любого диска из строя выходит весь массив.

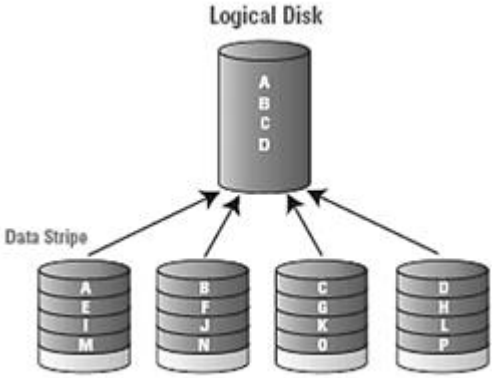

Рис. 7. Схема соединения дисков в RAID0

RAID 1 - зеркальное отображение/дуплекс. Диски зеркалируются или дублируются. Каждый байт записывается на два идентичных диска (см. рис. 8).

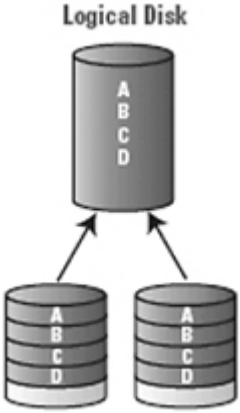

Рис. 8. Схема соединения дисков в RAID1

Преимущества: если один диск выходит из строя, другой продолжает работать. Данную концепцию наиболее просто понять и применить.

На этом уровне при наличии оптимизированных драйвера и контроллера обычно повышается скорость чтения данных, поскольку можно начать поиск данных на одном диске, в то время как другой диск обрабатывает предыдущий запрос. Однако скорость записи в этом случае замедляется, поскольку данные необходимо записать сразу на два диска. Влияние этой стратегии на производительность зависит от соотношения операций чтения/записи в используемых приложениях.

Недостатки: дороговизна, поскольку для функционирования системы требуется в 2 раз больше дискового пространства, чем это действительно необходимо. Кроме того, необходимо дополнительное место в сервере и дополнительное электропитание.

RAID 5 - разделение данных с чередованием блоков и распределенным контролем четности; разделение блоков данных между всеми дисками. Данные для контроля целостности хранятся на всех дисках (см. рис. 9).

Преимущества: операции чтения и записи могут осуществляться параллельно, что повышает скорость передачи данных. Этот тип массива высокоэффективен при работе с малыми блоками данных. Предоставляет избыточность с небольшими расходами. Эффективность пятого уровня растет в зависимости от числа дисков, используемых в массиве, поскольку объем данных для контроля целостности обычно занимает один диск, хотя хранятся эти данные на нескольких дисках одновременно.

Иногда в массивах пятого уровня используются смонтированные, но бездействующие диски. В случае возникновения неисправности у одного из дисков, входящих в массив, свободный диск может быть автоматически использован для замены поврежденного диска и восстановления данных.

Недостатки: RAID 5 менее производителен, чем RAID 0 или RAID 1 из-за необходимости рассчитывать данные для коррекции ошибок.

Существуют также и другие версии RAID: RAID 2, RAID 3, RAID 4. Они не получили широкого распространения ввиду того, что их преимущества или недостатки в том или ином виде входят в RAID 0, 1, или 5.

В заключение рассмотрения RAID различных уровней, отметим следующее: АС должен исходя из перечисленных достоинств и недостатков стратегий RAID, возможностей ОС и требований сопровождаемой ИС выбрать реализацию стратегии RAID. Иногда используются комбинированные стратегии RAID, например, RAID 10 - стратегия RAID 1 и стратегия RAID 0.

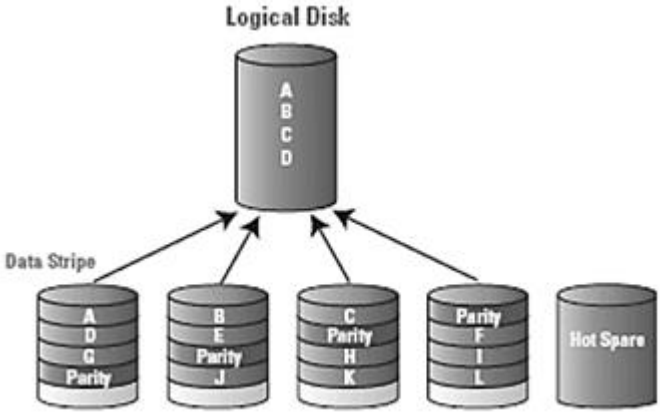

Рис. 9. Схема соединения дисков в RAID5

В современных ИС используются технологии сетей доступа к дисковым массивам - SAN, NAS и протокол iSCSI, обеспечивающий передачу команд SCSI по протоколам TCP/IP.

3.4. Вопросы администрирования файловых систем

Файл — это объект, представляющий собой данные и их атрибуты поименования и доступа. ОС организует доступ к данным не по их именам, а по адресам и соответственно должна поддерживать: таблицы преобразования имен в адреса (директории), информацию об атрибутах доступа и размерах данных, способы поиска записей в файлах (методы доступа к данным, например, по индексам). Совокупность директорий (каталогов) и других метаданных, т. е. структур данных, отслеживающих размещение файлов на диске и свободное дисковое пространство, называется **файловой системой**.

Некоторые ОС позволяют поддерживать несколько файловых систем. В этом случае под каждую из них выделяется свой том. АС должен помнить, что перед обращением к файловой системе надо смонтировать том, на котором она будет располагаться. При этой операции проводят проверку типа файловой системы тома и ее целостности, считывания системных структур данных (оглавления тома), инициализация соответствующего модуля ОС, включение файловой системы в общее пространство имен.

В различных файловых системах принят различный формат имен файлов и типы атрибутов доступа. Кроме того, каждая ОС поддерживает определенные и различные в разных файловых системах операции над файлами (открытия, закрытия, чтения/записи, поиска, обновления данных, обработки блоков переполнения). АС должен помнить, что сложные и развитые методы доступа обычно используются при реализации не универсальных ОС, а СУБД, как специализированных ОС для работы с данными. Поэтому при реализации ИС следует обратить внимание на методы доступа к данным, которые применяются в используемой СУБД и, по возможности, выбрать метод, наиболее адекватный задаче ИС.

Любая ОС имеет набор утилит для работы с файловой системой для реализации задач дефрагментации файлового пространства, шифрования данных, поддержки транзакций ОС, восстановления после сбоев. При этом АС должен учесть, что транзакции СУБД и транзакции ОС могут не соответствовать друг другу, а методы восстановления данных СУБД превосходить существующие в ОС. Кроме того, ОС, поддерживая файловые системы, не занимаются вопросами целостности данных. Это реализуется только СУБД. Задача АС правильно комбинировать имеющиеся системные средства и избегать их противоречий.

4. АДМИНИСТРИРОВАНИЕ СЕТЕВЫХ СИСТЕМ

4.1. Задачи проектирования сети

Тщательное проектирование сети является важнейшей задачей служб администратора системы. Если при проектировании сети допущены ошибки, то может возникнуть множество непредвиденных проблем в приложениях ИС. Процесс проектирования требует профессионального знания сетевых стандартов и особенностей применяемых сетевых технологий и обычно производится службами АС совместно со специализированными компаниями, имеющими лицензию на выполнение проектных работ в данной области.

Для решения задачи проектирования сетей принят трехуровневый подход (рис. 10).

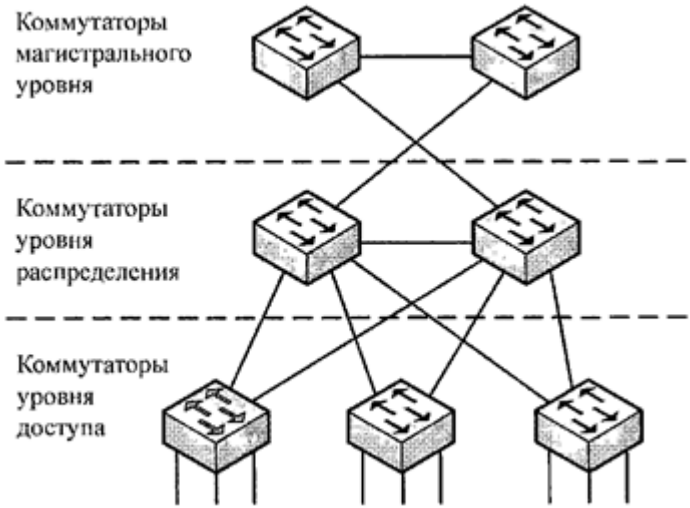

Рис. 10. Трехуровневая модель сети

В этой трехуровневой модели все сетевые устройства и соединения между ними группируются и подразделяются на следующие уровни:

- базовый (магистральный) уровень;
- уровень распределения;
- уровень доступа.

Для сетей в пределах здания эти уровни еще называют: магистральным (backbone), рабочей группы (workgroup) и настольным (standby).

Уровень доступа. На уровне доступа происходит передача данных в сеть и осуществляется входной контроль. Через этот уровень конечные пользователи получают доступ к сети. Коммутатор уровня доступа обеспечивает физический канал от интерфейса конечного пользователя до устройств, расположенных на уровне распределения. Уровень доступа использует списки доступа, которые предназначены для предотвращения несанкционированного доступа пользователей к сети. На этом уровне принимаются решения политик безопасности. Уровень доступа также предоставляет доступ к узлам удаленных сетей.

Уровень распределения определяет границы сети и обеспечивает манипуляцию пакетами в сети. Он расположен между уровнем доступа и магистральным уровнем. Его назначение состоит в отделении процессов магистрального уровня от остальной части сети. В частности, он должен создать границу входа в сеть путем использования списков доступа, определения широковещательных доменов, безопасности, управления размерами таблиц маршрутизации, обобщения (агрегации) адресов сети, распределения статических маршрутов, перераспределения динамических маршрутов, соединений с удаленными площадками и перераспределения потока информации между доменами. Таким образом, этот уровень определяет политику (стратегию) доступа к сети. Для обеспечения безопасности сети и экономии ресурсов путем предотвращения передачи нежелательных данных могут быть использованы различные политики.

Если в сети используются два или более протокола маршрутизации, например, протокол маршрутной информации RIP и протокол маршрутизации внутреннего шлюза IGRP, то обмен информацией между доменами с различными протоколами и ее перераспределение также выполняются на этом уровне.

Магистральный уровень предназначен для создания оптимизированной и надежной транспортной структуры для передачи данных с большими скоростями. Иными словами, базовый уровень должен передавать данные максимально быстро, а само устройство должно быть очень надежным и содержать самые быстрые процессоры в сети. Администратор системы должен учесть, что устройства этого уровня не должны быть загружены выполнением таких операций, как проверка списков доступа, шифрование данных, трансляция адресов и других функций, которые препятствуют коммутации пакетов с максимально возможной скоростью.

Устройства магистрального уровня должны иметь доступ к любому узлу сети. Это не означает, что они должны иметь физическую связь

непосредственно с каждым узлом, но все устройства должны быть достижимы согласно таблице маршрутизации.

На каждом уровне требуется свой тип коммутатора (табл. 4.1), который наилучшим образом решает задачи данного уровня. Функции и технические характеристики каждого коммутатора зависят от уровня, для которого предназначен этот коммутатор.

4.2. Системы сетевого администрирования и сопровождения

Для учета конфигураций, слежения за производительностью сетевой системы, защиты от несанкционированного доступа администратор системы использует специальные программные продукты - NMS (Network Management System).

Информационные системы администрирования - это программные или программно-аппаратные продукты, предназначенные для решения комплекса задач централизованного управления распределенными ИТ ресурсами, обеспечения их гарантированной доступности для пользователей в соответствии с заданными эксплуатационными требованиями. Они позволяют обеспечить управление всеми составляющими технологического, прикладного и организационно-технологического уровней информационной инфраструктуры предприятия. В данном учебном пособии не рассматриваются программно-аппаратные средства, с ними администраторам систем следует ознакомиться самостоятельно по дополнительным источникам.

Программные продукты управления ИС позволяют решать такие задачи, как:

- инвентаризация и управление учетом;
- мониторинг состояния элементов ИТ-инфраструктуры и управление производительностью;
- управление безопасностью;
- управление конфигурациями;
- управление отказами;
- автоматизация служб эксплуатации;
- оптимизация использования ИТ-ресурсов, их динамическая адаптация к меняющимся потребностям бизнеса;
- управление сервисами.

Обычно информационная система администрировании представляет собой набор модулей, предназначенных для решения различных задач. Модули могут использоваться как отдельно, так и в различных комбинациях, образуя единую систему управления. Принцип модульности

позволяет максимально гибко строить системы управления ИТ-инфраструктурами предприятий, используя только те программные модули, которые сфокусированы на решении конкретных задач управления, стоящих перед данным предприятием.

Другим важным принципом, реализующимся в системах администрирования, является проактивность управления. Обычно в системах администрирования применен аппарат настройки предупреждений и тревог (Alarm) о необычных событиях или превышениях пороговых значений метрик ИС. Администратор системы заранее оповещается о ситуации для принятия своевременных мер. Соответствующие записи о событиях в ИС создаются в сводных журналах о событиях системы администрирования (Syslog).

Большинство производителей прикладных программных средств, системных программных средств и оборудования разрабатывает и поставляет вместе с ними программные средства управления и конфигурации. Это создает проблемы при создании, внедрении и сопровождении единой системы администрирования. Кроме того, обычной является практика, когда отдельные компоненты систем управления задействуют для выполнения операций управления свои локальные ресурсы (коммуникационные протоколы, физические интерфейсы, аппаратные средства и системное программное обеспечение) и не имеют возможности интеграции на базе единой платформы управления. Их либо необходимо увязать между собой, либо реализовать на базе создаваемой системы администрирования аналогичную функциональность. Это сложный, длительный и дорогостоящий процесс, поэтому в общем случае понятие «типовая система управления» неприменимо.

В ряде случаев единственным способом решения проблемы является дополнительное прикладное программирование. Вместе с тем большинство существующих полнофункциональных систем управления реализуют принципы FCAPS.

Системы сетевого администрирования выполняют управление только сетевой подсистемой ИС, т. е. коммутаторами, маршрутизаторами, шлюзами и другими сетевыми устройствами, обычно на базе протокола SNMP. Но поскольку основной проблемой сетевого управления стала проблема управления производительностью, то современные системы сетевого администрирования часто базируются на протоколе управления NetFlow.

Особенностью всех систем, использующих протокол SNMP, является генерация избыточного сетевого трафика и, как следствие, дополнительная загрузка каналов. Кроме того, необходимо сопровождение

самой системы управления. Поэтому администратору системы следует производить расчет возможного дополнительного трафика и оценивать сложность и дополнительные затраты на сопровождение системы.

4.3. Планирование и развитие сетевой структуры

Сетевые средства развиваются чрезвычайно быстро. Так при необходимости перехода на новый протокол маршрутизации в корпоративной сети передачи данных следует рассматривать в первую очередь переход именно на протокол OSPF.

В настоящее время протокол OSPF считается более перспективным решением для использования в средних и крупных корпоративных сетях передачи данных. У него множество положительных отличий по сравнению с другими распространенными в настоящее время внутренними протоколами маршрутизации, главные из них: открытая спецификация, иерархическая архитектура, а также значительно лучшие временные параметры обнаружения и обработки изменений в топологии сети передачи. При этом появляется множество новых технологий и сетевых программных и аппаратных средств, например, WDM-мультиплексоры, протоколы BGP и MPLS, технология маршрутизации по политикам. Поэтому планирование и развитие сетевой системы ИС требует специальных постоянно обновляемых знаний от всех служб АС. Службы АС должны постоянно следить за новыми технологиями, методами диагностики и появлением новых стандартов в области сетевых технологий.

5. ACTIVE DIRECTORY WINDOWS SERVER 2012

Предлагаемые Microsoft технологии Active Directory прошли длинный путь с момента их появления в версии Windows 2000 Server. И одного продукта, называвшегося просто Active Directory (AD), в Windows Server 2012 они превратились в пять отдельных технологий. Все они предназначены для обслуживания каталогов и в качестве платформы для интеграции будущих технологий Microsoft. Четыре дополнительных роли службы Active Directory, которые предлагаются в Windows Server 20 1 2 , называются так: Active Directory Lightweight Directory Services - AD LDS (Облегченная служба Active Directory доступа к каталогам) , Active Directory Federation Services - AD FS (Служба. федерации Active Directory) , Active Directory Certificate Services - AD CS (Служба сертификатов Active Directory) и Active Directory Rights Management Services - AD RMS (Служба управления правами Active Directory) .

5.1. Эволюция службы каталогов

Служба каталогов в той или иной форме существовала с самого начала эпохи компьютеров - для обычного поиска файлов и для аутентификации в реализациях производственных сетей. Служба каталогов предоставляет подробную информацию о пользователях или объектах сети, примерно так же, как телефонная книга позволяет найти номер телефона по известной фамилии. Например, объект пользователя в службе каталогов может содержать номер телефона, адрес электронной почты, название подразделения и еще столько других атрибутов, сколько пожелает системный администратор.

Службы каталогов часто называют "белыми страницами" сети. Они обеспечивают определение и администрирование пользователей и объектов. Первые электронные каталоги были созданы вскоре после изобретения цифровых компьютеров и применялись для аутентификации пользователей и управления доступом к ресурсам. С расширением международной сети и ростом совместного использования компьютеров в функции каталогов было включено хранение основной контактной информации о пользователях. Примерами ранних каталогов могут служить MVS PROFS (IBM), база регистрационных данных Grapevine и WHOIS. Вскоре появились специализированные службы каталогов для специального поиска и ведения контактной информации для конкретных программных продуктов. Доступ к таким каталогам был возможен только с помощью специальных методов, а область их применения была ограниченной.

Приложениями, использующими эти типы каталогов, были такие программы, как Novell GroupWise Directory, Lotus Notes и файл /etc/aliases утилиты sendmail в UNIX. Дальнейшее развитие крупномасштабных служб каталогов для предприятий возглавила компания Novell, выпустив в начале девяностых годов прошлого века службу каталогов Novell Directory Services (NDS). Она была принята организациями NetWare, а затем в нее была включена поддержка смешанных сред NetWare/NT. Линейная структура доменов NT и отсутствие синхронизации и взаимодействия этих двух сред заставила многие организации перейти на использование NDS в качестве реализации службы каталогов. Именно эти недостатки NT были основной причиной выпуска службы AD DS компанией Microsoft.

Разработка облегченного протокола доступа к каталогам (Lightweight Directory Access Protocol - LDAP) была вызвана ростом сети Интернета и необходимостью более тесного взаимодействия и строгой стандартизации. Этот общепринятый метод доступа к информации каталогов и ее модификации использовал все возможности протокола TCP /IP, оказался надежным и функциональным, и для его применения были разработаны новые реализации служб каталогов. Сама служба AD DS разрабатывалась так, чтобы соответствовать стандарту LDAP.

Основные характеристики доменной службы Active Directory

Центральную роль в AD DS играют пять ключевых компонентов. Из-за требований совместимости новых служб каталогов со стандартами Интернета в существующие реализации были внесены соответствующие изменения и уделено больше внимания перечисленным ниже областям.

- **Совместимость с TCP /IP.** В отличие от ряда специализированных протоколов вроде IPX/SPX и NetBEUI, протокол TCP /IP с самого начала создавался межплатформенным. Последующее принятие TCP /IP в качестве Интернет-стандарта для обмена данными сделало его одним из лидеров в мире протоколов и, по сути, превратило в обязательный протокол для операционных систем уровня предприятия. В AD DS и Windows Server 20 1 2 стек протоколов TCP /IP используется в качестве основного метода для обмена данными.

- **Поддержка протокола LDAP.** Протокол LDAP (Lightweight Directory Access Protocol - облегченный протокол доступа к каталогам) был разработан в качестве стандартного Интернет-протокола для доступа к каталогам. Он применяется для обновления и запросов данных,

хранящихся в каталогах. Служба AD DS непосредственно поддерживает LDAP.

• **Поддержка системы доменных имен.** Система доменных имен (Domain Name System - DNS) была создана для преобразования упрощенных имен, понятных людям (таких как www.cco.com), в IP-адреса, понятные компьютерам (вроде 12.222.165.154). В AD DS она поддерживается и даже требуется для нормальной работы.

• **Поддержка безопасности.** Поддержка безопасности в соответствии со стандартами Интернета чрезвычайно важна для бесперебойного функционирования среды, к которой подключены миллионы компьютеров по всему миру. Отсутствие надежных средств защиты привлекает хакеров, поэтому в Windows Server 201 2 и AD DS средства безопасности были значительно расширены. Так, в Windows Server 201 2 и AD DS была встроена непосредственная поддержка IPSec, Kerberos, центров сертификации и шифрования с помощью протокола защищенных сокетов (Secure Sockets Layer - SSL).

• **Легкость администрирования**. При реализации мощных служб каталогов удобству администрирования и конфигурирования среды часто не уделяется должного внимания. А зря: этот аспект очень сильно влияет на общую стоимость эксплуатации. AD DS и Windows Server 2012 специально спроектированы так, чтобы ими было удобно пользоваться, и чтобы на освоение новой среды тратилось как можно меньше усилий. Для улучшения администрирования AD DS в Windows Server 2012 добавлены компоненты Active Directory Administration Center (Центр администрирования Active Directory), Active Directory Web Services (Веб-служба Active Directory) и модуль для администрирования Active Directory из оболочки Windows PowerShell. Они значительно усовершенствованы по сравнению с версиями из Windows Server 2008 и Windows Server 2008 R2. Поддержка PowerShell в Windows Server 2012 AD DS позволяет эффективнее справляться с возможными проблемами и полностью автоматически управлять работой контроллеров доменов и целых лесов из командной строки. Кроме того, в Windows Server 2012 улучшена поддержка виртуализации контроллеров доменов - эта концепция будет подробно рассмотрена в настоящей главе.

5.2. Структура службы ADDS

Логическая структура AD DS позволяет выбрать ее размер и для небольших офисов, и для крупных международных организаций. Встроенная возможность детализации обязанностей, связанных с админи-

стрированием, позволяет делегировать управление группам пользователей или отдельным пользователям. Предоставление прав на администрирование по принципу "все или ничего" осталось в прошлом. AD DS в основном следует модели каталогов X.500, но обладает и рядом собственных характеристик. Многие уже привыкли к лесам и деревьям AD DS, а некоторые ограничения, которые имелись в предыдущих версиях AD DS, теперь устранены. Чтобы понять AD DS, сначала нужно разобраться в ее основных структурных компонентах.

Домен AD DS

Домен AD DS, традиционно изображаемый в виде треугольника (рис. 11), является главной логической границей AD DS.

Рис. 11. Обозначение домена

В некотором смысле структура домена AD DS во многом схожа с более ранней структурой доменов Windows NT 4.0, которую он заменил. Информация о пользователях и компьютерах хранится и обрабатывается внутри домена. Однако появилось несколько серьезных изменений в структуре домена и в способе его взаимодействия с другими доменами в структуре AD DS.

Домены в AD DS разграничивают административную безопасность для объектов и содержат собственные политики безопасности. Важно помнить, что домены представляют собой логическую организацию объектов и могут охватывать несколько физических местоположений. Значит, уже не нужно создавать множество доменов для различных удаленных офисов или вычислительных центров, поскольку вопросы репликации и безопасности теперь гораздо удобнее решать с помощью сайтов AD DS или контроллеров RODC.

Деревья доменов AD DS

Дерево AD DS состоит из нескольких доменов, соединенных двунаправленными транзитивными отношениями доверия. Каждый домен в дереве AD DS использует общую схему и глобальный каталог. Корневым доменом дерева ADDS является companyabc.com, а

asia.companyabc.com и europe.companyabc. com — его поддомены (см. рис. 12).

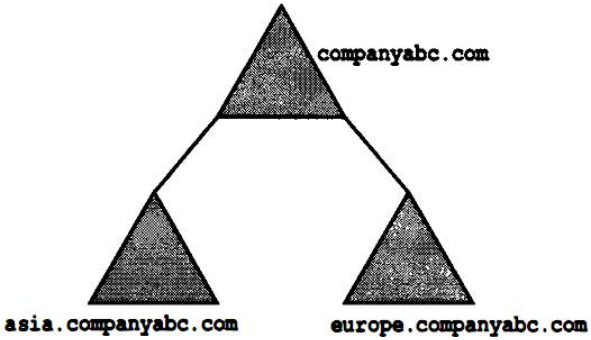

Рис. 12. Дерево ADDSc поддоменами

Транзитивное отношение доверия устанавливается автоматически. Оно означает, что если домен asia доверяет корневому домену companyabc, и домен europe также доверяет домену companyabc, то домен asia доверяет и домену europe. Доверительные отношения пронизывают всю доменную структуру.

Транзитивность отношений доверия в среде AD DS не означает, что правами доступа могут пользоваться все пользователи или даже администраторы других доменов. Доверительные отношения лишь обеспечивают путь от одного домена к другому. По умолчанию никакие права доступа от одного транзитивного домена к другому не передаются. Чтобы пользователи или администраторы другого домена могли получать доступ к ресурсам данного домена, его администратор должен предоставить им соответствующие права.

Все входящие в состав дерева домены используют общее пространство имен (в данном примере — companyabc. com), но содержат механизмы защиты для разграничения доступа из других доменов. То есть администратор домена europe может иметь относительный контроль над всем его доменом, а пользователи из домена asia или companyabc могут не располагать полномочиями на доступ к его ресурсам. Однако при желании администратор europe может разрешить каким-то группам пользователей из других доменов обращаться к ресурсам его домена. Права на администрирование могут назначаться очень избирательно.

Кстати, возможность создания поддоменов в лесе, как на рис. 12, не означает, что это обязательно имеет смысл. Многие среды замечательно

обслуживаются одним доменом для всех их ресурсов, разбросанных по миру. А после создания поддоменов становится не очень легко перемещать ресурсы.

Леса в AD DS

Лесами (forest) в AD DS называются группы связанных между собой деревьев доменов. Неявные отношения доверия объединяют корни всех деревьев в один общий лес.

Связями, объединяющими все домены и деревья доменов в общий лес, служит наличие общей схемы и общего глобального каталога. Хотя доменам и деревья доменов в этом лесу вовсе не обязательно использовать общее пространство имен. Например, домены microsoft. internal и msnbc. internal теоретически могут являться частями одного и того же леса, но при этом иметь собственные раздельные пространства имен.

Леса служат основной границей организационной безопасности в AD DS, и потому предполагают наличие некоторой степени доверия к администраторам всех входящих в их состав доменов.

Режимы аутентификации в AD DS

В Windows NT 4.0 для аутентификации применялась подсистема под названием NTLM (NT LAN Manager — диспетчер локальной сети NT). В ней зашифрованный пароль пересылался по сети в виде хеша. Ее недостатком было то, что любой желающий мог отслеживать в сети передаваемые хеши, собирать их и затем расшифровывать с помощью сторонних средств взлома паролей по словарю или "грубой силой".

Во всех версиях Windows Server после Windows 2000 стала применяться подсистема аутентификации Kerberos. Kerberos не пересылает информацию пароля по сети и поэтому гораздо безопаснее NTLM.

Обзор функциональных уровней в Windows Server 2012 AD DS

В Windows 2000 Server и Windows Server 2003 поддерживались собственные функциональные уровни для обеспечения обратной совместимости с доменами предыдущих версий. Аналогично Windows Server 2012 содержит функциональные уровни для поддержки совместимости.

По умолчанию при выполнении свежей установки Active Directory на контроллерах домена Windows Server 2012 автоматически создается домен Windows Server 2012 и функциональные уровни леса. Но при установке контроллеров домена Windows Server 2012 в существующем устаревшем домене можно выбрать функциональный уровень, с которого начнет работать лес. Если лес Active Directory уже существует, его

функциональный уровень можно поднять до Windows Server 2012 следующим образом.

• Проверьте, что все контроллеры доменов в лесе обновлены до Windows Server 2012 или заменены новыми контроллерами Windows Server 2012.

• В диспетчере серверов на контроллере домена выберите в меню Tools (Сервис) пункт Active Directory Domains and Trusts (Active Directory — домены и доверие).

• В левой панели щелкните правой кнопкой мыши на имени нужного домена и выберите в контекстном меню пункт Raise Domain Functional Level (Повысить функциональный уровень домена).

• В окне Raise Domain Functional Level выберите вариант Windows Server 2012 и щелкните на кнопке Raise (Повысить).

• Два раза щелкните на кнопках OK, чтобы завершить выполнение задачи.

• Повторите шаги 1-5 для всех остальных доменов в лесе.

• Выполните такие же шаги для корневого дерева леса, но на этот раз выберите вариант Raise Forest Functional Level (Повысить функциональный уровень леса) и следуйте выводимым подсказкам.

После повышения уровня всех доменов и леса до Windows Server 2012 в лесе можно будет использовать новейшие функциональные средства AD DS. Важно помнить, что до выполнения этой процедуры в среде со смешанными режимами Windows Server 2012 работает в более низком режиме совместимости.

5.3. Компоненты ADDS, отношения в доменах

Основные компоненты AD DS изначально разрабатывались с целью легкости их настройки и защиты. AD DS и все ее составляющие физически размещаются в одном файле базы данных, но содержат самые разнообразные объекты и их атрибуты. Многие из описываемых характеристик наверняка известны тем, кто знаком с другими службами каталогов, но среди них есть и новинки.

Связь AD DS с моделью X.500

AD DS в основном следует информационной модели службы каталогов X.500, которая определяет службу каталогов через распределенный подход, определенный информационным деревом каталога (Directory Information Tree — DIT). Это дерево логически разбивает структуру службы каталогов в уже знакомый формат: *имя_сервера.имя_поддомена.имя_домена.com*

В модели X.500 информация каталога хранится в иерархической структуре, получившей название агентов системы каталогов (Directory System Agent — DSA). Технология AD DS основана на многих базовых принципах определения X.500, но сама AD DS не совместима с реализациями X.500, поскольку протокол X.500 основан на модели OSI, которая неэффективно работает с протоколом TCP/IP, используемым AD DS.

Концепция схемы AD DS

Схемой в AD DS называется набор определений для всех типов имеющихся в каталоге объектов и связанных с ними атрибутов. Именно схема задает способ хранения и представления в AD DS данных обо всех пользователях, компьютерах и других объектах, чтобы они имели стандартный вид по всей структуре AD DS. Она защищается с помощью списков управления разграничением доступа (Discretionary Access Control List - DACL) и отвечает за предоставление возможных атрибутов для каждого объекта в AD DS. По сути, схема представляет собой базовое определение самого каталога и является основой функционирования среды домена. При делегировании прав на управление схемой избранной группе администраторов следует соблюдать осторожность, поскольку вносимые в схему изменения влияют на всю среду AD DS.

Объекты схемы

Сохраняемые внутри структуры AD DS элементы, вроде пользователей, принтеров, компьютеров и сайтов, в рамках схемы называются объектами. У каждого такого объекта имеется свой список атрибутов, которые определяют его характеристики и могут применяться для его поиска. Например, объект пользователя для работника по имени Иван Петров будет иметь атрибут FirstName (Имя) со значением "Иван" и атрибут LastName (Фамилия) со значением "Петров". Помимо этих, могут назначаться и другие атрибуты: название подразделения, адрес электронной почты и многое другое. Пользователи, которые выполняют поиск информации в AD DS, смогут строить на основе этой информации свои запросы и находить, например, всех пользователей, которые работают в отделе сбыта.

Расширение схемы

Одним из главных преимуществ структуры AD DS является возможность напрямую изменять и расширять схему, включая в нее произвольные атрибуты. Обычно расширение набора атрибутов происходит во

время установки системы Microsoft Exchange Server, когда схема значительно увеличивается в размере. При обновлении с Windows Server 2003 или Windows Server 2008 AD до Windows Server 2012 AD DS тоже происходит расширение схемы, и в нее добавляются атрибуты, характерные для Windows Server 2012. Многие сторонние продукты также выполняют свои расширения схемы, которые позволяют отображать различные типы информации из каталога. Учтите, что расширения схемы следует выполнять только в случаях абсолютной необходимости, поскольку неаккуратное расширение может внести хаос в среду AD DS.

Внесение изменений в схему с помощью утилиты ADSI

Для просмотра всех деталей схемы AD DS существует интересный способ - использование утилиты ADSIEdit (AD DS Service Interfaces - интерфейсы службы AD DS). Эта утилита разработана для упрощения доступа к AD DS, однако она позволяет просматривать и любые другие совместимые внешние каталоги LDAP. Она позволяет просматривать, удалять и изменять атрибуты схемы. Соблюдайте предельную осторожность при внесении изменений в схему, поскольку проблемы в схеме сложно устранить.

5.4. Определение организационных единиц домена

Согласно приведённому в RFC-документе определению стандарта LDAP, организационные единицы (Organizational Unit - OU) представляют собой контейнеры, которые позволяют логически хранить информацию каталогов и назначать ей в AD DS адреса с помощью протокола LDAP. В AD DS организационные единицы являются основным методом организации информации о пользователях, компьютерах и других объектах в более удобном для понимания виде. На рис. 13 приведена корневая организационная единица, в которую вложены три других организационных единицы - отдел маркетинга, отдел информационных технологий и отдел исследований. Подобное вложение одних организационных единиц в другие позволяет организациям распределять информацию о пользователях в несколько контейнеров, что облегчает просмотр и администрирование сетевых ресурсов.

Понятно, что организационные единицы могут делиться и далее на организационные единицы отдельных ресурсов для упрощения их организации и делегирования прав на их администрирование. Далеко расположенные офисы могут иметь собственные организационные единицы для локального администрирования. Однако организационные единицы

следует создавать лишь тогда, когда в организации необходимо делегировать администрирование другому коллективу администраторов. Если одно и то же лицо или группа лиц осуществляет административное управление всем доменом, то нет смысла усложнять среду, добавляя в нее организационные единицы. Слишком большое количество организационных единиц может негативно влиять на групповые политики, входную регистрацию и другие факторы.

Рис. 13. Структура организационных единиц

Некоторые администраторы пытаются скопировать в структуре домена AD DS политические границы организации, рисуя сначала черновики, а затем довольно скоро привлекая к этому процессу менеджеров. В результате для каждого отдела создаются отдельные поддомены с множеством уровней. Однако структура AD DS позволяет добиться такой же степени административного дробления и без создания множества поддоменов. При проектировании доменов рекомендуется начать с единственного домена и добавлять новые домены только в случае крайней необходимости.

Организационные единицы можно структурировать так, чтобы отдельные подразделения имели различные уровни административного контроля над своими пользователями.

Например, секретарю технического отдела можно поручить управление изменением паролей пользователей в рамках его отдела. Другое преимущества применении организационных единиц в таких ситуациях состоит в том, что пользователей можно легко перетаскивать мышью из одной OU в другую. Например, при переводе пользователя из одного подразделения в другое его перемещение в новое OU выполняется очень просто.

Важно иметь в виду, что структуру OU можно изменить в любой момент, когда администратор сочтет нужным провести структурные изменения. Обычно при этом накладываются дополнительные ограничения - после отображения групповых политик и административных прав, назначенных структуре OU. Это предоставляет AD DS дополнительное преимущества - легкость исправления ошибок, допущенных при проектировании OU, поскольку изменения можно внести в любой момент.

5.5. Роль DNS и безопасность в ADDS

Когда в Microsoft начали разрабатывать AD DS, главным приоритетом было обеспечение ее полной совместимости с системой доменных имен (Domain Name System - DNS).

В результате AD DS была создана не только полностью совместимой с DNS, но и настолько интегрированной с ней, что не может без нее существовать.

Полностью соответствуя стандартам, принятым для DNS, служба AD DS расширяет стандартный набор средств DNS и предлагает новые возможности, вроде DNS, интегрированной в AD, что существенно упрощает администрирование для сред DNS. Кроме того, AD DS может легко адаптироваться к существующей сторонней системе DNS, например, UNIX BIND, при условии, что используется версия BIND 8.2.x или выше.

Из-за важности роли DNS в Windows Server 2012 AD DS полное понимание всех аспектов DNS является обязательным.

Концепции пространств имен DNS

Пространство имен DNS представляет собой ограниченную логическую область, образуемую именем DNS и его поддоменами. Например, имена europe.companyabc.com, asia.companyabc.com и companyabc.com являются частями одного и того же непрерывного пространства имен DNS. Пространство имен DNS в AD DS может быть опубликовано в Интернете, наподобие microsoft.com или msn.com, или скрыто от всех, что зависит стратегии и требований безопасности тех, кто ее реализует.

• **Внешние (опубликованные) пространства имен.** Имя DNS, распознаваемое из любого места в Интернете, называется опубликованным или внешним пространством имен. Подобные пространства имен раньше часто применялись в организациях, которые для полного удобства хотели, чтобы их обычно используемое в Интернете доменное имя представляло структуру AD DS. Однако практика показывает, что такая модель не очень удобна. Безопасность играет все более важную роль, и поэтому систему DNS следует устанавливать отдельным компонентом: наличие внутренних зон AD DNS с возможностью доступа из Интернета не рекомендуется.

• **Внутренние (скрытые) пространства имен.** Для многих организаций публикация внутренней доменной структуры недопустима с точки зрения безопасности. Такие организации могут определять схемы AD DS с внутренним пространством имен, не доступным для чтения из Интернета. Например, компания может иметь внешнее пространство имен DNS cco.com и структуру AD DS, соответствующую пространству имен cco.internal или какому-то другому. Тем более что для внутренних пространств имен годится любая комбинация, ведь в них нет никаких ограничений на использование доменов .com, .net, .gov и т.д. При желании домен можно даже назвать ilovemydomain.verymuch (хотя, конечно, это не рекомендуется). Из практических соображений для частной адресации специально зарезервировано пространство имен .internal, и во многих случаях оно очень удобно для использования.

Динамическая служба доменных имен

Динамическая служба доменных имен (Dynamic Domain Name System - DDNS) разработана как средство для устранения проблемы, связанной с необходимостью ручного обновления таблиц DNS после внесения изменений. В Windows Server 2012 она автоматически обновляет таблицы DNS на основе регистраций и может работать в сочетании с протоколом DHCP, автоматически обрабатывая изменения при добавлении и удалении клиентов из сетевой инфраструктуры. DDNS не обязательна для корректной работы AD DS, но она существенно облегчает администрирование по сравнению со старыми ручными методами.

Сравнение стандартных зон DNS и зон DNS, интегрированных с AD

Стандартная DNS хранит все записи с именами в текстовом файле и поддерживает его в актуальном состоянии с помощью динамических

обновлений. Если вы привыкли работать с UNIX BIND DNS или с какой-то другой стандартной разновидностью DNS, то точно так же ведет себя стандартная DNS в Windows Server 2012.

AD DS способна работать и с другими реализациями DNS, позволяя администраторам интегрировать их. В таком случае сами зоны DNS существуют в AD DS в виде объектов, что делает возможным их автоматический перепое. Трафик репликации DNS разгружает трафик AD DS, и записи DNS сохраняются внутри объектов в каталоге. В реализации AD DS в Windows Server 2012 зоны DNS, интегрированные с AD, оптимизируются за счет их сохранения в разделе приложений, что позволяет уменьшить объем трафика репликации и повысить производительность системы.

Сосуществование AD DS DNS со сторонними DNS

Зачастую локальные администраторы сомневаются, стоит ли развертывать AD DS, из-за того, что хотят сохранить собственные реализации сторонних DNS - обычно это UNIX BIND. Windows Server 2012 DNS может сосуществовать в таких средах, если DNS поддерживает динамические обновления и записи SRV (BIND версии 8.2.x или выше). Такие ситуации возникают совсем не редко, поскольку персонал в IT -отделах зачастую делится на группы приверженцы Microsoft и группы приверженцы UNIX, у каждой из которых имеется своя идеология и собственные планы. Способность Windows Server 2012 спокойно сосуществовать в подобных средах играет очень важную роль.

Безопасность AD DS

Цель системы безопасности Active Directory - защита ценных сетевых активов. Кроме того, на систему безопасности самой Windows Server 2012 повлияла предпринятая Microsoft инициатива по обеспечению безопасности компьютерных технологий, которая сместила основной акцент при разработке продуктов Microsoft на их защиту. Сейчас Microsoft уделяет безопасности своих продуктов столько внимания, сколько не уделяла никогда ранее, и перед выпуском подвергает всю новую функциональность специальному тестированию на предмет защищенности.

Аутентификация Kerberos

Механизм Kerberos был разработан в Массачусетском Технологическом институте как безопасный метод для аутентификации пользовате-

лей без пересылки их пароля по сети ни в зашифрованном, ни в незашифрованном виде. Такая возможность передачи пароля значительно уменьшает опасность хищения пароля, т.к. злоумышленники не могут получить копию пароля во время его передачи по сети и расшифровать его с применением приемов "грубой силы".

Схема функционирования Kerberos довольно сложна, но, в сущности, сводится к следующему: компьютер отправляет клиенту, которому требуется пройти аутентификацию, пакет с информацией. В этом пакете содержится "загадка", правильный ответ на которую может быть получен только с помощью подлинных учетных данных пользователя. Пользователь прилагает к этой загадке "ответ" и отсылает ее обратно серверу. Если ответ был сформирован с помощью правильного пароля, пользователь проходит аутентификацию. Хотя этот вид аутентификации применяется в Windows Server 2012, это не собственная разработка Microsoft, а Интернет-стандарт.

Дополнительные меры защиты

Реализации AD DS безопасны настолько, насколько безопасна среда Windows Server 2012, в которой они работают. Безопасность структуры AD DS можно усилить с помощью дополнительных мер предосторожности, вроде безопасного обмена данными между серверами по протоколу IPSec, использования смарт-карт или других технологий шифрования. Кроме того, пользовательскую среду можно защитить параметрами групповых политик для ограничения паролей пользователей, защиты доменов и прав доступа при входной регистрации.

6. ПРОЕКТИРОВАНИЕ СТРУКТУРЫ ACTIVE DIRECTORY

Прежде чем принимать какие-либо решения по структуре доменов, важно сначала хорошо разобраться в структуре и функциях доменов в AD DS. В последних версиях Windows Server появились серьезные изменения, требующие повторного ознакомления с процессом создания доменов. Кроме того, опыт реального проектирования доменов AD привел к изменению некоторых исходных положений.

6.1. Структура доменов ADDS

Доверительные отношения между доменами

Доверительные отношения между доменами различных лесов раньше требовали явного определения для каждого домена. Это приводило к экспоненциальному накоплению доверительных отношений и сложности управления ими. В Windows Server 2003 и более поздних версиях возможности доверительных отношений были расширены транзитивными доверительными отношениями с автоматическим созданием путей "вверх и вниз по дереву".

Такие доверительные отношения, гораздо более понятные и удобные для устранения неполадок, значительно улучшили управляемость сетей Windows.

Транзитивные отношения доверия

Двунаправленные транзитивные отношения доверия устанавливаются автоматически при создании поддоменов или добавлении в лес AD DS нового дерева доменов.

Транзитивные отношения обычно являются двунаправленными, когда каждый домен доверяет другим доменам. То есть пользователи каждого домена имеют доступ к ресурсам, например, принтерам или серверам, в другом домене, если им явно предоставлены права в этом домене. Помните, что существование доверительных отношений между двумя доменами не означает, что пользователи, одного домена, автоматически получают доступ ко всем ресурсам другого домена: это лишь первый шаг для получения доступа. Для этого им должно быть назначены соответствующие права доступа.

Явные отношения доверия

Явные отношениями доверия называются такие отношения, которые устанавливаются вручную - подобно тому, как это делалось в Windows

NT. Такие отношения могут устанавливаться, например, для объединения двух несвязанных деревьев доменов в один лес.

Явные отношения доверия являются однонаправленными, но из двух таких отношений можно составить двунаправленное.

На рис. 13 показан пример задания явного доверия между доменом companyabc и доменом companyxyz, которое объединяет их в единую структуру леса.

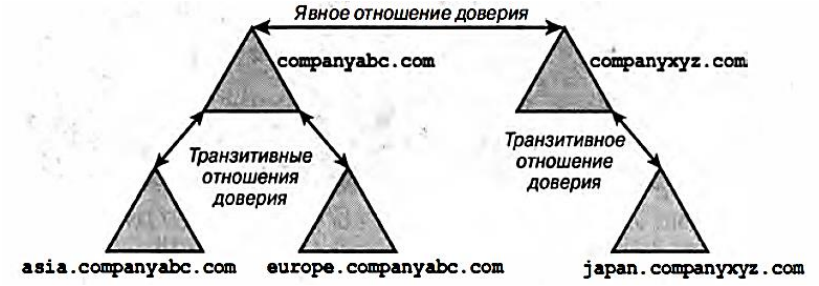

Рис. 13. Явное доверие между двумя деревьями доменов

Когда явное доверие устанавливается для направления потока доверительных отношений от одного поддомена к другому, оно называется прямым доверием. Прямые доверия просто ускоряют аутентификацию, устраняя необходимость в перемещениях по дереву вверх и вниз.

На рис. 14 показано, что при наличии транзитивного доверия между доменами asia.companyabc.com и europe.companyabc.com создано также прямое отношение доверия для уменьшения времени аутентификации при обращениях между двумя поддоменами данной организации.

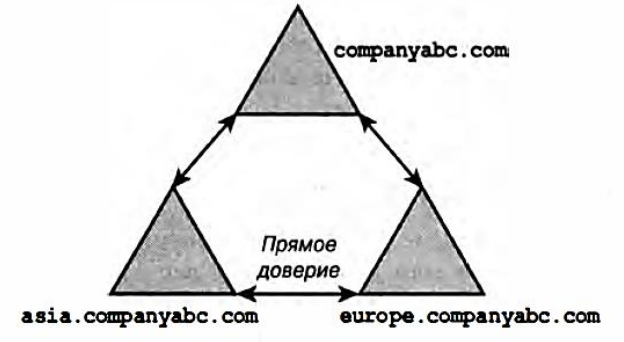

Рис. 14. Прямое доверие между двумя поддоменами леса

Еще одним возможным способом применения явных отношений доверия является обеспечение связности между лесом AD DS и внешним доменом. Подобные типы явно определенных отношений называются внешними отношениями доверия и позволяют различным лесам совместно использовать информацию без фактического объединения данных схемы или глобальных каталогов.

6.2. Модели доменов

При проектировании доменной структуры в AD DS достаточно следовать такому базовому принципу: начать с самого простого варианта и расширять его только при необходимости в удовлетворении какого-то конкретного требования. Этот принцип вообще важно соблюдать при проектировании любых компонентов AD DS. При проектировании доменов он означает, что всегда нужно начинать с создания одного домена и затем добавлять другие, если того потребуют сложившиеся в организации условия. Следование этой простой философии в процессе проектирования существенно сократит объем возможных трудностей.

При проектировании AD DS необходимо также рассмотреть вариант применении общей схемы для диаграмм. Технология Active Directory разработана гибкой и позволяет по-разному реализовать службы каталогов.

Теперь можно выбирать из множества доступных моделей проектирования, в зависимости от индивидуальных потребностей организаций. К числу главных моделей относятся:

- модель с единственным доменом;
- модель с несколькими доменами;
- модель с несколькими деревьями в одном лесе;
- модель с федеративными лесами;
- модель с выделенным корнем;
- модель с фиктивным доменом;
- модель специализированного домена.

В реальности не все структуры AD попадают в одну из этих категорий, поскольку существует масса возможных вариаций и разновидностей структуры AD. Но большинство доменных структур либо относятся к одной из этих категорий, либо представляют собой гибриды со свойствами двух различных моделей

Модель с единственным доменом

Наиболее простой из всех структур AD DS является модель с единственным доменом.

Структура домена такого типа обладает главным преимуществом по сравнению с другими моделями - простотой. Одна граница безопасности определяет границы домена, и все объекты размещаются внутри этой границы. Устанавливать доверительные отношения с другими доменами не нужно, а реализовывать технологии вроде групповых политик для простых структур гораздо проще. Эта модель годится для большинства организаций, поскольку AD DS была упрощена, а ее возможность охватывать множество физических границ - значительно улучшена.

Выбор модели с единственным доменом

Модель с единственным доменом идеально подходит для многих организаций, а с учетом возможных модификаций - для очень многих. Структура с единственным доменом обладает несколькими преимуществами, главным из которых является простота. Любой администратор или инженер с опытом реальной работы согласится с тем, что чаще всего самое простое решение является наилучшим. Чрезмерное усложнение архитектуры системы привносит потенциальный риск и усложняет устранение неполадок в этих системах.

Следовательно, объединение сложных доменных структур в более простую структуру с единственным доменом AD DS позволяет уменьшить расходы на администрирование и минимизировать связанные с этим проблемы.

Еще одним преимуществом в случае создания структуры с единственным доменом является возможность централизованного администрирования. Многие организации с сильной централизованной IT-структурой стремятся объединить контроль над всеми информационными структурами и пользователями. AD DS и, в частности, модель с единственным доменом, обеспечивает высокий уровень административного управления и возможность делегировать задачи администраторам более низкого уровня. Это стало серьезным стимулом для использования AD DS.

Но не все структуры AD DS могут состоять из единственного домена, и некоторые факторы могут ограничить применение структуры с единственным доменом. При наличии в организации таких факторов может возникнуть необходимость в расширении доменной модели, чтобы она содержала в лесе другие домены и другие доменные структуры.

Например, единая граница безопасности, образуемая одним доменом, может оказаться не совсем такой, какая необходима организации.

Для делегирования прав на администрирование элементов безопасности могут использоваться организационные единицы, но члены группы Domain Admins (Администраторы домена) все равно смогут перекрывать права доступа в разных OU. Если контуры безопасности внутри организации должны иметь точные границы, то единый домен может оказаться неподходящим вариантом. Например, если отдел кадров требует, чтобы ни у кого из пользователей IT -отдела не было доступа к ресурсам его среды, то структуру домена придется расширить в соответствии с этим дополнительным требованием безопасности.

Еще одним недостатком модели с единственным доменом является то, что при наличии в лесу единственного домена компьютер с ролью эталона схемы должен находиться в этом же домене. То есть эталон схемы должен располагаться в домене, в котором содержатся все пользовательские учетные записи. Хотя доступ к эталону схемы можно жестко контролировать административным путем, риск раскрытия эталона повышается, когда роль эталона схемы размещена в пользовательском домене.

Модель с несколькими доменами

По различным причинам в организациях может возникать необходимость в добавлении в их среду более одного домена, но при сохранении функциональных возможностей, присущих единственному лесу. В таких случаях в лес можно добавить один или более доменов.

По умолчанию между поддоменами и доменами в AD DS существуют двусторонние транзитивные отношения доверия. Однако это отнюдь не означает, что членам других доменов автоматически разрешен доступ к ресурсам. Пользователь из поддомена B не получает автоматически никаких прав в домене A; эти права должны обязательно предоставляться явным образом через соответствующие группы. Понимание этого принципа поможет в определении логики добавления доменов.

Как уже было сказано, при проектировании структуры AD DS в Windows Server 2012 рекомендуется всегда сначала создать один домен и добавлять дополнительные домены только в случае крайней необходимости. Причинами возникновения такой необходимости могут быть перечисленные ниже факторы.

• **Децентрализованное администрирование.** Если в различных филиалах в основном применяются собственные структуры информационных технологий, и руководство не планирует объединять их в одну централизованную модель, то идеальным вариантом будет добавление нескольких взаимосвязанных доменов. Каждый домен в таком случае

будет играть роль границы безопасности для большинства видов деятельности и не позволять администрирование за своими пределами. Однако такой подход чреват проявлением ограничений, которые присуши средам с множеством доменов. Другими словами, лучше все-таки попытаться централизовать администрирование перед развертыванием AD DS, поскольку это даст гораздо больший набор преимуществ AD. Также лучше организовывать администрирование по границам организационных единиц, а не по доменам, поэтому данный вариант следует рассматривать в первую очередь.

• **Географические ограничения.** Если различные филиалы компании соединяются очень медленными или ненадежными каналами связи или если они находятся на больших расстояниях друг от друга, распределение пользователей по отдельным доменам может оказаться целесообразным решением. Такой подход позволит ограничить объем репликации между доменами, а также упростить сопровождение в рабочее время для офисов, находящихся в удаленных часовых поясах. Однако имейте в виду, что создавать множество доменов только из-за низкой скорости каналов связи между офисами вовсе необязательно, поскольку в Windows Server 2012 AD DS для сокращения объема трафика, подлежащего передаче по медленным каналам, используется концепция сайтов AD DS. Главной причиной для создания множества доменов при географической удаленности офисов является необходимость обеспечения гибкости в администрировании.

• **Уникальное пространство имен DNS.** Если в каких-то подразделениях организации нужно использовать для AD DS собственное зарегистрированное в Интернете пространство имен, такое как hotmail.com или microsoft.com, но при этом использовать общий лес, их следует добавлять в виде отдельных доменов.

• **Необходимость в повышенной безопасности.** В зависимости от потребностей организации, может понадобиться вынести роль эталона схемы в домен, отдельный от домена пользователей. В таком случае модель с единственным доменом не годится, и потребуется реализовать модель с выделенным корнем или модель с фиктивным доменом. При обдумывании добавления дополнительных доменов помните о главном принципе - чем проще, тем лучше. Однако если во время проектирования действительно возникает необходимость в добавлении других доменов, лучше их добавить, иначе в результате может получиться совершенно неэффективная среда.

Модель с несколькими деревьям и в одном лесе

Предположим, что организация планирует реализовать структуру AD DS и использовать для нее внешнее пространство имен. Однако в текущий момент в ее среде уже применяются несколько пространств DNS-имен, и их тоже необходимо включить в ту же структуру. Вопреки широко распространенному заблуждению, эти пространства имен можно интегрировать в единый лес AD с помощью нескольких деревьев, существующих в одном лесе. Одной из часто неправильно понимаемых характеристик AD DS является различие между непрерывным лесом и непрерывным пространством DNS-имен. Множество пространств DNS-имен можно интегрировать в единый лес AD DS в виде отдельных деревьев этого леса. Например, на рис. 15 показано, как компания Microsoft (теоретически) могла бы организовать несколько своих доменов AD DS, чтобы они относились к одному и тому же лесу, но к разным пространствам DNS-имен.

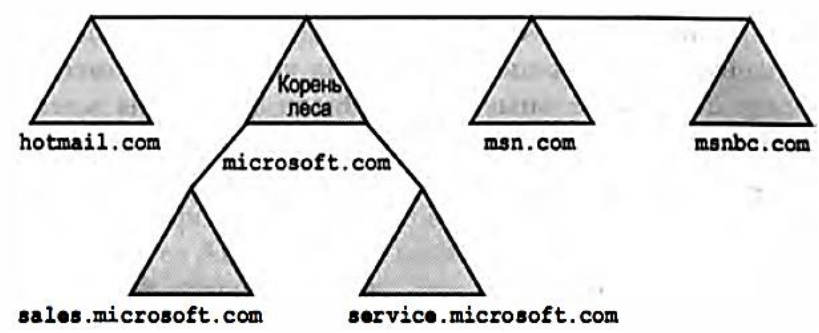

Рис. 15. Пример леса AD DS с несколькими уникальными деревьями

Корневым в лесе является только один домен (в данном случае microsoft.com), и только он управляет доступом к схеме леса. Все остальные домены, в том числе поддомены Microsoft.com и другие домены, которые занимают другие структуры DNS, являются членами этого же леса. Все отношения доверия между доменами являются транзитивными и перетекают из одного домена в другой.

Развертывание модели домена с несколькими деревьями

Если в организации в текущий момент используется несколько отдельных пространств DNS-имен для управления различными едини-

цами, то можно (среди прочих) рассмотреть подобную модель проектирования. Важно понимать, что просто использование нескольких пространств DNS-имен не делает организацию автоматически кандидатом на внедрение такой модели. Например, организация может обладать пятью отдельными пространствами DNS-имен, но ей нужно создать структуру AD DS на основе совершенно нового пространства имен, единообразного по всей организации. Объединение AD DS в такой единый домен может упростить логическую структуру среды, и при этом позволить использовать прежние пространства DNS-имен отдельно от AD DS.

Если в организации интенсивно применяются отдельные пространства имен, подобный вариант может оказаться более подходящим. При этом каждое дерево доменов в лесе сможет сохранить определенную степень автономии, как видимую, так и реальную. Часто такая модель позволяет удовлетворить даже самых привередливых администраторов филиалов, требующих полного контроля над всей своей IT -структурой.

Модель с федеративными лесами

Особой характеристикой реализации AD D S в Windows Server 2012 является возможность создания транзитивных отношений доверия между лесами. Эта возможность позволяет задать между двумя лесами с совершенно раздельными схемами транзитивные отношения доверия, которые предоставляют пользователям из этих лесов общий доступ к информации и общую схему аутентификации.

Возможность устанавливать и синхронизировать отношения доверия между лесами, однако, не появляется автоматически и требует сначала повысить функциональный уровень каждого леса.

Модель федеративного леса удобна для двух случаев. Первый - необходимость объединения двух различных структур AD DS, которая возникает в результате приобретения других компаний, слияния с другими корпорациями или других видов организационной реструктуризации.

В подобных ситуациях необходима связь между двумя лесами AD для обмена информацией. Например, две крупных организации с полностью заполненными данными лесами AD могли бы воспользоваться такой моделью при слиянии и объединить свои среды, как показано на рис. 16, без применения сложных средств для миграции доменов.

В этом примере, благодаря установке между корнями лесов двусторонних доверительных отношений, пользователи двух организаций могут получать доступ к информации друг друга.

Рис. 16. Схема доверительных отношений между лесами

Вторым сценарием, при котором может выбираться проектирование такой структуры лесов, является ситуация, когда различным подразделениям и филиалам внутри организации требуется полная защита и права на владение информационной структурой, но все же с возможностью обмена информацией.

Это эффективно разграничит две среды, предоставив каждому подразделению полный контроль над своей средой, после чего между их лесами можно будет установить одно- или двусторонние доверительные отношения для обмена данными и их синхронизации.

Подобная структура иногда вызвана потребностью в полном разграничении безопасности между различными подразделениями организации. С момента появления AD DS в Windows 2000 Server было обнаружено несколько уязвимых мест в обеспечении междоменной безопасности, из-за чего граница безопасности сместилась на уровень леса. В частности, с помощью атрибута SIDHistory администратор доверяемого домена леса может имитировать и получить доступ к ролям администратора схемы (Schema Admin) и администратора предприятия (Enterprise Admin). Из-за этих уязвимостей некоторые организации могут разделять леса и просто устанавливать доверительные отношения между лесами, специально для снятия с пользователей атрибута SIDHistory.

Концепция федеративных лесов значительно улучшает возможности лесов AD DS в смысле обмена информацией с другими средами. Помимо этого, организации, которые раньше не решались на внедрение AD из-за отсутствия надежной границы безопасности между доменами, теперь могут пользоваться преимуществами структуры федеративных лесов и оставить отделам или подразделениям полный контроль над

собственными лесами, но при этом позволить обмен данными с другими доменами.

Модель домена с пустым корнем

Схема является самым критически важным компонентом AD DS и потому ее следует тщательно защищать и оберегать. Несанкционированный доступ к контроллеру домена эталона схемы может привести к серьезным проблемам, и, пожалуй, является наилучшим способом для повреждения всего каталога. Поэтому понятно, что выделение ключей к схеме из пользовательской базы представляет собой вполне разумный и заслуживающий рассмотрения вариант. Отсюда и появилась модель домена с пустым корнем, изображенная на рис. 17.

Рис. 17. Модель с пустым корнем

Требования к безопасности в каждой организации свои. Требования к безопасности в компании, занимающейся секретными военными разработками, значительно отличаются от требований в компании, выпускающей детские игрушки. И для компаний с высокими запросами в отношении безопасности модель с пустым выделенным корнем может оказаться весьма подходящим вариантом.

Дополнительным преимуществом такой среды является то, что она позволяет переименовывать домены, добавлять домены и, по сути, входить и выходить из поддоменов без изменения названия леса. Хотя в Windows Server 2012 имеется средство для переименования доменов, это все-таки довольно сложный процесс, а модель с выделенным корнем позволяет упростить внесение изменений. Например, в случае слияния

двух компаний, при наличии выделенного корня с именем root.network и размещении всех доменов ресурсов в пространстве companyabc.com в том же лесе, добавление в лес домена company.net можно выполнить гораздо легче, чем его присоединение к домену root.network.

Прелесть модели доменов с выделенным корнем состоит в том, что ее можно встроить в любую из определенных ранее моделей доменов. Например, крупная группировка деревьев с опубликованными пространствами имен может иметь корень дерева с любым подходящим именем.

В примере на рис. 18 продемонстрирован один из возможных вариантов конфигурирования подобной среды. Эта модель не ограничивает гибкость AD DS, поскольку доступны все возможности для множества других конфигураций.

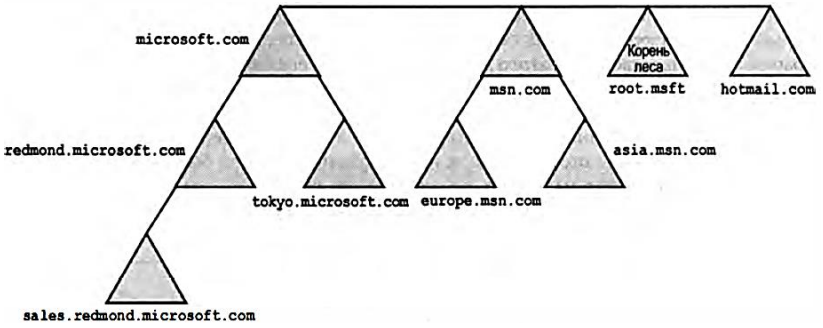

Рис. 18. Модель доменов с пустым корнем и различными именами деревьев

Многие организации не соглашаются с увеличением затрат на оборудование, а данная модель более дорогостоящая. В реальности она требует установки в корневом домене как минимум двух контроллеров: одного для обработки запросов на аутентификацию и одного для резервирования. Очень важно всегда помнить об этом и сопоставлять предъявляемые организацией требования к безопасности и объем затрат и преимуществ такой модели проектирования.

Модель с фиктивным доменом

Модель с фиктивным доменом, также называемая моделью со стерильным родительским доменом, заслуживает специального упоминания потому, что представляет собой сочетание модели нескольких доменов с единым пространством имен и модели с выделенным корнем. Попросту говоря, модель с фиктивным доменом, как видно на рис. 19,

содержит незаполненный домен в качестве корня леса и несколько поддоменов, заполненных пользовательскими учетными записями и другими объектами. У такой модели проектирования есть два очевидных преимущества.

Во-первых, как и в модели с выделенным корнем, схема отделена от пользовательских доменов, что снижает уязвимость пользователей и помогает защитить схему.

Во-вторых, пространство имен для пользовательских учетных записей отражает структуру организации, что устраняет какие-либо политических проблем. То есть, поскольку все пользователи во всех подразделениях организации находятся в доменной структуре на одном и том же логическом уровне, ни одна из групп не чувствует себя более главной или подчиненной по отношению к другим. Эта проблема может показаться смехотворной, однако психологическая природа людей непредсказуема, и потому вполне возможно, что для некоторых организаций эта модель будет предпочтительнее.

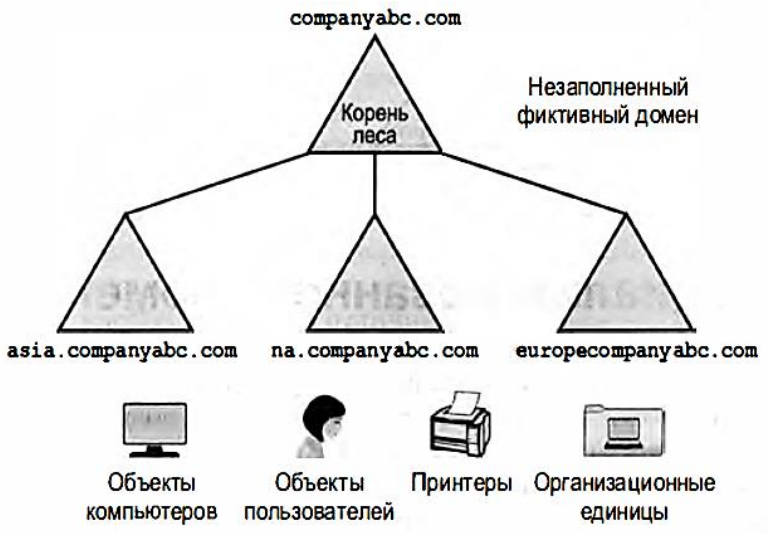

Рис. 19. Модель с фиктивным доменом

Модель специализированного домена

Специализированный домен или лес - это домен или лес, созданный для удовлетворения какой-то конкретной потребности. Например, в организации такой домен может быть создан для вынесения временных и

работающих по контракту пользователей в отдельную категорию и ограничения их участия в главном лесе AD DS, а также для установки между ним и остальными доменами доверительных отношений для обеспечения им доступа к ресурсам.

Еще одним возможным способом применении отдельной структуры специализированного домена является размещение в нем приложении уровня службы, которое по причинам безопасности или другим причинам требует исключительного доступа к схеме. То есть если в отделе кадров запускается приложение, которое сохраняет конфиденциальную информацию о сотрудниках компании в каком-нибудь приложении, использующем совместимый с LDAP каталог - например, AD DS - то для этого приложении можно создать специальный отдельный домен. Затем можно задать доверительные отношения между лесами для обеспечения совместного доступа к информации между этими двумя средами. Подобные ситуации встречаются редко, поскольку такие приложении обычно пользуются собственными каталогами, но все-таки они возможны. Из-за требования уникальности схемы AD DS во всем лесе, при наличии у этих приложений потребности в исключительном доступе или использовании общих атрибутов схемы применение единственного леса невозможно. Эта концепция, известная как AD LDS (Active Directory Lightweight Domain Services - Облегченная доменная служба Active Directory).

В целом, для развертывания в AD DS дополнительных доменов должны существовать веские причины. С добавлением в среду каждого нового домена возрастают накладные расходы, и логическая структура сети начинает выглядеть запутанно. Однако в некоторых отдельных случаях без специализированных доменов обойтись не удастся.

6.3. Проектирование структуры организационных единиц и групп

Организация пользователей, компьютеров и других объектов в структуре Windows Server 2012 Active Directory Domain Services (AD DS) предоставляет администраторам значительную гибкость и много возможностей по управлению их средами. Структура как организационных единиц, так и групп может корректироваться для удовлетворения практически любых производственных требований. Однако администраторы нередко весьма смутно представляют, как нужно проектировать и использовать организационные единицы и группы, особенно в модели администрирования на основе ролей, которое появилось в Windows Server 20 12. Довольно часто они применяют организационные

единицы безо всякой причины, а структуру групп делают неэффективной и запутанной. При правильной подготовке и заблаговременном изучении способов применении функциональное проектирование организационных единиц и групп может творить настоящие чудеса и значительно упростить среду Windows Server 2012 AD DS.

Организационной единицей (Organizational Unit - OU) называется контейнер административного уровня (рис. 20), который используется для логической организации объектов в AD DS.

Рис. 20. Пример структуры организационных единиц в AD DS

Концепция организационной единицы основана на стандарте облегченного протокола доступа к каталогам (Lightweight Directory Access Protocol - LDAP), на базе которого создавалась AD DS, хотя между самим LDAP и AD DS существуют концептуальные различия.

Объекты в Active Directory могут логически помещаться в организационные единицы в соответствии с указаниями администратора. По умолчанию объекты всех пользователей помещаются в контейнер Users (Пользователи), а объекты всех компьютеров - в контейнер Computers (Компьютеры), хотя их можно переместить оттуда в любой момент.

С технической точки зрения стандартные папки Users (Пользователи) и Computers (Компьютеры) в AD DS являются не организационными единицами, а объектами класса Container. Это очень важно понимать, поскольку объекты класса Container ведут себя не так, как организационные единицы. Чтобы иметь возможность использовать службы вроде групповых политик, работа которых зависит от функциональности организационных единиц, объекты пользователей и компьютеров лучше переместить из стандартных контейнеров в структуру OU.

Структура OU может быть вложенной, т.е. содержать организационные подъединицы с множеством уровней в глубину. Однако учите, что чем сложнее структура OU, тем труднее ее администрирование, и тем больше требуется времени на отработку запросов. Не рекомендуется создавать структуру OU с более чем 10 уровнями вложенности. Однако

разумнее применять еще меньше уровней, чтобы обеспечить быстрый отклик на запросы.

Организационные единицы в основном нужны для делегирования прав на администрирование различным группам администраторов. Существуют и другие возможные способы применения организационных единиц, но делегирование прав все-таки является главной причиной создания OU в среде AD DS.

Группы в AD

Концепция групп предназначена для логической организации пользователей в легко идентифицируемые структуры. Тем не менее, между функционированием групп и OU имеются серьезные отличия, которые перечислены ниже.

Пользователи могут просматривать данные о членстве в группах. Если информацию о членстве в OU могут просматривать только администраторы с помощью специальных средств администрирования, то информацию о членстве в группах могут просматривать все пользователи, которые задействованы в работе домена.

Членство в нескольких группах. Структура OU похожа на структуру папок в файловой системе. Любой файл в любой момент времени может находиться только в одной папке или OU. Относительно членства в группах подобных ограничений нет: пользователь может быть членом любой группы или нескольких групп, и его членство в той или иной группе может изменяться в любой момент.

Группы как параметры доступа. Каждая группа доступа в AD DS обладает уникальным идентификатором безопасности (Security ID - SID), который назначается ей при ее создании. У организационных единиц нет связанных с ними записей контроля доступа (Access Control Entry - ACE), поэтому они не могут применяться для обеспечения безопасности на уровне объектов. Это отличие является одним из самых важных, поскольку группы доступа позволяют пользователям разрешать или запрещать доступ к ресурсам на основании членства в группах.

Почтовые группы. Посредством групп рассылки и почтовых групп пользователи могут отправить одно почтовое сообщение группе и тем самым распространять его среди всех членов этой группы. Группы сами представляют собой списки рассылки, оставаясь в то же время доступными для обеспечения безопасности.

Группы в Windows Server 2012 делятся на два вида: группы доступа и группы рассылки. Кроме того, они могут различаться по области действия, т.е. быть локальными в компьютере, локальными в домене, глобальными или универсальными.

Группы доступа

Группа доступа (security group) - наиболее знакомый администраторам тип групп. Они применяются для массового назначения прав доступа к ресурсам и тем самым упрощения администрирования больших групп пользователей. Группы доступа могут создаваться для каждого отдела в организации. Например, администратор может создать для пользователей из отдела маркетинга группу доступа под названием Marketing (Маркетинг), а затем предоставить этой группе права доступа к каким-то конкретным каталогам в среде.

С каждой группой доступа связан уникальный идентификатор безопасности (Security Identifier - SID) – примерно так же, как и у каждого отдельного пользователя в AD DS. Уникальность SID позволяет применять правила безопасности к объектам и ресурсам в домене. Эта концепция также объясняет, почему невозможно просто удалить старую группу и переименовать новую, чтобы получить те же права доступа, которые были назначены старой группе.

Под **группой рассылки** подразумевается такая группа, члены которой могут получать отправляемые группе почтовые сообщения по протоколу SMTP (Simple Mail Transfer Protocol - простой протокол электронной почты). В Windows Server 2012 этой возможностью может пользоваться любое приложение, которое способно применять AD DS для поиска в адресной книге (т.е. LDAP-поиска).

Группы рассылки часто пугают с почтовыми группами, которые применяются в средах с Exchange 2000/2003/2007/2010/2013. Кроме того, в большинстве случаев группы рассылки не применяются в средах без Exchange Server, поскольку их функциональные возможности ограничиваются только инфраструктурами, которые способны их поддерживать.

В средах с Exchange Server группы рассылки могут использоваться для создания списков рассылки, не позволяющих применять правила безопасности.

В AD DS имеется также концепция **почтовых групп** (mail-enabled group). Эти группы представляют собой, по сути, те же группы доступа, но могут указываться в адресах электронной почты и использоваться для отправки SMTP-сообщений всем входящим в них членам. Такие

группы в основном применяются вместе с Exchange Server, но могут использоваться и вместе со сторонними почтовыми системами, интегрированными с AD DS.

В большинстве организаций значительную часть потребностей могут удовлетворять группы доступа с включенной почтовой функцией: они позволяют работать как с безопасностью, так и электронной почтой.

Область действия группы

В AD DS для групп существуют четыре основных области действия (scope). Каждая из этих областей служит своим целям, но все они предназначены просто для облегчения администрирования и возможности просмотра пользователей крупных групп либо одновременного выполнения с ними каких-то действий. По областям действия группы делятся на:

- локальные группы компьютера;
- локальные группы домена;
- глобальные группы;
- универсальные группы.

Область действия групп может оказаться одним из самых запуганных аспектов AD DS. Однако при соблюдении определенных критериев при создании групп и назначении их членов она становится более попятной.

Локальными группами компьютера (machine local group) называются группы, которые встроены в операционную систему и могут применяться только к объектам, локальным для компьютера, на котором они существуют. То есть это стандартные локальные группы вроде Power Users, Administrators и т.д., которые создаются в обособленной системе. До укрощенного администрирования через сеть для управления доступом к ресурсам сервера применялись именно локальные группы. Недостаток такого подхода состоял в том, что пользователи должны были иметь отдельную учетную запись на каждой машине, к которой им нужен был доступ. В доменной среде применять эти группы для назначения прав доступа не рекомендуется, поскольку затраты на администрирование в таком случае будут огромными.

Термином "**локальная группа домена**" (domain local group) обозначаются группы доменного уровня, которые могут применяться для задания прав доступа к ресурсам домена, в котором они находятся.

Локальные группы домена могут содержать члены из любого места в лесе AD DS или любого доверяемого домена за его пределами, а

именно, из: глобальных групп, учетных записей пользователей, универсальных групп, других локальных групп домена.

Локальные группы домена применяются главным образом для доступа к ресурсам, поскольку для каждого ресурса создаются разные локальные группы домена, а затем к ним добавляются другие учетные записи и/или группы. Это позволяет легко определить, какие пользователи и группы имеют доступ к ресурсу.

Глобальные группы (global group) - реинкарнация старых глобальных групп, которые предлагались в Windows NT, но с несколько другими характеристиками. В этих группах могут содержаться объекты следующих типов:

- учетные записи пользователей;
- глобальные группы из их собственного домена.

Глобальные группы в основном применяются для разбиения пользователей на легко идентифицируемые категории и для назначения прав доступа к ресурсам. От универсальных групп глобальные отличаются тем, что данные о членстве в них прекращают реплицироваться на границах доменов, т.е. их репликация за пределами доменов является ограниченной.

Концепция **универсальных групп** (universal group) впервые появилась в Windows 2000 Server и по-прежнему востребована в Windows Server 2012. Универсальные группы действительно являются универсальными. Они могут содержать объекты из любого доверяемого домена и могут использоваться для применения прав доступа к любому ресурсу домена. Данные о членстве в универсальных группах реплицируются по всему лесу. Что еще хуже, в Windows 2000 Server AD DS объекты универсальных групп хранили данные о членстве в одном многозначном атрибуте. Это означало, что при внесении любого изменения в данные о членстве в универсальной группе, требовалось заново реплицировать по всему лесу все данные о членстве в универсальной группе. Это ограничивало возможности универсальных групп.

В Windows Server 2003 появилось понятие инкрементной репликации данных о членстве в универсальных группах, которая позволяет реплицировать данные о членстве в универсальных группах для каждого члена отдельно. Это значительно сократило влияние репликации универсальных групп на среду и сделало концепцию универсальных групп более пригодной для распределенных сред. На сегодняшний день эта возможность доступна для применения в любых доменах с функциональным уровнем Windows Server 2003 или выше.

7. БРАНДМАУЭРЫ

7.1. Основы анализа сети

Приступая к обеспечению безопасности компьютера, нужно иметь представление о том, как работают сетевые службы, какие службы действуют в настоящее время, какие порты открыты и т. д.

Прежде всего рассмотрим табл. 1, в которой в обобщенном виде представлены важнейшие сокращения.

Таблица 1

Важнейшие сокращения сетевых терминов

Сокращение	Значение
DNS	Служба доменных имен
HTTP	Протокол передачи гипертекста
ICMP	Протокол управления сообщениями в Интернете
IP	Интернет-протокол
NFS	Сетевая файловая система
TCP	Протокол управления передачей
UDP	Протокол пользовательских датаграмм

Интернет-протокол. Практически все распространенные сетевые службы базируются на IP-пакетах. Если, например, интернет-пользователь хочет обратиться к вашему компьютеру через FTP, то компьютер запускает FTP-клиент. Этот клиент посылает на ваш компьютер специальные пакеты. Если на вашем компьютере установлен FTP-сервер, он принимает эти IP-пакеты и реагирует на запрос, пересылая свои IP-пакеты клиенту.

Кроме самих данных, в IP-пакетах содержатся (в том числе) еще четыре важных фрагмента информации: IP-адрес отправителя, порт отправителя, адрес назначения и порт получателя. Благодаря этим данным становится известно, откуда приходит пакет и куда он должен быть направлен.

IP-адреса и порты. IP-порты применяются для идентификации различных служб. Например, для запроса веб-документа обычно используется порт 80. Номера портов - это 16-битные числа. Порты вплоть до 1024 считаются привилегированными и зарезервированы для серверных служб (например, для HTTP-сервера). Остальные порты могут использоваться и клиентами, но и среди них есть несколько номеров, которые не должны применяться клиентом, так как в свою очередь зарезервированы для выполнения определенных целей.

Например, в система семейства Linux для многих IP-номеров портов заданы псевдонимы. В табл. 2 перечислены важнейшие номера портов, а также имена, под которыми они обычно используются (если такие имена есть), и краткое объяснение.

Таблица 2

Важнейшие IP-порты

Название	**Порт**	**Функция**
ftp	20,21	FTP
ssh	22	SSH
telnet	23	Telnet
smtp	25	Электронная почта
domain	53	DNS
Bootps и bootpc	67, 68	DHCP
http	80	Сеть
kerberos	88	Kerberos
pop3	110	Электронная почта
portmap	111	Portmap (для NFS)
ntp	123	Время (сетевой протокол синхронизации времени)
netbios-ns	137	Служба имен Microsoft/NetBIOS
netbios-dgm	138	Служба датаграмм Microsoft/NetBIOS
netbios-ssn	139	Служба доступа к файлам Microsoft (SMB, Samba)
imap	143	Электронная почта
ldap	389	LDAP
	427	Файловый протокол Apple (AFP)
https	443	Сеть (зашифрованный)
microsoft-ds	445	Файловая система CIFS (SMB, Samba)
printer	515	Печать с использованием LPD/LPR
	548	Файловый протокол Apple (AFP)
ipp	631	Печать с использованием IPP/CUPS
rmi	1099	Удаленный вызов методов (Java)
	1433	Microsoft SQL Server
pptp	1723	PPTP/VPN
nfs	2049	NFS
	3128	Squid (сетевые прокси)
mysql	3306	Сервер базы данных MySQL
	5353	Конфигурация сети с помощью Zeroconf/Bonjour

Окончание табл. 2

Название	Порт	Функция
	5999-6003	X-дисплей
	9100	Сетевой принтер HP-JetDirect

IP-протоколы. Существуют различные протоколы для работы с IP-пакетами: большинство интернет-служб используют TCP. Этот протокол требует подтверждения о получении пакета. Но бывают и протоколы, которым такое подтверждение не нужно. К их числу относится, например, ICMP (применяется программой ping) и UDP (используется DNS и NFS).

Фильтр IP-пакетов. IP-пакеты могут создаваться локальными программами или приходить на компьютер извне — через сетевой или PPP-интерфейс. Ядро решает, как поступить с пакетами. Упрощенно говоря, ядро может либо отбросить данные пакеты, либо переадресовать работающим программам или другим интерфейсам. При этом описанные выше характеристики пакетов могут использоваться в качестве критериев для принятия решений. Чтобы применить такой фильтр пакетов на практике, необходимо сообщить ядру, как оно должно поступать с различными IP-пакетами.

Определение активных сетевых портов. Принцип работы большинства сетевых служб заключается в том, что эти службы наблюдают за определенным портом. Если на этот порт приходят IP-пакеты, то конкретная служба занимается обработкой пришедшей информации и отвечает на нее. Пакеты, которые были присланы на ненаблюдаемые порты, просто игнорируются и поэтому не представляют опасности.

Чтобы оценить степень опасности, которой подвергается компьютер, нужно получить список всех наблюдаемых портов.

Netstat. При определении сетевой активности локального компьютера очень помогает команда netstat. В зависимости от того, с какими параметрами команда вызывается, она выдает массу различной информации.

7.2. Основы защиты сетевых служб

Чтобы как можно надежнее защитить эти службы, необходимо выполнить ряд шагов:

• Деинсталлируйте все сетевые службы, которые вам не нужны. Службы, которые не установлены, не функционируют и поэтому совершенно безопасны.

• Часто при работе с самыми нужными сетевыми службами бывает достаточно лишь предоставить доступ к службе всего для нескольких определенных клиентов (которые, в частности, находятся в локальной сети). Например, практически исключен случай, в котором вам пришлось бы предоставлять доступ к службам сервера печати в Интернете. Что касается Apache, Samba, MySQL и многих других крупных служб, то меры защиты нужно предпринимать в соответствующем конфигурационном файле.

• Необходимые сетевые службы должны выполняться с минимальным набором прав. Если это возможно и целесообразно, запустите службы без прав администратора с учетной записи, созданной специально для этих целей, или в среде, которая не позволит обращаться к файлам.

• В качестве дополнительного уровня защиты рекомендуется использовать специальный брандмауэр, который предназначен для фильтрации пакетов и который в соответствии с определенными правилами блокирует пакеты, приходящие из Интернета на адреса различных служб.

• Ни одна программа не защищена от ошибок. Программные ошибки позволяют потенциальным агрессорам завершать ваши программы с помощью отправки на компьютер специальных пакетов, а в особо тяжелых случаях даже выполнять на вашем компьютере свои команды. Чтобы свести к минимуму связанный с этим риск, ядро может наблюдать за выполнением программ на основании заранее заданных правил. Такой метод называется мандатным управлением доступом (Mandatory Access Control, MAC). В Linux для реализации этой функции используются два метода: SELinux и AppArmor.

Обновления, журналирование. Невозможно обеспечить достаточную безопасность действующей конфигурации компьютера за один раз — только с помощью регулярных обновлений вы сможете поддерживать ваше ПО в актуальном состоянии. Рекомендуется регулярно просматривать файлы регистрации вашего компьютера.

7.3. Сетевая фильтрация

Брандмауэры: общая информация

Термин «брандмауэр» у всех на устах, но общепринятого определения этого феномена не существует. Функции брандмауэра могут выпол-

няться оборудованием: в таком случае под брандмауэром обычно понимается компьютер, стоящий на стыке локальной сети и Интернета. Многие ADSL-роутеры могут иметь простейшие функции брандмауэров.

Нередко брандмауэром может быть и программный пакет, установленный на компьютере и при условии правильной конфигурации повышающий безопасность компьютера. Во многих дистрибутивах содержатся многофункциональные инструменты, предназначенные для настройки конфигурации брандмауэра.

Под **брандмауэром** будем понимать совокупность методов, повышающих надежность обмена информацией, проходящей по TCP/IP через фильтр пакетов. Такой фильтр анализирует все сетевые пакеты, приходящие на компьютер, а также пакеты, которые уходят с компьютера в сеть. В зависимости от того, все ли правила соблюдаются, пакеты могут быть пропущены или заблокированы.

Брандмауэры для частных ПК

Сегодня большинство частных ПК постоянно подключены к Интернету, доступны по фиксированному IP-адресу, назначаемому провайдером, а значит, подвергаются опасности.

Если, к примеру, на компьютере действует SSH-сервер, то злоумышленник может попытаться войти в сеть через этот сервер. Для этого агрессоры используют сценарии, автоматически подбирающие логины, просто подставляя слова из словаря. Таким образом, хороший пароль дорогого стоит! Другая опасность таится во WLAN: на настоящий момент хорошо защищенными можно считать только те сети WLAN, в которых применяется механизм WPA2, и то лишь при условии, что используемый пароль является достаточно длинным и сложным.

Можно возразить, что атака на ваш компьютер не имеет смысла, ведь находящиеся на нем данные вряд ли кого-то заинтересуют. Может быть, и так. Но не каждая атака предпринимается с целью выведать данные, а потом манипулировать ими. Часто злоумышленник хочет установить у вас на компьютере маленькую программу, которой позже сможет воспользоваться. Жертвами подобных атак становятся миллионы компьютеров с Windows, которыми могут удаленно управлять злоумышленники.

Брандмауэры для локальных сетей

Обычно корпоративные локальные сети больше нуждаются в обеспечении безопасности, чем домашние ПК. Одновременно создаются лучшие условия для построения нужной инфраструктуры. На практике

в фирменной локальной сети за выход в Интернет и обеспечение безопасности часто отвечает отдельный компьютер. Все остальные сетевые службы работают на других компьютерах. Эта концепция изображена на рис. 21.

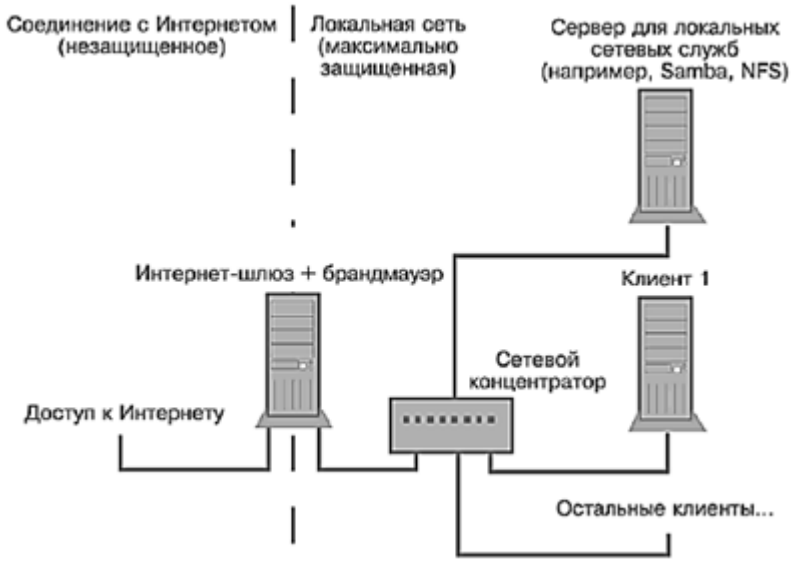

Рис. 21. Брандмауэр для локальной сети

В очень небольших сетях функции брандмауэра и сетевого сервера может выполнять один компьютер. Но такой подход не является оптимальным, так как на этом компьютере придется запустить и эксплуатировать множество сетевых служб, которые могут быть использованы для нанесения вреда сети.

В очень больших сетях часто бывает не один, а даже два брандмауэра. Первый служит лишь для обеспечения базовой безопасности, но пропускает такие интернет-протоколы, как HTTP или FTP. Сетевое пространство в таком случае называется демилитаризованной зоной (Demilitarized Zone, DMZ). Этот термин означает, что внутри сети лишь ограниченные меры безопасности. Как правило, в этой зоне располагается веб-сервер, а также другие сетевые серверы, которые должны быть общедоступны (то есть могут быть найдены через Интернет).

Демилитаризованная зона отделяется от оставшейся части локальной сети вторым брандмауэром. Уже за ним располагаются все другие

службы, отвечающие за работу локальной сети и абсолютно недоступные извне. Однако конфигурация многоступенчатого брандмауэра - очень обширная тема, выходящая за рамки этой книги. Руководства по конфигурации таких барьеров даются в специальной литературе.

Сетевой фильтр

Рассмотрим сетевую фильтрацию для операционных систем семейства Linux. Внутри ядра обработкой правил брандмауэра занимается система, называемая сетевым фильтром. На рис. 22 в очень упрощенном виде показано, какими путями IP-пакеты могут передвигаться в системе фильтрации пакетов.

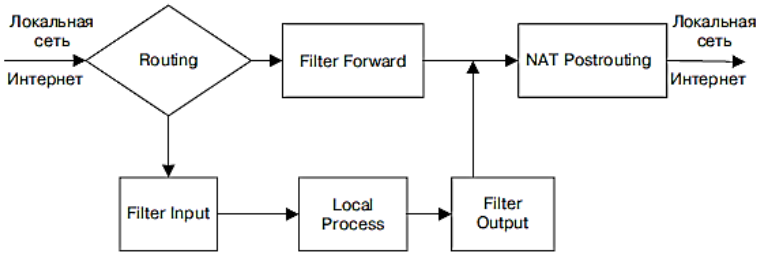

Рис. 22. Упрощенное представление системы iptables/netfilter

В следующем списке очень кратко описаны состояния IP-пакета в ядре.

Routing (Маршрутизация). Основываясь на информации об IP и адресе порта, ядро решает, должен пакет обрабатываться на локальном компьютере или его следует передать через сетевой интерфейс на другой компьютер (который может находиться как в локальной сети, так и в Интернете).

Filter Input (Входной фильтр). На основании определенных правил проверяется, следует ли обработать пришедший пакет с помощью локальных программ (например, сетевых демонов).

Local Process (Локальный процесс). В этом окне символически изображены все программы, обрабатывающие IP-пакеты на локальном компьютере либо создающие IP-пакеты (то есть это все сетевые службы, например, FTPD, HTTPD).

Filter Output (Выходной фильтр). На основании отдельных правил определяется, может ли IP-пакет снова покинуть ядро.

Filter Forward (Фильтр переадресации). Этот фильтр определяет, какие пакеты, которые следует только переадресовать (но не обрабатывать), могут пройти через ядро.

NAT Postrouting. Если компьютер должен предоставлять другим компьютерам доступ в Интернет путем маскарадинга, этот механизм выполняет нужные операции с IP-пакетами других компьютеров.

Действия. За переадресацию пакетов отвечает ядро - независимо от того, приходят они с сетевого интерфейса или создаются на компьютере одной из локальных программ. Ядро может совершать на различных уровнях фильтрующей системы три разных действия.

Deny (Drop) - переадресация пакетов отклоняется без запроса о подтверждении (можно сказать, что при этом пакет удаляется и больше не существует).

Reject - переадресация пакетов отклоняется с запросом о подтверждении. С пакетом происходит то же, что и в первом случае, но отправитель с другим ICMP-пакетом получает уведомление о том, что его пакет не был принят.

Accept - пакет переадресовывается.

Таблицы. В принципе, сетевой фильтр построен так: каждый IP-пакет проходит через различные части ядра, где в определенных пунктах проверяется на основании установленных правил. При соответствии правилам пакет переадресовывается, в противном случае - удаляется или отправляется назад. Сетевой фильтр управляется тремя таблицами.

Таблица фильтра – обычно в ней содержится вся система правил для отдельных пакетов (брандмауэр).

Таблица трансляции сетевых адресов – действует лишь в том случае, если в ядре активизирована функция маскарадинга. Она обеспечивает возможность различных изменений адресов (трансляции сетевых адресов) для пакетов, приходящих в ядро извне либо покидающих ядро.

Таблица mangle – также позволяет выполнять различные операции с IP-пакетами. Таблица служит для выполнения специальных задач и далее в книге рассматриваться не будет.

Цепочки правил (chains). В каждой из упомянутых таблиц предусмотрено несколько цепочек правил:

- таблица фильтра — Input, Forward, Output;
- таблица трансляции сетевых адресов — Prerouting, Output и Postrouting;
- таблица mangle — Prerouting и Output.

Процесс маршрутизации управляется в основном изменением IP-таблиц, содержащих вышеперечисленные цепочки правил. Существуют

вспомогательные программные средства, упрощающие администратору работу с IP-таблицами, например, Shorewall.

Shorewall – инструмент для настройки брандмауэра (файрвола) в Linux, программное обеспечение под свободной лицензией GNU GPL. Технически является надстройкой над подсистемой iptables ядра Linux и обеспечивает упрощённые методы конфигурирования данной подсистемы. Он предоставляет более высокий уровень абстракции для описания правил работы файрвола.

Программа не является демоном, то есть не работает постоянно. Правила хранятся в текстовых файлах, при запуске shorewall считывает свои файлы конфигурации и преобразует их в настройки понятные iptables, после чего данные настройки файрвола могут действовать до перезапуска операционной системы.

8. СРЕДСТВА ВИРТУАЛИЗАЦИИ

8.1. Основы виртуализации

Виртуализация позволяет параллельно использовать на одном компьютере несколько операционных систем. Эта возможность очень востребована на практике: можно установить Linux в Windows, выполнять Windows в Linux, тестировать новую альфа-версию дистрибутива xyz, не опасаясь повредить действующую (стабильную) версию Linux, уверенно отделять друг от друга функции сервера (виртуализация сервера) и т. д.

Технологии виртуализации

Гость и хозяин. При описании систем виртуализации закрепилась метафора, рассматривающая основную систему как хозяина (host), а работающие на ней виртуальные машины как гостей (guests).

Технологии. Существуют различные методы виртуализации операционных систем. В следующем списке перечислены наиболее распространенные из них и названы некоторые программы (фирмы), которые пользуются этими технологиями.

Полная виртуализация (виртуальные машины, эмуляция). В данном случае программа имитирует работу виртуального аппаратного обеспечения, то есть компьютера, состоящего из процессора, ОЗУ, жесткого диска, сетевой карты и т. д. Гостевые системы «считают», что виртуальное аппаратное обеспечение является реальным. Чтобы такая система функционировала, работающая на хозяине программа виртуализации должна отслеживать код гостя и заменять определенные команды другими фрагментами кода. Эту задачу выполняет гипервизор (Virtual Machines Monitor, VMM - «монитор виртуальных машин»). Такая программа-гипервизор также отвечает за события, связанные с хранением информации и управлением процессами.

Преимущества: на виртуальной машине может функционировать практически любая операционная система. При этом в операционную систему не требуется вносить никаких изменений.

Недостатки: работает сравнительно медленно.

Программы/фирмы: VMware, QEMU, Parallels, VirtualBox, Microsoft Virtual PC.

Паравиртуализация. В данном случае хозяин также же предоставляет виртуальные машины, на которых выполняются программы гос-

тей. Отличие от полной виртуализации состоит в том, что гостевую операционную систему для виртуализации требуется модифицировать, после чего эта система напрямую сообщается с VMM.

Преимущества: высокая эффективность.

Недостатки: требует специальной модификации операционных систем для целей виртуализации. Для такой системы с открытым кодом, как Linux, это не составляет никакой проблемы, чего не скажешь о коммерческих операционных системах, например, Windows.

Программы/фирмы: Xen, UML (Linux в пользовательском режиме).

(Пара)виртуализация с поддержкой аппаратного обеспечения. Современные процессоры производства Intel и AMD содержат аппаратные функции, предназначенные для упрощения процессов виртуализации. В Intel такая технология называется Intel-VT (ранее - Vanderpool), а в AMD - AMD-V (ранее - Pacifica).

Преимущества: высокая эффективность, при некоторых вариантах внедрения не требуется вносить изменения в операционную систему.

Недостатки: необходимы специальные процессоры.

Программы/фирмы: KVM, Xen.

Виртуализация на уровне операционной системы (контейнеры). При использовании данного метода настоящие виртуальные машины не применяются. Вместо этого при таком подходе машины применяют общее ядро и фрагменты файловой системы хозяина. К важнейшим задачам системы виртуализации относится, в частности, обеспечение изоляции между хозяином и гостями для исключения каких бы то ни было проблем с безопасностью.

Достоинства: очень эффективна, сберегает ресурсы (ОЗУ, дисковое пространство и т. д.).

Недостатки: может применяться только тогда, когда хозяин и гости используют в точности одну и ту же операционную систему, и совершенно одинаковую версию ядра. Операционная система должна быть модифицирована соответствующим образом.

Программы/фирмы: OpenVZ, Virtuozzo, Linux-VServer.

Все перечисленные методы, кроме первого, требуют внесения изменений в ядро, причем соответствующие операции производятся через Linux. В настоящее время, по крайней мере официально, в состав ядра входят только те функции виртуализации, которые относятся к KVM и UML. При использовании других методов ядро необходимо модифицировать с помощью неофициальной заплатки. Если, например, вы рабо-

таете с Xen-образным дистрибутивом, то знайте, что дистрибьютор заблаговременно встраивает в ядро функции, необходимые для работы в Xen.

8.2. Виртуальное аппаратное обеспечение

Эмулирование виртуального аппаратного обеспечения — это очень сложный процесс. В зависимости от механизма виртуализации или варианта его внедрения вы рано или поздно столкнетесь с границами возможностей вашего компьютера.

ОЗУ. Память компьютера должна быть достаточно объемной, чтобы выполнять все требования ресурсов хозяина и гостей, работающих на нем. Чем больше систем должны функционировать одновременно, тем больше оперативной памяти требуется. Например, на компьютере, которым я пользуюсь для тестирования, объем оперативной памяти достигает 6 Гбайт. Этого достаточно, чтобы без проблем работать одновременно в 6–7 дистрибутивах Linux.

Жесткий диск. Большинство систем виртуализации сохраняют файловые системы гостей в большом файле в системе хозяина. Таким образом, гости получают доступ к файлам жесткого диска не прямо, а опосредованно, через систему виртуализации. Следовательно, доступ к файлам в «гостевой» системе осуществляется значительно медленнее, чем в системе хозяина, в 2–3 раза.

CD/DVD-приводы. CD- и DVD-приводы выделяются хозяином гостям. В любом случае предоставляется доступ «только для чтения». Мне не известна ни одна система виртуализации, которая позволяла бы записывать CD и DVD в гостевой системе.

Большинство программ виртуализации дают возможность присвоить каждому виртуальному CD или DVD ISO-файл. Тогда гость вместо того, чтобы пользоваться реальным приводом, обращается к такому файлу. Это исключительно полезно в тех случаях, когда необходимо многократно устанавливать одни и те же программы. При необходимости вы можете без особого труда сами извлечь ISO-файл с CD или DVD.

Графический адаптер. Для более или менее эффективного использования графических возможностей на каждой гостевой системе необходимо установить специальный драйвер, настроенный на виртуализационное ПО хозяина. В зависимости от применяемой системы виртуализации существуют определенные ограничения в области использования трехмерной графики.

Звуковые функции. Большинство программ виртуализации предоставляют гостевой системе виртуальную звуковую карту и перенаправляют звуковой вывод на аудиосистему хозяина. Если вы не выдвигаете экстраординарных требований, то такого механизма вполне достаточно.

USB-устройства и внешнее аппаратное обеспечение. Ввод, осуществляемый с помощью клавиатуры и мыши, направляется из системы-хозяина в систему-гость. От применяемой системы виртуализации зависит, к каким внешним устройствам будут иметь доступ пользователи гостевых машин. USB-устройства, к сожалению, поддерживаются не всеми системами виртуализации, а если и поддерживаются, то с серьезными ограничениями.

8.3. Программы виртуализации

Спектр предлагаемых инструментов виртуализации, как в коммерческом сегменте, так и среди свободно распространяемого ПО, необозримо велик. В следующем списке кратко рассмотрены важнейшие флагманы рынка виртуализации. В скобках указано, является ли данный продукт коммерческим или распространяется свободно, какая фирма занимается разработкой и реализует на рынке соответствующую продукцию.

VMware (коммерческий, EMC). Фирма VMware - бесспорный лидер на рынке программ для виртуализации. Список производимой ею продукции начинается с пользовательских программ для ПК (рабочая станция и проигрыватель VMware) и заканчивается рядом мощных программ для сервера (VMware Server, ESXi, vSphere). Отдельные программы распространяются бесплатно, но не с открытым кодом. В качестве системы-хозяина поддерживаются Windows, Linux, а в отдельных случаях и Mac OS X. Некоторые продукты VMware работают вообще без операционной системы, «с нуля» (bare metal).

VirtualBox (частично бесплатная программа, Sun/Oracle). Функции программы VirtualBox в целом похожи на функции рабочей станции VMware, таким образом VirtualBox также подходит для настольной виртуализации. В качестве системы-хозяина поддерживаются Windows, Linux и Mac OS X. Для частных пользователей программа VirtualBox бесплатна; кроме того, есть свободно распространяемая версия этой программы, которая может использоваться и коммерческим образом, на условиях стандартной общественной лицензии (GPL). VirtualBox исключительно быстро развивалась в последние годы. Такой факт, что за год выходило несколько версий программы, говорит о том, что

VirtualBox хорошо совместим с новейшими версиями ядра и X-версиями.

KVM/QEMU (свободно распространяемая программа, Red Hat). Собственно, KVM - это просто модуль ядра, который радикально ускоряет работу эмулятора QEMU при использовании современных процессоров, при том что раньше этот эмулятор работал достаточно медленно. С тех пор как KVM официально вошел в состав ядра, а Red Hat купил Qumranet - фирму, разработавшую KVM, — значение модуля KVM резко выросло и он уже считается стандартным виртуализационным решением в дистрибутивах Fedora, Ubuntu и, конечно же, для версии 6 Red Hat Enterprise Linux. KVM одинаково хорош для применения как на ПК, так и на сервере. И все же по таким показателям, как понятность для пользователей, совместимость и скорость, KVM пока не может конкурировать с аналогичными коммерческими программами — Vmware, VirtualBox и Xen. В качестве системы-хозяина поддерживается только Linux.

Xen (частично бесплатная программа, Citrix). Xen - это гипервизор, функционирующий без операционной системы. Виртуализированные гостевые системы работают в так называемых доменах (domU), причем первый домен имеет особые привилегии и в определенном смысле сравним с системой-хозяином в других программахвиртуализации. Во многих практических ситуациях Xen значительно эффективнее, чем другие системы виртуализации. Однако в то же время настройка и конфигурирование гостевых систем (доменов) требует гораздо больших усилий. Это не в последнюю очередь объясняется тем, что расширения ядра, необходимые для правильной работы Xen, очень объемны и, несмотря на все приложенные усилия, пока не входят в состав официальной версии ядра. Если же вы готовы вложить в работу с Xen много времени, то достигнете выдающихся результатов, но для использования от случая к случаю Xen не годится.

OpenVZ и Virtuozzo (частично бесплатные программы, Parallels), а также Linux-VServer (свободно распространяемое ПО). OpenVZ, базирующийся на его основе коммерческий продукт Virtuozzo и технически сходное виртуализационное решение Linux-VServer позволяют обустраивать много изолированных сред в одном дистрибутиве Linux. OpenVZ или Virtuozzo при работе исходят из того, что в системах «хозяина» и его «гостей» работает одна и та же версия Linux. Эта концепция отлично подходит для тех случаев, когда необходимо виртуали-

зировать несколько (много!) аналогичных серверов. Такая система частично используется провайдерами интернет-хостинга, которые предлагают недорогие виртуальные корневые серверы.

Hyper-V (коммерческая программа, Microsoft). Корпорация Microsoft поначалу не успела поучаствовать в разделе рынка виртуализации, но сейчас прилагает титанические усилия, чтобы сделать собственное виртуализационное решение — Hyper-V — конкурентоспособным. Hyper-V воспринимает систему Windows Server как систему-хозяина, но при этом может поддерживать Linux в качестве гостевой системы. Компания даже разработала для этой цели собственные драйверы ядра Linux, причем эти драйверы с открытым кодом (такой шаг дался Microsoft с большим трудом, так как эта корпорация очень долго представляла Стандартную Общественную Лицензию в самом черном свете).

9. АДМИНИСТРИРОВАНИЕ ПРОЦЕССА КОНФИГУРАЦИИ

9.1. Процесс конфигурации ИС

Под **конфигурацией ИС** будем понимать разработку и реализацию концепции, позволяющей администратору системы быть уверенным в непротиворечивости, целостности, проверяемости и повторяемости параметров системы.

Для небольшой и несложной ИС конфигурация ее параметров обычно осуществляется администратором системы вручную. По мере роста ИС и увеличения сложности ее реализации необходимо администрирование процесса конфигурации ИС с помощью управляющих систем. И обычно требуется переход к управлению процессом конфигурации с помощью управляющих систем (MS и NMS) от ручного управления.

Для этого необходимо предпринять ряд шагов. Сначала следует установить базовую конфигурацию и задокументировать ее. Затем нужно определить механизм изменения и модификации базовой конфигурации. После этого внедрить процесс проверки текущей конфигурации на соответствие заданным базовым параметрам (аудит конфигурации).

Для **первого шага** следует установить некоторую текущую конфигурацию как базовую и соответствующую ей связь между устройствами и программными продуктами. Это не столько техническая, сколько организационная процедура по фиксированию текущих параметров и функциональных схем взаимодействия устройств и программ в некотором журнале. Время проведения этой процедуры и дата ее окончания определяются администратором системы. После этой даты все изменения параметров должны проводиться по новым процедурам, установленным администратором системы.

Вторым шагом является организация централизованной БД, хранящей параметры устройств и программных продуктов. Обычно такие централизованные БД поддерживаются управляющими системами. Управляющая система создает схемы взаимодействия устройств (например, карты сети) и программных продуктов. Но для небольшой ИС администратор системы может использовать средства любой СУБД для организации такого хранилища данных. Обычно процесс документирования конфигураций частично выполняется MS, частично вручную администратором системы.

Третьим шагом в администрировании конфигураций является выработка механизма опроса конфигураций, подтверждения их и документирования изменений. Этот механизм должен дать администратору системы уверенность в том, что изменения конфигураций прошли корректно, и о модификации параметров извещены соответствующие службы администратора системы, разработчики прикладных систем и (при необходимости) производственные структуры организации. АС должен быть уверен, что проинформированные службы обоснованно приняли (либо отвергли) эти изменения.

Некоторые сетевые управляющие системы позволяют сначала изменить параметры у себя, а затем распространить их по устройствам ИС с помощью процесса модификации. После этого NMS получают подтверждение о происшедших обновлениях и изменяют функциональные схемы взаимодействия устройств. В любом случае изменения параметров ИС должны быть известны пользователям и подхвачены средствами сопровождения с тем, чтобы АС был уверен в соответствии реальных изменений и задокументированной информации.

Четвертым шагом является реализация процесса аудита параметров относительно базовых, поскольку, вне зависимости от способа изменения параметров (автоматически или вручную) существует вероятность того, что внесены некорректные обновления или изменения параметров, не синхронизированные между собой. Процесс аудита похож на процесс документирования, но с обнаружением ситуаций и оповещением о них администратора системы (если процесс управляется, например, NMS). Аудит может производиться автоматически через регулярные интервалы времени или инициироваться администратором системы.

9.2. Задачи и проблемы конфигурации

Различные аппаратные средства и разные программные продукты имеют наборы сходных параметров и одинаковые принципы их задания. Поэтому можно выделить ряд стандартных проблем и задач конфигурации, к ним относятся следующие: стандартизация параметров, задание параметров при инициализации ресурсов, обеспечение загрузки компонент, восстановление параметров, инвентаризация параметров и документирование функциональных схем работы компонент системы, конфигурация параметров согласно политике организации. Рассмотрим эти задачи.

Стандартизация параметров. АС должен создать стандарт на задание параметров для каждого вида коммуникационных устройств, серверов, ОС, СУБД и модулей прикладных систем. Такой стандарт должен стать стандартом организации, где функционирует ИС. При этом необходимо учитывать, что стандарты данной организации не должны противоречить отраслевым стандартам.

Задание параметров при инициализации ресурсов. Задание параметров работы оборудования, ОС, СУБД или ИС при установке продукта администратором системы практически определяет дальнейшую эффективность, а часто и работоспособность системы. АС в процессе первоначальной загрузки модулей ИС должен внимательно относиться к умолчаниям (default), которые рекомендовали разработчики компонент ИС. Умолчания следует обязательно документировать (отражать в документации базовой конфигурации) и менять только в случае необходимости при понимании сути производимых компонентами ИС действий.

Обеспечение загрузки компонент (provision/deprovision). Новые устройства или программные компоненты ИС должны легко загружаться или удаляться вместе с их параметрами. Современные ИС быстро развиваются и требуют постоянных изменений. Длительный процесс таких изменений приведет к финансовым потерям. Поэтому АС должен иметь возможность (вручную или автоматически) быстро загрузить/выгрузить в БД управляющей системы соответствующие параметры (стандартизированные и соответствующие определенной политике). В автоматическом режиме это может быть произведено, например, с использованием протокола SNMP, по которому включаемая/выключаемая компонента ИС посредством агента оповестит управляющую систему об изменениях. Последняя, в свою очередь, посредством пересылки и загрузки/выгрузки конфигурационных файлов у данной компоненты ИС быстро и стандартно обеспечит процесс изменений.

Восстановление параметров. В некоторых ситуациях программным обеспечением могут быть потеряны параметры его загрузки. Перезагрузка их администратором системы вручную (пользуясь документацией) приведет к очень медленному восстановлению системы. Поэтому АС должен иметь архивные копии БД всех параметров компонент ИС. Современные управляющие системы предоставляют возможность регулярно копировать базу данных параметров и хранить копии за различные даты. В ситуациях неработоспособности ИС, которые могут быть вызваны неправильными обновлениями параметров, восстановление

определенной версии параметров системы приводит к восстановлению ИС.

Инвентаризация параметров и документирование функциональных схем работы компонент системы. Эта задача обсуждалась ранее. Укажем только, что АС при ее решении должен проверять версии установленных компонент ИС, иметь графическое представление о взаимодействии всех аппаратных и программных компонент, производить аудит работы всех сетевых протоколов. Следует также отметить, что инвентаризация системы входит в регламентные работы администратора системы и должна выполняться регулярно по выработанному им расписанию регламентных работ.

Конфигурация параметров согласно политике организации. В процессе стандартизации параметров АС должен учитывать и отражать в конфигурации корпоративные технологические стандарты, сетевые стандарты, стандарты безопасности, отраслевые стандарты. В этом случае при изменениях в этих стандартах все конфигурации различных компонент ИС меняются одинаково и одновременно по единым правилам (политике).

9.3. Технологии конфигурации и оценка ее эффективности

С точки зрения производственных подразделений предприятия важны влияния действий администратора системы по конфигурации ИС на время восстановления системы и на защиту ИС от несанкционированного доступа. Эффективность конфигурации ИС определяется успехом администратора системы в решении этих двух задач. Рассмотрим их подробнее.

Метрики систем

Чтобы определить, что такое безошибочная работа ИС, нужны критерии - метрики. Рассмотрим так называемые бизнес-метрики, т. е. те критерии безошибочной работы ИС, которые интересны компании с точки зрения осуществления ее производственной деятельности.

Существуют три основные бизнес-метрики работы ИС.

Ожидаемое время восстановления системы MTTR (Mean Time to Restore). Эта метрика задается бизнес-подразделениями компании службам администратора системы. Есть виды бизнеса, которые могут просуществовать без ИС только несколько минут, а затем цена простоя за минуту станет критически высокой.

Другие виды бизнеса могут ждать восстановления системы несколько дней без финансовых потерь. Это критическая метрика для планирования процедуры восстановления. Стоимость по применению превентивных мер для восстановления системы растет в геометрической прогрессии в зависимости от значения MTTR.

Ожидаемое время между отказами MTBF (Mean Time Between Failures), или наработка на отказ, - это метрика работы оборудования, задаваемая производителем. Так как современное компьютерное оборудование работает достаточно надежно (очень часто производителем дается пожизненная гарантия), то часть производителей не приводит эту метрику в своей технической документации. Администратору системы следует в этом случае брать ее из публикуемых аналитических данных по данному виду оборудования.

Время подъема системы Uptime - это результирующая метрика, которая говорит о том, сколько времени пользователь не пользуется ИС из-за проблем диагностики ошибки и восстановления системы, т. е. это совокупность времени для поиска ошибок, их диагностики, времени восстановления и запуска ИС в промышленном режиме. Эта метрика задается бизнес-подразделениями службам администратора системы в SLA (Service Level Agreement), регламентирующая время работы ИС. Определяется она исходя из финансовых возможностей предприятия и, соответственно, его оснащенностью средствами диагностики и восстановления. Для служб администратора системы эта метрика является отчетной и определяет их возможность поддерживать ИС в работоспособном состоянии.

Основной метрикой зачастую является MTTR. Если эта метрика измеряется в минутах, то АС имеет немного времени на восстановление параметров ИС. Поэтому при создании стратегии архивирования параметров и конфигурации системы необходимо учитывать их влияние на эту метрику.

Защита от несанкционированного доступа

Защита от несанкционированного доступа (НСД) является одной из основных проблем для всех ИС. Более подробно она будет рассмотрена главе В этой главе будет определено, как ее решение связано с задачей конфигурации параметров. Администратору системы необходимо создать профайл (список) параметров данной организации, влияющих на защиту от несанкционированного доступа. На этот список параметров обычно влияют не только технологические требования организации или требования руководства, но и отраслевые или федеральные требования.

Политика безопасности с точки зрения конфигурации должна включать в себя:

- способ задания паролей пользователей и способ задания паролей АС;
- политику доступа к ИС;
- политику доступа мобильных пользователей;
- политику кодирования информации;
- политику использования антивирусов и антиспамов.

После конфигурации ИС администратор должен проверить свою работу, задав себе простые вопросы и ответив на них:

- информация в ИС доходит по назначению и не попадает куда-либо еще?
- ИС циркулирует только авторизованная информация?
- информация записывается на известные и разрешенные администратором системы тома?
- информация искажается?
- нет ли неопознанной, «ничейной» информации?
- информация, требующая кодирования, так кодированной и осталась?

АС должен регулярно осуществлять превентивные (предупреждающие, опережающие) тесты ИС на присутствие в системе хакеров, например, пользователей, позиционирующих себя сотрудниками организации, в то время как они таковыми не являются. Эти проверки надо сопровождать отчетами для анализа слабых мест в конфигурации параметров безопасности.

Наконец, АС должен иметь доступ к официальным сайтам компаний-разработчиков компонент, используемых в ИС. Администратор должен иметь подписку на официальную рассылку изменений к компонентам ИС (например, версии драйверов, исправления ошибок - patch). Все изменения конфигураций следует получать только из официальных источников. Только в этом случае можно гарантировать систему от некорректной конфигурации компонент.

Изменения некоторых параметров системы могут привести к ошибкам, особенно если они осуществляются вручную. Поэтому АС необходимо постоянно следить за соответствием действующих параметров требованиям, сформулированным в профайле безопасности. Причем речь идет о том, что нужно исключить доступ неправильно работающих компонент, т. е. тех устройств или программ, которые становятся источниками ошибок или угроз.

Еще одной проблемой защиты от НСД являются сотрудники, заканчивающие работу в организации по различным причинам. Известно, что они являются *основным* источником раскрытия системы защиты от НСД. Администратор системы обязан *централизовано хранить* все идентификаторы и пароли пользователей, сведения о разрешенных ему правах доступа к различным компонентам ИС с тем, чтобы быстро и в едином месте их блокировать в случае увольнения сотрудника.

Практические рекомендации к технологиям конфигурации

Для реализации задач по конфигурации параметров в ОС, СУБД, прикладных системах существуют собственные средства. К этим средствам АС должен добавить дополнительные программные продукты, позволяющие выдавать по расписанию отчеты о конфигурациях, архивировать согласно расписанию и восстанавливать параметры. Помимо этого необходимо использовать специальные системы защиты от НСД, например сетевые средства RADIUS (Remote Authentication Dial-In User Service)/TACAS (Terminal Access-Controller Access Control System), позволяющие централизовать сетевую защиту.

Приведем пример – **пример профайла** параметров и **отраслевых требований защиты** от НСД для компании, обслуживающей платежные банковские карты.

Уровень защиты повышается с увеличением числа банковских транзакций и числа пользователей. А потери от неверной конфигурации даже для одного пользователя могут быть очень ощутимы. Отрасль регулируется специальным стандартом **PCI DSS**, требованиями Центрального банка Российской Федерации (ЦБ РФ), требованиями платежной системы Visa International, требованиями платежной системы MasterCard Worldwide. Администратору системы для составления профайла необходимо изучить все эти требования. Для того чтобы предоставить объем необходимых сведений для грамотной работы администратора системы, кратко опишем регулирующие документы.

В 1998 г. ЦБ РФ было принято Положение № 23-П «О порядке эмиссии кредитными организациями банковских карт и осуществления расчетов по операциям, совершаемым с их использованием». Этим положением были установлены требования к кредитным организациям по эмиссии банковских карт, правила осуществления расчетов и порядок учета кредитными организациями операций, совершаемых с использованием банковских карт. Указанный нормативный акт отразил практически все аспекты организации и осуществления расчетов с использованием банковских карт.

В декабре 2004 г. ЦБ РФ было выпущено Положение № 266-П «Об эмиссии банковских карт и об операциях, совершаемых с использованием платежных карт», дополняющее Положение № 23-П и действующее до настоящего времени. Требования к членам платежной системы MasterCard Worldwide, описываются в периодически обновляемой группе документов MSP (Member Service Provider) Rules Manual («Руководство по правилам для членов»), к этой группе документов ежегодно выходят дополнения и изменения в виде документа MSP Rules Manual Update.

Платежная система Visa International также периодически выпускает инструкции по организации процесса работы с ее картами. Требования Visa выпускаются в виде двух документов: Visa International Operating Regulations и Visa Regional Operating Regulations.

Первый документ содержит глобальные правила участия в платежной системе, правила по управлению рисками, требования к эмитентам карт, правила по выпуску карт, проведения торговых операций и способы разрешения споров. Второй документ вносит изменения и дополнения к первому для каждого из регионов. Россия входит в выделенный Visa регион CEMEA (Central and Eastern Europe, Middle East, and Africa - Центральная и Восточная Европа, Средний Восток и Африка).

В этом документе указаны суммы лимитов транзакций и платежей в рублях, внесены отдельные поправки к правилам проведения транзакций (например, разрешены в большинстве случаев транзакции в валюте, отличной от рублей).

О стандарте PCI DSS. Этот термин наиболее часто используется в связи с деятельностью Payment Card Industry Security Standards Council (Совет по стандартам в области безопасности платежных карт). Это независимый совет, первоначально сформированный American Express, Discover Financial Services, JCB, MasterCard Worldwide и Visa International в целях управления развитием стандартов по безопасности данных PCI (Payment Card Industry Data Security Standard — PCI DSS). Компании, занимающиеся процессингом, т. е., выпуском платежных карт, хранением данных о картах, передачей данных о платежах с использованием платежных карт, должны соблюдать требования PCI DSS. Иначе они рискуют быть оштрафованными и лишенными лицензии. Организации, работающие с платежными картами, должны периодически подтверждать свое соответствие требованиям PCI. Эта проверка соответствия проводится аудиторами - людьми, которые явля-

ются сертифицированными экспертами PCI DSS (QSAs). Текущая версия стандарта определяет 12 требований, разделенных на 6 логически связанных групп. Перечислим эти группы и требования.

1. Построение и обслуживание безопасной сети:

- установите и поддерживайте средства межсетевой защиты, чтобы защитить данные о владельцах платежных карт;
- не используйте поставляемые продавцом значения по умолчанию для системных паролей и других параметров безопасности.

2. Защита данных о владельцах платежных карт:

- защитите хранящиеся данные о владельцах платежных карт;
- зашифруйте данные о владельцах платежных карт при передаче их через открытые сети общего пользования.

3. Поддержка программ мониторинга уязвимостей:

- используйте и регулярно обновляйте антивирусное программное обеспечение;
- разрабатывайте и поддерживайте устойчивые системы и приложения.

4. Контроль доступа к информации:

- ограничьте доступ к данным о владельцах платежных карт по принципу необходимого знания (предоставление доступа только к тем данным, которые безусловно необходимы сотруднику для выполнения его функций);
- назначьте уникальный идентификатор (логин) для каждого пользователя для доступа к компьютерам;
- ограничьте физический доступ к данным о владельцах платежных карт.

5. Использование средства мониторинга и тестирования сетей:

- следите за доступом ко всем сетевым ресурсам и данным о владельцах платежных карт;
- регулярно тестируйте системы безопасности.

6. Поддержка политики информационной безопасности:

- разработайте и поддерживайте политику, направленную на осуществление информационной безопасности.

Соответственно стандарту PCI DSS в параметрах конфигурации сетевых компонент ИС должны быть указаны:

- конфигурация параметров файрвола;
- отсутствие использования умолчаний для системных паролей и других параметров защиты от НСД;
- защита хранимой информации во время передачи транзакции;

- кодирование информации при передаче через публичные сети;
- использование и регулярное обновление антивирусов, например, для устройств под управлением ОС IOS;
- предоставление уникального идентификатора каждому пользователю на сетевом устройстве;
- контроль доступа к сетевым ресурсам;
- регулярный запуск тестов системы защиты от НСД возможными средствами управляющей системы.

При конфигурации ИС с точки зрения безопасности следует помнить, что лучший способ ее обеспечения – выполнять правильно все ее процедуры, определенные во всех компонентах ИС.

10. АДМИНИСТРИРОВАНИЕ ПРОЦЕССА ПОИСКА И ДИАГНОСТИКИ ОШИБОК

Процесс поиска и диагностики ошибок в ИС может быть чрезвычайно сложным и многосторонним. В данном случае он будет рассматриваться на основе поиска и диагностики ошибок сетевых систем. Но поскольку практически любой специалист по информационным технологиям сталкивается в настоящее время со средой протоколов TCP/IP, особое внимание и место в этой главе уделено практическому решению проблем, возникающих при их использовании. Как уже отмечалось, администрирование систем осуществляется на основе различных моделей управления, а администрирование сетевых систем - на основе модели FCAPS, согласно которой, все аспекты управления сетью могут быть описаны с помощью пяти областей управления.

Как уже отмечалось, рекомендации ITU-T X.700 и близкий к ним стандарт ISO 7498-4 делят задачи системы управления на пять функциональных групп:

(F) Fault Management (управление отказами) - обнаружение отказов в устройствах сети, сопоставление аварийной информации от различных устройств, локализация отказов и инициирование корректирующих действий.

(C) Configuration Management (управление конфигурированием) - возможность отслеживания изменений, конфигурирования, передачи и установки программного обеспечения на всех устройствах сети.

(A) Accounting Management (управление учетом) - возможность сбора и передачи учетной информации для генерации отчетов об использовании сетевых ресурсов.

(P) Performance Management (управление производительностью) - непрерывный источник информации для мониторинга показателей работы сети (QoS, ToS) и распределения сетевых ресурсов.

(S) Security Management (управление безопасностью) - возможность управления доступом к сетевым ресурсам.

Здесь рассматриваются вопросы первой группы - управление администрацией системы отказами и соответствующие действия по поиску и диагностике ошибок системы, приводящих к отказам или ухудшению производительности системы.

10.1. Задачи функциональной группы F

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 знаний и опыта администратора системы. Фильтрация позволяет выделить только важные сообщения из весьма интенсивного потока сообщений об ошибках, который обычно наблюдается в большой сети. 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 в системе может быть **автоматическим** и **полуавтоматическим.** При автоматическом устранении ошибок ИС непосредственно управляет оборудованием или программными комплексами и обходит отказавший элемент за счет резервных каналов или специальных технологий, например, протоколов. В полуавтоматическом режиме основные решения и действия по устранению неисправности выполняют службы администратора системы, а специализированная система управления MS (Management System) только помогает в организации этого процесса, например, оформляет квитанции на выполнение работ и отслеживает их поэтапное выполнение. Система MS - это специализированное программное обеспечение (ПО), например, HP Open View, которое ведет журнал ошибок, собирает статистику, фиксирует конфигурации средств системы, опознает тревожные ситуации. Но это ПО только помогает администратору системы и не устраняет аппаратные или кабельные проблемы. Для управления только сетевыми системами используют NMS (Network Management System). Обычно при реализации своих функций NMS использует протокол SNMP.

Дадим пояснения к схеме работы NMS. SYSLOG - это сервер, который собирает все журналы (логи) системы, например, журнал ошибок, журнал сообщений. На коммутаторе работает программный продукт - SNMP-агент, который посылает информацию о своей деятельности по протоколу SNMP специальному серверу NMS, где работает другой программный продукт - SNMP-менеджер. Агенты SNMP могут работать и на файл-сервере (FS) и на сервере БД (DBS). Информация собирается менеджером в БД MIB для дальнейшего анализа и соответствующих действий администратора системы и NMS.

В группе задач F иногда выделяют особую подгруппу задач управления проблемами, подразумевая под проблемой сложную ситуацию, требующую для разрешения обязательного привлечения квалифицированных администраторов систем и технических служб для решения вопросов в ручном режиме. То есть проблема разрешается без NMS с использованием дополнительных программных и аппаратных средств

(протокольных анализаторов, генераторов сетевого трафика, эмуляционных продуктов).

В модели FCAPS идентифицировано 12 задач управления администратора системы как необходимых для успешной работы по управлению отказами и поиску ошибок. К ним относятся:

1) определение ошибки;
2) коррекция ошибки;
3) изоляция ошибки;
4) восстановление после ошибки;
5) поддержка тревожных сигналов (alarms);
6) фильтрация тревожных сигналов;
7) генерация тревожных сигналов;
8) проблема объяснения ошибки (корреляция);
9) проведение диагностических тестов;
10) ведение журнала ошибок;
11) сбор статистики ошибок;
12) сопровождение ошибок.

Эти задачи обычно в том или ином объеме решаются системой управления, используемой администратором системы. Однако АС должен понимать, что управляющая система помогает ему, а не думает за него. Помимо управляющей системы, а также в ситуации, когда она не используется вовсе, АС должен пользоваться моделью поиска ошибок, которую рекомендуют обычно разработчики операционных систем.

10.2. Базовая модель поиска ошибок

Базовая модель поиска ошибок предусматривает последовательное выполнение администратором системы следующих действий.

1. *Убедиться в том, что ошибки действительно есть.* Другими словами, после сообщения пользователя о некорректной работе ИС надо убедиться в том, что этот пользователь выполняет все процедуры корректно и правильно оценивает работу ИС. Например, некая операция действительно занимает много времени, а пользователь считает, что ИС медленно работает.

2. *Провести инвентаризацию.* Это означает, что необходимо выяснить, все ли части ИС на месте: все кабели существуют, все части ИС взаимодействуют и правильно соединены. При этом NMS может помочь провести автоматический опрос параметров работы оборудования и программного обеспечения, дать план системы. У администратора системы должна быть исполнительная документация по ИС с картой сети

и списками всех параметров загрузки серверов, рабочих станций, коммутационного оборудования (worksheet). Нужно убедиться в том, что «все на месте» и соответствует документации.

3. *Сделать копии ИС (backup).* Причем желательно это делать «быстрыми средствами» (например, не утилитой копирования СУБД, а утилитами ОС «том в том» или «диск в диск»).

4. *Сделать перезагрузку всех компонент ИС (restart).* Есть два режима перезагрузки: холодный режим (с отключением питания) и горячий режим (без отключения питания). При холодном рестарте заново загружается все ПО оборудования, все драйверы, все процессы ОС и СУБД, заново инициализируется память серверов. Поэтому при ошибочных ситуациях надо использовать холодный рестарт. Однако если есть ошибки оборудования, то оно после этого может вообще не загрузиться. Перед перезагрузкой нужна не забыть завершить работу всех процессов различных ОС и СУБД (обычно команды типа Down или Shutdown).

5. *После перезагрузки необходимо упростить работу ИС*, например, завершить работу всех резидентных программ, не обязательных для работы в простейшем варианте ИС.

6. *Если система загрузилась, нужно проверить права и привилегии работающих пользователей* (например, одно приложение запускается и работает нормально с данными правами пользователя, а другое нет).

7. *Надо убедиться, что версии программного обеспечения являются текущими.* Следует работать не на последней версии продуктов, а на стабильной, хорошо отлаженной. Нужно убедиться в том, что никто из пользователей не поставил себе никаких обновлений программного обеспечения. Хотя при правильных действиях АС и NMS такой возможности у пользователя не должно быть.

8. *Только после всех перечисленных действий надо собирать информацию об ошибке.* Для этого следует проанализировать журналы ИС (логи). Выявить симптомы проблемы, а также тех, кто был ею затронут, проанализировать использование процессов во время возникновения ошибки, изменения, произошедшие в системе, после которых появились сообщения об ошибке в журналах.

9. *Необходимо разработать план по изоляции ошибки.* Для этого строятся гипотезы о причинах ошибки в ИС. Это могут быть ошибки каналов связи (80% всех ошибок), аппаратные ошибки, ошибки системного программного обеспечения, прикладного программного обеспечения. Всегда следует учитывать, что тираж аппаратных средств больше,

чем тираж программных продуктов. Например, процессоров Intel выпускается больше, чем установок какой-либо одной ОС, поэтому аппаратных ошибок будет меньше, чем программных. Аналогично тираж системного программного обеспечения больше, чем тираж прикладного ПО, поэтому в первом меньше ошибок, чем в последнем. Просто чем больше тираж продукта, тем лучше он отлажен.

10. *После разработки плана по изоляции ошибки следует ранжировать гипотезы по вероятности их подтверждения.* Начинать проверку целесообразно не с самой вероятной гипотезы, а с той, которую можно быстрее всего проверить. Тем самым можно быстро отсечь часть гипотез и сузить процесс проверки.

11. *Затем гипотезы проверяются по очереди (строго по одной в единицу времени), в определенной последовательности.* В восходящем направлении — от рабочей станции к коммутационной аппаратуре или серверу либо в нисходящем направлении — от сервера или коммутационной аппаратуры к рабочей станции. Для проверки используются только специальные проверенные версии программных продуктов, специальные тестовые кабели и проверенные надежные тестовые диагностические средства.

12. *Наконец, последним действием является документирование проблемы и способа ее решения в специальном журнале.* Обязательно должны быть созданы инструкции службам администратора системы по действиям, предотвращающим повторное появление проблемы.

10.3. Стратегии определения ошибок

Существуют два подхода к поиску неисправностей - теоретический и практический.

При **теоретическом** подходе специалист-теоретик анализирует ситуацию до тех пор, пока не будет найдена точная причина ошибки. При таком решении, например, сетевой проблемы требуется современный высокопроизводительный протокольный анализатор для набора и анализа огромного количества сетевого трафика в течение значительного времени. Затем сетевому специалисту необходим длительный теоретический анализ данных. Этот процесс надежен, однако не многие компании могут себе позволить, чтобы их ИС или сеть не функционировала в течение нескольких часов или даже дней.

При **практическом** подходе опыт специалиста-практика подсказывает, что при возникновении неисправности целесообразно начинать менять сетевые платы, кабели, аппаратные средства и программное обеспечение до тех пор, пока система не начнет работать. Это вовсе не

означает, что все компоненты системы функционируют должным образом, главное, что они вообще функционируют. К сожалению, во многих руководствах по эксплуатации в разделе поиска неисправностей фактически рекомендуется прибегнуть к стилю специалиста-практика, вместо предоставления подробной инструкции по устранению технических неисправностей. Этот подход быстрее предыдущего. Однако он очень ненадежен и первопричина неработоспособности системы может быть так и не устранена.

Ни тот, ни другой метод чаще всего не дают желаемых результатов при поиске и устранении неисправностей. Поэтому действия администратора системы должны базироваться на стратегии управления ошибками.

Стратегия управления ошибками может быть проактивной либо реактивной. С ростом объема ИС возрастает потребность в ее надежности и, соответственно, возрастает потребность в предварительном мониторинге производительности системы, предупреждениях пользователям о возможных проблемах, постоянной бдительности администратора системы. Такая стратегия предупреждения ошибок называется проактивной. Стратегия, при которой АС не предупреждает появление ошибок, а разбирается с ошибками по мере их возникновения, называется реактивной. АС должен приложить усилия и воспользоваться средствами MS или NMS для перехода от реактивной стратегии к проактивной.

Обычно систем ы управления отказами (ошибками) - NMS разбивают сложную задачу идентификации и диагностики ошибки на четыре подзадачи:

- определение ошибки;
- генерация тревожного сигнала;
- изоляция ошибки;
- коррекция ошибки.

При этом возможны две технологии работы NMS - пассивная и активная.

Пассивная технология. С помощью протокола SNMP устройства оповещают управляющую систему о выполнении заранее предусмотренного и заданного параметрами системы условия, например, отличие какого-либо параметра от номинального значения. Эта технология должна применяться администратором системы при идентификации проблем, не связанных с аппаратными сбоями, например, при изменении производительности, проблемах интерфейсов и т. д.

Активная технология. Система NMS тестирует ИС (например, с помощью утилиты PING) и опрашивает каждое из устройств на регулярной основе. Если какое-либо устройство не реагирует в заданный администратором системы интервал времени или его параметры отличаются от желаемых, посылается сообщение администратору системы о сбое устройства.

АС должен выбрать систему управления, позволяющую использовать обе стратегии. Кроме того, правильно спроектированная система управления дает возможность администратору системы выполнять далее перечисленные логические действия по управлению ошибками.

• *Выбрать время, когда управление ошибками осуществляется полностью, не осуществляется вовсе или осуществляется частично.* Время работы ИС определяется в специальном документе - соглашении об уровне сервиса SLA (Service Level Agreement). И это время может отличаться от часов работы данного предприятия. Например, предприятие работает с 9.00 до 18.00, а ИС работает 24 часа, 7 дней в неделю и 365 дней в году. Часть времени ИС может быть занято под специальные действия, не требующие контроля над возможными ошибками. Это можно указать в параметрах настройки MS. Например, мониторинг ошибок проводится в течение 20 из 24 часов. Если это требование выполняется, считается, что ошибок нет.

• *При настройке MS создать специальные триггеры, определяющие, какую ситуацию в данной системе следует рассматривать как ошибочную.* В некоторых случаях надо подавлять сообщения об ошибках. Например, сообщение о том, что производительность упала на 0,5%, что не существенно для большинства систем.

• *Настроить параметры автоматической перезагрузки системы и переустановки параметров (reset).* Можно настроить параметры MS так, чтобы в определенных случаях система сама перезагружалась и устанавливала определенные параметры в номинальные значения.

• *Установить подавление предупреждений об ошибках в некоторых случаях.* Например, если известен дефект работы устройства, но он не влияет на работу ИС.

10.4. Средства администратора по сбору и поиску ошибок

Помимо управляющих систем (MS и NMS) существует ряд средств диагностики ошибок, необходимых службам администратора системы. Рассмотрим эти средства.

Средства ОС и СУБД. В составе любой ОС и СУБД всегда есть специализированные утилиты (возможно, модули ядра) или утилита «Монитор». Это программные продукты, запускаемые на файл-сервере либо на сервере БД, либо на специализированных выделенных серверах под управлением ОС. Монитор или мониторы позволяют собирать статистику ошибок, анализировать их, выдавать предупреждения администратору системы о сбоях и т.д. Эти утилиты частично выполняют функции MS или NMS. Загружаются они при загрузке ОС либо при запуске приложения (сессии приложения), либо при запуске ядра СУБД.

Средства эмуляции предназначены для эмуляции системной консоли оборудования в удаленном варианте. Они обычно входят в состав любой операционной системы и используются, например, для управления консолью любого сетевого оборудования с персонального компьютера администратора системы. Существует промышленный стандарт на такую эмуляцию, реализованный в программах Telnet и SSH. Программное обеспечение Telnet первоначально использовалось на UNIX-серверах и предназначено для конфигурации и администрирования сетевых устройств с машины администратора системы.

Работает продукт на третьем и четвертом уровнях модели OSI. Его можно применять в целях удаленного управления только в том случае, если АС уверен в отсутствии сетевых ошибок или в отсутствии необходимости обновления параметров. SSH используется в тех же целях, но в продукте реализована часть функций защиты от несанкционированного доступа при его применении. Они используют в своей работе только возможности серийного порта и кабеля, запускаются на станции администратора системы, присоединяемой непосредственно по интерфейсу физического уровня модели OSI к сетевому устройству. В этом случае нет вероятности сетевой ошибки, которая в свою очередь помешала бы исправлению ошибки, обнаруженной администратором системы.

Дополнительные продукты используются для активного поиска ошибок в быстром режиме, например: анализаторы протоколов для сетевых систем, эмуляторы трафика (для эмуляции загрузки ИС), симуляторы атак (для проверки защиты от НСД), симуляторы ошибок (для проверки защищенности ИС от ошибок).

Специализированные утилиты используются для тестирования ИС с помощью средств ОС или СУБД, например, утилиты Ping или Traceroot.

Заключение

Процесс администрирования ИС – это достаточно трудоемкий процесс, который требует больших усилий по мере роста системы.

Помимо необходимости больших усилий по сопровождению резко возрастает время, затрачиваемое службами администратора системы, на обучение пользователей и обслуживающего ИС персонала.

Все новые компьютерные технологии, такие как мобильные сети или центры обработки данных, используются при построении ИС, создавая большие возможности для реализации прикладных функций. Но, к сожалению, они же чрезвычайно усложняют и диверсифицируют ИС. Крупные компьютерные компании - производители программных или аппаратных средств обычно предлагают свои стратегии администрирования и свою архитектуру управляющих систем, часто не совпадающие с реализациями других производителей.

Постоянно происходит развитие моделей управления ИС и соответствующих протоколов. Стандартизирующими организациями и компьютерными сообществами обновляются или создаются стандарты в различных областях реализации ИС. АС должен владеть знаниями как существующих технологий и методов их администрирования, так и новых технологий, а также способами обеспечения их сосуществования со старыми технологиями. Развитие инструментария для реализации управляющих систем также происходит постоянно.

Несмотря на стремительное развитие технических средств, для служб администратора системы всегда останутся проблемы организационные и «политические», решение которых требует немало времени и сил, а проблема постоянного повышения квалификации и компетенции администратора системы в безграничной области информационных технологий останется ключевой.

Библиографический список

1. **Беленькая М.Н., Малиновский С.Т., Яковенко Н.В.** Администрирование в информационных системах. Учебное пособие для вузов. - М.: Горячая линия - Телеком, 2011. - 400 с., ил. - ISBN 978-5-9912-0164-3.
2. **Кофлер М.** Linux. Установка, настройка, администрирование. - СПб.: Питер, 2014. - 768 с.: ил. - ISBN 978-5-496-00862-4.
3. **Моримото, Рэнд, Ноэл, Майкл, Ярдени, Гай, и др.** Microsoft Windows Server 2012. Полное руководство. : Пер. с англ. — М.: ООО "И.Д. Вильямс", 2013. - 1456 с. : ил. — Парал. тит. англ. - ISBN 978-5-8459-1848-2 (рус.).

Учебное издание

Михайлов Владимир Вячеславович

АДМИНИСТРИРОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ

Конспект лекций

Подписано в печать 30.06.17. Формат 60x84/16. Усл. печ. л. 6,5. Уч.-изд. л. 7,0.
Тираж 85 экз. Заказ Цена
Отпечатано в Белгородском государственном технологическом университете им. В. Г. Шухова
308012, г. Белгород, ул. Костюкова, 46