Александр Кенин

САМОУЧИТЕЛЬ СИСТЕМНОГО АДМИНИСТРАТОРА

2-е издание

Санкт-Петербург
«БХВ-Петербург»
2008

УДК 681.3.06
ББК 32.973.26-018.2
К35

Кенин А. М.

К35 Самоучитель системного администратора. — 2-е изд., перераб. и доп. — СПб.: БХВ-Петербург, 2008. — 560 с.: ил. — (Системный администратор)

ISBN 978-5-9775-0170-5

Изложены основные задачи системного администрирования, подробно описаны технологии, используемые при построении информационных систем, способы построения и обслуживания как одноранговых сетей (домашних и на малых предприятиях), так и сетей с централизованным управлением. Рассмотрены вопросы управления с помощью групповых политик, организации почтового обслуживания, взаимодействия с Интернетом, основы создания безопасной информационной системы, настройки и определения неисправностей, шифрования сообщений, создания электронных подписей и использования средств управления компьютерными системами. Книга написана на основе многолетнего опыта администрирования компьютерных сетей.

Второе издание дополнено описаниями принципов построения логической структуры сети, включены новые разделы по виртуализации и использованию систем на основе Linux в доменах Windows. С учетом предложений читателей доработаны разделы информационной безопасности и автоматизации разворачивания программ.

Для начинающих системных администраторов

УДК 681.3.06
ББК 32.973.26-018.2

Группа подготовки издания:

Главный редактор	*Екатерина Кондукова*
Зам. главного редактора	*Евгений Рыбаков*
Зав. редакцией	*Григорий Добин*
Редактор	*Ирина Артемьева*
Компьютерная верстка	*Ольги Сергиенко*
Корректор	*Зинаида Дмитриева*
Дизайн серии	*Инны Тачиной*
Оформление обложки	*Елены Беляевой*
Зав. производством	*Николай Тверских*

Лицензия ИД № 02429 от 24.07.00. Подписано в печать 30.11.07.
Формат 70×100 1/16. Печать офсетная. Усл. печ. л. 45,15.
Тираж 3000 экз. Заказ №
"БХВ-Петербург", 194354, Санкт-Петербург, ул. Есенина, 5Б.

Санитарно-эпидемиологическое заключение на продукцию
№ 77.99.02.953.Д.006421.11.04 от 11.11.2004 г. выдано Федеральной службой
по надзору в сфере защиты прав потребителей и благополучия человека.

Отпечатано с готовых диапозитивов
в ГУП "Типография "Наука"
199034, Санкт-Петербург, 9 линия, 12

ISBN 978-5-9775-0170-5

© Кенин А. М., 2008
© Оформление, издательство "БХВ-Петербург", 2008

Оглавление

Предисловие **13**

Глава 1. Системное администрирование **15**

Системный администратор 15
Регламент работы 16
Открытые стандарты 17
Конкурсы 18
Переход на новые версии программного обеспечения 18
Сертификация 19
Немного этики 20
О мистике 21

Глава 2. Решения на открытых кодах **23**

Мифы 23
- Миф 1. Linux — это система, которой надо обучаться 23
- Миф 2. Linux — это сложная система, собирать которую придется самостоятельно 25
- Миф 3. Linux — работа в командной строке? 25
- Безопасность в Linux и Windows 26
- Стоимость владения 27
- Несколько моментов, о которых следует знать 27
- Структура папок Linux 30
- Текстовый редактор vi 31
- Проблемы с графической средой 32
- Выполнение команд с правами другого пользователя 33
- Программное обеспечение рабочего места 33

Установка Linux 34
- Многовариантная загрузка 34
- Тестирование Linux на виртуальной машине 36

Работа с ресурсами домена: Samba 37
Установка 38
Подключение к домену (Kerberos) 39
Предоставление ресурсов в общий доступ 42
Учетная запись *Гость* 44
Подключение к общим ресурсам 44
Сервер Linux в качестве контроллера домена 44
Межсетевой экран iptables 45
Настройки запуска 45
Программы графического управления iptables 46
Принципы работы iptables 48
Создание правил межсетевого экрана 49
Аутентификация доступа в Интернет 51
Squid 52
Некоторые дополнительные настройки iptables 53
Почтовый сервер 54
Удаленное подключение к Linux 55
OpenSSH-сервер 55
Подключение OpenSSH-клиента 55
Использование графического режима 56

Глава 3. Структура сети 57

Структурированные кабельные сети 57
Категории СКС 57
Волоконно-оптические сети 58
Сети 10G 59
Схема разъема RJ45 60
Варианты исполнения СКС 62
Внимание: патч-корды 62
Составные линии 62
Прокладка силовых кабелей 63
Питание по сети Ethernet 63
Требования пожарной безопасности 64
Физическая топология сети здания 65
Логическая структура сети 70
Маршрутизация в сетях предприятий 73
Надежность сетевой инфраструктуры 77
Качество обслуживания в сетях предприятия 83
Тестирование каналов связи 83
Приоритезация трафика 85
Беспроводные сети 90
Стандарты беспроводной сети 91
Проектирование беспроводной сети предприятия 91
Безопасность беспроводной сети 93

Терминология компьютерной сети ... 96
Протоколы ... 96
Модель OSI ... 97
Стек протоколов TCP/IP ... 98
IPv6 ... 99
Параметры TCP/IP протокола ... 100
Настройка серверов WINS, DHCP, DNS ... 126

Глава 4. Компьютерные сети малых предприятий ... 151

Домашние сети ... 151
Одноранговые сети ... 153
Выбор операционной системы ... 153
Microsoft Windows Fundamentals for Legacy PCs ... 154

Глава 5. Сеть с централизованным управлением ... 155

Управление локальными ресурсами ... 155
Возможность добавлять рабочие станции в домен ... 156
Изменения настроек системы при подключении ее к домену ... 157
Методы управления локальной системой ... 158
"Кто кого": локальный или доменный администратор ... 160
Проблема аудитора ... 163
Каталог ... 163
Домены Windows ... 164
Служба каталогов Windows (Active Directory) ... 165
Управление структурой домена предприятия ... 171
Создание нового домена ... 172
Переименование домена ... 175
Утилиты управления объектами службы каталогов ... 176
Делегирование прав ... 181
Просмотр и восстановление удаленных объектов каталога ... 183
Распределенная файловая структура ... 186
Создание DFS ... 187
Репликация DFS ... 187
Учетные записи и права ... 189
Понятие учетной записи ... 189
Локальные и доменные учетные записи ... 191
Группы пользователей ... 192
Создание и удаление учетных записей ... 203
Права учетной записи ... 205
Автоматически создаваемые учетные записи ... 207
Учетная запись *Система* ... 209
Встроенные группы ... 210
Ролевое управление ... 214

Глава 6. Управление с помощью групповых политик 215

Групповые и системные политики 216
Порядок применения политик и разрешения конфликтов 218
"Обход" параметров пользователя 219
Время применения политик 220
Последствия отключений политик 220
Рекомендации по применению политик 221
Контейнеры *Computers* и *Users* 221
Рекомендации по применению групповых политик 222
Политики по установке программного обеспечения 222
Политики ограниченного использования программ 224
Административные шаблоны 230
Редактирование параметров безопасности 231
GPO-консоль 231

Глава 7. Организация почтового обслуживания 233

Основы пересылки почтовых сообщений 233
Используемые протоколы 236
SMTP 236
POP3 237
IMAP 237
HTTP 237
RPC 238
Пример "прямой" проверки почтового сервера 238
Установка почтового сервера организации 242
Создание внутрикорпоративной почты малых организаций 242
Установка корпоративного почтового сервера Интернета 244
Антивирусная защита почтовых сообщений 246
Пересылка файлов в письме 246
Проверка сообщений на почтовом сервере 247
Спам 248
Способы борьбы со спамом 248
Безопасность электронной почты 256
Получение сертификата 256
Электронная подпись 257
Шифрование текста 258

Глава 8. Взаимодействие с глобальной сетью 261

Защита информационных систем 261
NAT 263
Межсетевой экран (брандмауэр) 264
Что может брандмауэр и чего не стоит от него ожидать? 265
Учитываемые параметры фильтрации 265
Варианты организации брандмауэров 266

Intrusion Prevention Systems 267
Защищенный доступ в сеть 269
Варианты брандмауэров 271
Настройка параметров МСЭ при помощи групповой политики 275
Совместное использование интернет-подключения 278
Публикация компьютеров в Интернете при совместном использовании подключения 279
Ограничения совместного использования подключения к Интернету 281
Как снизить затраты на доступ в Интернет? 282
Удаленная работа 283
Удаленное подключение пользователей 284
Терминальный доступ 294
Создание локальных копий данных на мобильных устройствах 305

Глава 9. Безопасность 311

Удобство в работе и безопасность. Человеческий фактор 312
Интернет-ресурсы, посвященные безопасности 312
Анализ рисков 314
Три "кита" безопасности 316
Основные направления работ по защите информационной системы 317
Организационное обеспечение информационной безопасности 317
Индивидуальная настройка серверов 318
Security Configuration Manager 319
Обеспечение сетевой безопасности информационной системы 319
Фильтрация по MAC-адресам 320
Протокол 802.1x 321
Безопасность приложений 329
План обеспечения непрерывности функционирования информационной системы 330
Volume Shadow Copy 330
Устройства хранения данных 332
Типы операций резервного копирования 332
Объекты резервного копирования 334
Automated System Recovery 335
Копирование образов диска 336
Необходимые права для операции backup 338
Восстановление данных 339
Резервное копирование и восстановление зашифрованных данных 339
Восстановление контроллера домена 340
Создание копий информации отдельных служб 341
Системы непрерывного копирования данных 342
Защита от вредоносных программ и вторжений 343
Антивирусные программы 343
Защита от вторжений 348
Защита от постороннего кода 349

Обнаружение нештатной сетевой активности 355
Защита от использования ошибок программного кода 356
Бесконечный процесс обновлений 356
Где узнать о необходимости установки обновления? 357
Тестирование 360
Способы обновления операционных систем 361
Интеграция обновлений ПО 369
Физическая безопасность 371
Ограничения доступа к станциям 371
Меры защиты от копирования 372
Шифрование данных на компьютере 373
Шифрование папок и файлов 373
Подводные камни технологии шифрования 375
Создание временно подключаемых шифрованных дисков 376
Шифрование диска 376
Безопасность паролей 381
Мифы и реальности парольной защиты 381
Варианты восстановления забытых паролей 382
Рекомендации по составлению сложного пароля 384
Технические пути решения проблемы 385
Восстановление пароля администратора 390
Человеческий фактор 391

Глава 10. Виртуализация 393

Программы виртуальных машин 394
Виртуальный сервер или рабочая станция 394
Лицензирование программного обеспечения виртуальных машин 395
Ресурсы виртуальных машин 396
Жесткие диски 396
Процессор 398
64 и 32 398
Оперативная память 398
CD/DVD 399
Сетевые адаптеры 399
Порты 400
Безопасность 400
Расширения виртуальных машин 401
Автоматический запуск виртуальных машин 402
Выключение виртуальных машин 402
Операции в виртуальных машинах 403
Копирование 403
Подключение папки основного компьютера к виртуальной системе 403
Подключение CD, дискет и других устройств чтения/записи 404
Сочетание управляющих клавиш 404

Совместимость программного обеспечения с виртуальными системами 404
Создание виртуальных машин 405
Миграция компьютера на виртуальную машину 405
Создание виртуального диска как копии физического 406
Контроль параметров производительности 407
Счетчики производительности 407
Советы по повышению производительности виртуальных систем 407

Глава 11. Порядок настройки и определения неисправностей 409

Прежде чем начать... 409
Пять девяток 410
Где найти помощь 412
Обнаружение неисправностей сетевой инфраструктуры 414
Неисправности аппаратной части компьютера 417
Контроль теплового режима работы системы 418
Восстановление данных с жестких дисков 419
Восстановление "упавших" систем 420
Восстановление удаленных данных 428
Аудит 432
Протоколирование работы системы 433
Просмотр журналов системы 433
Настройка параметров журналов 435
Протоколирование пользовательских событий 436
Автоматизация реагирования на события журнала 437
Настройка аудита событий безопасности 437
Настройка дополнительного протоколирования 438
Анализ производительности 438
Задача *Производительность* 444
Счетчики состояния системы 444
Основные узкие места системы 445
Дополнительные возможности Vista 451
Server Performance Advisor 452
Диагностика доступа к ресурсам компьютера 453
Диагностика службы каталогов 454
Обнаружение неисправностей AD 455

Глава 12. Цифровые сертификаты 459

Симметричное шифрование 459
Шифрование с помощью двух ключей 460
Цифровой сертификат 462
Структура Public Key Infrastructure 463
Центр сертификации 463
Доверенные центры сертификации 464
Установка центра сертификации 465
Настройка центра сертификации 466

Публикация шаблонов сертификатов 467
Резервное копирование центра сертификации 468
Отзыв сертификатов 470
Получение цифровых сертификатов 470
Корпоративная политика управления сертификатами 474
Настройка хранения закрытых ключей пользователей 474
Порядок восстановления закрытых ключей 476
Электронная подпись 477
Шифрование документов 478
Электронная подпись документа MS Office 478
Электронные подписи программных кодов 479
Pretty Good Privacy 482
Защищенные каналы связи 483
Secure Sockets Layer 483
Secure Channel 484
Internet Protocol security 485
Служба управления правами (RMS) 492
Принципы работы службы управления правами 493
Установка сервера RMS 494
Ограничения RMS 494

Глава 13. Средства управления системами 495

Инвентаризация 495
Учет компьютеров и программ 495
Построение логической структуры СКС 496
Инвентаризация физических каналов связи 498
Контроль функционирования ПО 499
ПО управления серверами от вендоров 499
Службы технической поддержки производителей 500
Intelligent Platform Management Interface 501
Методы управления компьютерной сетью 503
Windows Scripting Host 503
Windows Management Interface 506
Контроль функционирования систем. Microsoft Operation Management Server 510
Контроль прикладного ПО 513
Удаленное администрирование 514
Microsoft System Management Server 518
Отдельные утилиты третьих фирм 519
Утилиты от Sysinternals 519
ПО восстановления системы 519
ПО инвентаризации систем 519
Утилиты дефрагментации дисков 520
Снифферы 520
Программы очистки диска 522

Глава 14. Автоматизация установки программного обеспечения 523

Автоматизация процесса установки 523
Установка прикладного ПО 523
Варианты запуска программы установки 526
Ограничения устанавливаемого ПО 532
Клонирование рабочих станций 532
Перенос информационной системы на новое оборудование 533
Дублирование жесткого диска 534
Автоматическая удаленная установка систем Microsoft 539
Сравнение различных вариантов клонирования систем 543

Приложение 545

Ежедневные операции 545
Еженедельные операции 547
Плановые операции другой периодичности 547
План-отчет операций 548

Предметный указатель 551

Предисловие

Эта книга написана для всех тех, кто занимается созданием и эксплуатацией информационных систем. Создавая книгу, я не ставил перед собой задачу описания последовательности нажатия тех или иных кнопок и клавиш для достижения нужного эффекта. В первую очередь, я хотел передать свое видение и личную оценку технологий и решений, рассказать "почему и зачем", указать направление, потому что, представляя проблему, вы легко сможете при возникновении конкретных вопросов воспользоваться справочными материалами как самих программных продуктов, так и опытом пользователей Интернета.

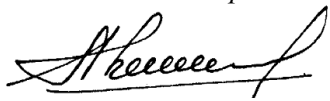
Занимаясь более 15 лет администрированием и развитием компьютерных систем, оказывая техническую поддержку, я постоянно сталкиваюсь с однотипными проблемами и вопросами пользователей и специалистов. И каждый раз я пытаюсь простыми и доходчивыми словами объяснить основы, на которых построена современная информационная система, понимая которые можно успешно контролировать ситуацию.

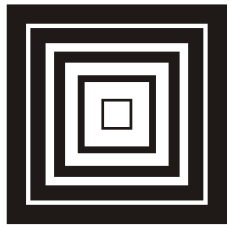
Возможно, что в некоторых местах я не академически строг. Вероятно, что некоторые читатели критически воспримут рекомендации, которые даются мною на основании, прежде всего, личного опыта. Цель книги заключается и в том, чтобы выработать у пользователя собственную позицию, а не идти на поводу рекламных материалов и заказных статей.

Я попытался осветить основную часть проблем, с которыми приходится сталкиваться системным администраторам в практической деятельности. В книгу вошли материалы и оценки по состоянию на осень 2007 г. По возможности я попытался дать ссылки на программные продукты, которые могут помочь специалистам в повседневной работе управления компьютерными системами.

Предполагается, что читатель этой книги знаком с основами компьютерных технологий. Свои замечания и предложения вы можете направлять непосредственно мне по электронной почте на адрес **kenin@hotbox.ru**.

Ваш Александр Кенин





ГЛАВА 1

Системное администрирование

Специалиста, который объединял компьютеры пользователей в единую сеть и поддерживал работоспособность такой системы, назвали *системным администратором*. В настоящее время увеличивающаяся структуризация сети, появление разнообразных прикладных программ, разработка новых сетевых служб и т. п. все более и более усложняют задачу квалифицированного управления компьютерной системой.

Системный администратор

В нашей стране практически отсутствует понимание места и роли системного администратора. В небольших организациях таковым считают работника, который в одиночку выполняет обязанности по обслуживанию компьютерного парка. В крупных организациях системными администраторами называют как специалистов, которые сопровождают рабочие места пользователей, так и сотрудников, отвечающих за функционирование тех или иных информационных систем предприятия. При этом *технического* специалиста, отвечающего за работу всей системы, как правило, в штате организации нет. Считается, что эти функции выполняют руководители отделов IT, но руководство подразделением и системное администрирование — это, как мне кажется, весьма различающиеся направления работы.

Системный администратор — это специалист, отвечающий за функционирование и развитие информационной системы. Это тот человек, который должен представлять работу всех компонентов в комплексе, в то же время понимая особенности каждого отдельного элемента. Системный администратор — высшее звено иерархии информационной системы. Он должен координировать работу и специалистов служб технической поддержки, и администраторов подразделений, и руководителей отдельных автоматизированных систем,

и офицера информационной безопасности — всех сотрудников "узкой" специализации.

Конечно, знать в совершенстве все технологии, применяемые в современных информационных системам, одному человеку практически невозможно. Как следствие этого, на крупных предприятиях создаются целые группы сотрудников, части из которых поручается только поддержание функционирования систем, другому коллективу — развитие и внедрение новых технологий, третьим — взаимодействие с пользователями и т. д. В итоге не остается специалиста, сохраняющего комплексное понимание *всех служб* сети. А на малых предприятиях, где все развитие и поддержание функционирования сети сосредоточено в одних руках, как правило, нет потребности в интегрированных сетевых решениях и отсутствуют необходимые средства, чтобы удерживать высококвалифицированного работника.

В результате системное администрирование зачастую становится только первой ступенью вхождения в компьютерный бизнес для молодых работников, которые, освоив первичные функции управления компьютерными системами, без особых раздумий о безопасности данных, надежности информации, предупреждении отказов, комфортности пользователей и т. д. — "лишь бы работало", стараются при первом же удобном случае перейти в группы разработки IT-проектов или стать продавцами программ и компьютеров. А предприятия остаются без системного администратора, вновь и вновь сталкиваясь с проблемами функционирования компьютерной системы.

Хороший системный администратор "созревает" не за один год. Многое невозможно узнать только по технической документации или по итогам специализированных курсов. Необходим опыт и, прежде всего, комплексный взгляд на систему, не затуманенный всепоглощающей рекламой того или иного производителя программного обеспечения. Нужен именно *системный* подход к *системному администрированию*.

Эта книга написана в помощь тем системным администраторам, которые дорожат своей работой, любят свою сеть и хотят получить от своей деятельности максимум эффекта. В книге не делается акцент на последовательности выполнения той или иной операции: это хорошо описано в технической документации. Я попытаюсь объяснить основные принципы, заложенные в основу тех или иных технологий, управлять которыми приходится системному администратору, а также попробую дать свое видение различных вариантов решений, с которым читатель волен согласиться или нет.

Регламент работы

Деятельность администратора — это непрерывный процесс возникновения проблем, их решения, появления новых вопросов и т. д. Качество же работы

практически пропорционально его "незаметности": чем стабильнее работает система (нет проблем у пользователей) и чем быстрее разрешаются инциденты, тем профессиональнее специалист, обслуживающий такую систему.

Во многих организациях целесообразно использовать формализованную оценку качества услуг администратора. Желательно разработать определенный регламент, который должен описывать порядок разрешения инцидентов. Например, можно определить время ввода в эксплуатацию нового компьютера, срок восстановления системы из состояния голубого экрана смерти и т. п. Чем более подробно будут классифицированы возможные ситуации, тем меньше претензий потенциально возникнет у пользователей в отношении уровня их обслуживания.

Не стоит оценивать факт наличия подобного регламента лишь с точки зрения контроля над системным администратором. Данный документ может служить аргументом, например, для переноса сроков завершения работ в случае одновременного возникновения нескольких неисправностей.

Вводя регламент, следует использовать ту или иную автоматизированную форму для фиксирования обращений пользователей и контроля их исполнения. Эта же программа может сослужить хорошую службу администраторам, только приступающим к работе в организации, в качестве базы знаний данного предприятия, по которой можно осуществлять предварительное обучение нового специалиста. Подобрать подобный продукт не составляет особого труда, поскольку большинство требований, предъявляемых на малых и средних предприятиях к данному классу ПО, реализовано в программах с открытым кодом. Достаточно выполнить поиск на сайте SourceForge.net (**http://www.sourceforge.net/**) и выбрать наиболее подходящий вариант из нескольких десятков проектов.

Открытые стандарты

На практике большинство информационных систем включает в себя компьютеры с различными операционными системами и прикладными программами. На каждом участке применяется наиболее оптимальное решение. Гарантом их работоспособности являются единые стандарты взаимодействия.

Страница Интернета может быть просмотрена в любом обозревателе — Firefox, Internet Explorer, Opera и т. д. Отсутствуют проблемы взаимной аутентификации пользователей Windows — Linux. В Windows реализован открытый стандарт Kerberos, а для взаимодействия по протоколам NTLM и т. п. имеется бесплатный продукт Samba, входящий в состав всех дистрибутивов Linux. Объединение каналов при передаче информации осуществляется на основе стандарта 803.2ad независимо от конкретной модели сетевого оборудования,

установленной в сети передачи данных. Документы, подготовленные в MS Office, открываются в OpenOffice (бесплатная офисная система, предназначенная для Linux), и наоборот.

Подобных примеров можно привести много.

В то же время многие фирмы предлагают собственные уникальные технологии для реализации в информационной системе. Применять их или нет — серьезная проблема в каждом конкретном случае. Если вы используете уникальную технологию, то обычно получаете более высокую производительность, чем при типовом решении, но оказываетесь привязанными к конкретному вендору. При этом перспектива дальнейшей поддержки технической части решения производителем часто бывает не очевидной, если, конечно, очистить предложения от рекламных слоганов.

В любом случае я бы советовал ориентироваться в первую очередь на использование решений, описанных в открытых стандартах. И только в случае невозможности такого выбора применять проприетарные технологии и разработки.

Конкурсы

Внедрение новых технических решений часто происходит на основе открытого конкурса. Системные администраторы могут оказать серьезное влияние на результаты конкурса путем формулирования технических требований, причем в открытом конкурсе можно практически заранее выбрать победителя, если конкретизировать требования до такой степени, что они могут быть выполнены только определенной моделью оборудования[1]. А можно сформулировать лишь основные, принципиальные требования проекта, рассмотреть полученные в итоге конкурса подходы к решению проблемы и выбрать оптимальный вариант.

Переход на новые версии программного обеспечения

Большинство действующих на момент подготовки книги администраторов работает в условиях, когда основной объем эксплуатируемого программного обеспечения представляет собой нелицензированные версии. Поэтому "в кро-

[1] С учетом того что вендоры предоставляют специальные скидки для конкурсов, то предприятие-партнер может предложить такие цены, которые позволят выиграть конкурс при прочих равных условиях. На практике автору не один раз приходилось сталкиваться с условиями конкурса, составленными подобным образом.

ви" живет желание применить новую версию ПО сразу после его выпуска, хотя в большинстве реальных ситуаций конечные пользователи не получат от такого перехода никаких дополнительных преимуществ. Подумайте, какие новые функции эксплуатируются в офисных программах? Подавляющему большинству пользователей достаточно тех возможностей, которые им были доступны, например, уже в MS Office 97.

В любом случае необходимо оценить выгоды, которые вы надеетесь получить от перехода на новую версию программного обеспечения, и сравнить их с затратами на эту операцию (стоимость обновления версий ПО, стоимость модернизации оборудования и т. п.). Оказывается, что очень часто можно следовать старому доброму совету: если программа работает, то не надо ее трогать.

Примечание

Конечно большое количество версий ПО, одновременно находящихся в *эксплуатации*, усложняет работу администратора. Например, необходимо следить за обновлениями всего парка ПО, устанавливать вместо одного патча два или три, загружая их из сети Интернет. Но обычно серьезных проблем такая ситуация не создает.

Сертификация

Если некоторое время назад в чести были трудовые династии, то сейчас смена работы через 2—3 года стала реальным способом увеличения заработной платы. При этом посредниками между работниками и работодателями выступают кадровые агентства, а работник зачастую оценивается только по формальным признакам. Почти повсеместно подбором и приемом персонала занимаются менеджеры, не являющиеся специалистами по кадровой работе, а оценивающие "бумажную" составляющую резюме.

Поскольку такие "правила игры" реально существуют, то системному администратору следует не забывать во время своей работы получать необходимые сертификаты. Если руководство согласно оплатить курсы обучения, на которых готовят к сдаче экзамена на такие сертификаты, — хорошо. В противном случае следует найти собственные средства для оплаты сертификации в какой-либо области.

Сертификат — то же, что и права на вождение автомобиля. Он не подтверждает, что вы *хорошо* водите машину, однако является документом, который свидетельствует в вашу пользу. Для большинства сотрудников кадровых служб количество имеющихся у вас сертификатов пропорционально возможности положительного решения, тогда как их отсутствие может стать поводом для отказа.

Примечание

И наоборот, наличие сертификата часто отнюдь не свидетельствует об уровне специалиста. Например, автору неоднократно приходилось отказывать в приеме на работу лицам, предоставлявшим многочисленные сертификаты, но в процессе собеседования не подтверждавшим указанные в них практические навыки управления системой.

Вопросы, на которые необходимо ответить во время сдачи сертификационного экзамена, составлены на основе зарубежной практики. Очень часто с ситуациями, по которым они составлены, администратору, работающему в наших организациях, сталкиваться не приходится. Поэтому наличие даже большого опыта практической работы не позволит вам сдать экзамены с первого захода. Целесообразно найти в Интернете (или магазинах) учебные пособия для подготовки к тестам и после их изучения потренироваться на реальных вопросах[1].

Немного этики

По роду своей деятельности системный администратор имеет потенциальный доступ практически ко всей информации, хранящейся на предприятии в электронном виде. И именно барьеры этического плана должны удерживать его от соблазна узнать чужую зарплату или прочесть чью-либо корреспонденцию. Корректность также имеет большое значение в работе системного администратора. Например, многим администраторам приходится применять программы, перехватывающие экран и клавиатуру компьютера пользователя. У автора данная программа настроена таким образом, что при удаленном подключении на экране пользователя *всегда* выводится соответствующее предупреждение[2].

В немалой степени от системного администратора зависят способы реализации корпоративных политик в области безопасности. С одной стороны, это желание руководителей осуществлять полный контроль над деятельностью подчиненных[3] (перлюстрация корпоративной электронной почты, контроль

---

[1] С этой целью, во-первых, можно познакомиться с материалами, публикуемыми на таких сайтах, как **http://www.braindumpcentral.com/**. Во-вторых, не очень сложно найти экзаменационные программы, пусть даже и не последней версии, на которых следует потренироваться в сдаче теста. Кроме того, для многих тестов доступны электронные учебники — см., в частности, **http://www.ebuki.apvs.ru/** (выполните, например, поиск по строке "exam").

[2] Я специально акцентирую на этом внимание, поскольку встречал в прессе высказывания "специалиста" о том, как ему нравится наблюдать за реакцией пользователей при удаленном перехвате управления, когда компьютер переставал "слушаться" владельца.

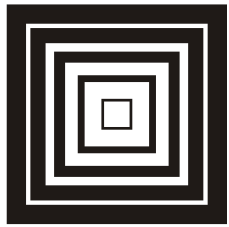
[3] По данным статистики, желание полностью контролировать сотрудников чаще всего возникает у руководителей малых предприятий.

посещения страниц Интернета и т. п.), с другой — право каждого на личную тайну.

Системный администратор *вынужден* быть дипломатом и поддерживать хорошие отношения как с руководством, так и с коллективом сотрудников, находя компромиссные решения противоречивых ситуаций.

О мистике

И в заключение. Автор неоднократно замечал взаимосвязь между своим внутренним состоянием и стабильностью работы системы. Если вы садитесь за компьютер в плохом настроении, то не ждите, что он ответит вам "полным пониманием". Если вы не станете дружески относиться к своим системам, то будьте готовы к постоянным неожиданностям.



ГЛАВА 2

Решения на открытых кодах

За рынок операционных систем для промышленных предприятий среднего и малого масштаба в настоящее время идет серьезная борьба: с одной стороны, Microsoft прикладывает значительные усилия по выходу на промышленный рынок, с другой — наблюдаются необычайно быстрые темпы роста инсталляций операционной системы Linux.

Мифы

Бесплатные операционные системы и прикладные программы являются серьезным конкурентом коммерческим продуктам. На большинстве рабочих мест можно безболезненно перейти на программы с открытым кодом. Естественно, что вокруг этой проблемы существует много рекламных спекуляций, призванных внушить пользователям и руководителям определенные представления о "правильном" пути.

Автор не ставит целью дать подробную инструкцию по работе с Linux-системами. Открытых источников очень много, и во многом они лучше того, что я смог бы предложить читателю. Постараемся просто объективно сравнить основные характеристики коммерческого и бесплатного продуктов и познакомить читателей с другим классом операционных систем, чтобы каждый смог самостоятельно составить собственное мнение о быстро развивающихся продуктах. Чтобы решение о выборе того или иного продукта было обоснованным, попытаемся рассмотреть некоторые усердно насаждаемые мифы.

Миф 1. Linux — это система, которой надо обучаться

Современные операционные системы и прикладные программы, особенно самые массовые, строятся, прежде всего, на стандартах. Как Linux, так и

Windows могут использовать одинаковые сетевые протоколы, единую пользовательскую базу (сервер с учетными записями пользователей может быть как на основе Linux, так и Windows) и т. п. Вы обнаружите, что по внешнему виду программы просмотра Интернета Firefox достаточно сложно определить, в Windows или Linux она запущена, а также что документы офиса, подготовленные в пакете OpenOffice, прекрасно открываются в Microsoft Office, сохраняя все свое оформление, и наоборот (рис. 2.1).

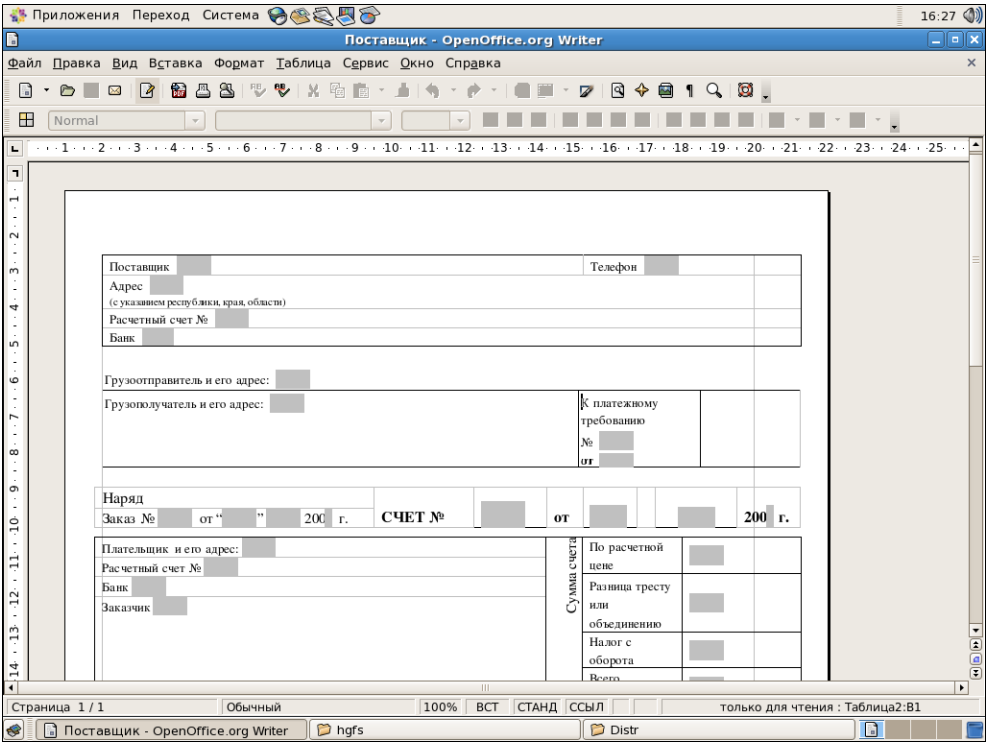


Рис. 2.1. Окно документа Microsoft Office в программе OpenOffice. На рисунке показан счет, созданный на основе шаблона Microsoft Office (доступен для загрузки в качестве образца с сайта Microsoft по адресу **http://office.microsoft.com/ru-ru/templates/TC010700121049.aspx?CategoryID=CT101172551049**) и открытый в пакете OpenOffice в среде Linux (операционная система CentOS). Нетрудно убедиться, что, несмотря на сложную структуру документа, его оформление сохранилось при открытии в OpenOffice

Естественно, что полной тождественности различных продуктов быть не может. Возникающие проблемы носят, прежде всего, психологический характер. Когда я решил сменить обозреватель Интернета (в то время это был вынужденный шаг, поскольку производительности моего компьютера не хватало для работы в Internet Explorer), то несколько дней меня не покидало чувство дискомфорта и желание вернуться в привычную среду. Сейчас я уже

ни за что не откажусь от работы в Firefox: эта программа мне кажется более удобной и предоставляет большие возможности. Существенно меньшие неудобства были связаны с началом работ в OpenOffice. Если читателю интересно, то он может ознакомиться с одним из практических результатов внедрения данной программы (см., например, **http://www.i-rs.ru/article/articleview/462/1/54/**).

Миф 2. Linux — это сложная система, собирать которую придется самостоятельно

Время, когда желавшему установить у себя Linux, приходилось самостоятельно собирать дистрибутив из различных компонентов, искать драйверы для тех или иных устройств, разбираться с настройками "железа" и т. п., давно прошло. Сегодня в распоряжении пользователей большое количество разнообразных дистрибутивов Linux на любой вкус. Их можно скачать из сети Интернет, но более рационально заказать диски в онлайновых магазинах. Дистрибутивы Linux включают в себя очень большое количество прикладных программ, различных драйверов и т. д., причем состав драйверов, включенных в дистрибутив Linux, даже шире, чем в Windows, и обеспечит подключение практически любого имеющегося у вас оборудования. В связи с этим обычный размер дистрибутива составляет 1 Гбайт или более. Если у вас не безлимитный тариф доступа в Интернет, то покупка диска за 100—150 руб. будет экономически оправданной.

Миф 3. Linux — работа в командной строке?

Одно из распространенных опасений связано с использованием в Linux командной строки. Да, для работы сервера Linux графический интерфейс излишен. И администраторы, приобретающие даже незначительный опыт работы, стараются выполнять большинство операций именно в режиме командной строки. Тем не менее, графический интерфейс в данной операционной системе также присутствует, и вы можете ее настроить с его помощью почти так же, как это делается в Windows, разве что с незначительными изменениями. Для тех, кто не желает отказаться от интерфейса рабочей станции Windows, создан даже специальный дистрибутив Linux, оформление которого сохранено в привычном для пользователей Windows варианте (рис. 2.2).

В то же время, использование командной строки имеет ряд преимуществ. Во-первых, команды очень легко автоматизировать, используя пакетные файлы. Во-вторых, графический интерфейс сам может быть причиной ошибок, кроме того, на оформление затрачиваются серьезные ресурсы системы. В-третьих, использование текстовых файлов конфигурации программ позволяет очень легко переносить настройки с одной системы на другую, а для резервирова-

ния системы в большинстве случаев достаточно сохранить несколько текстовых файлов.

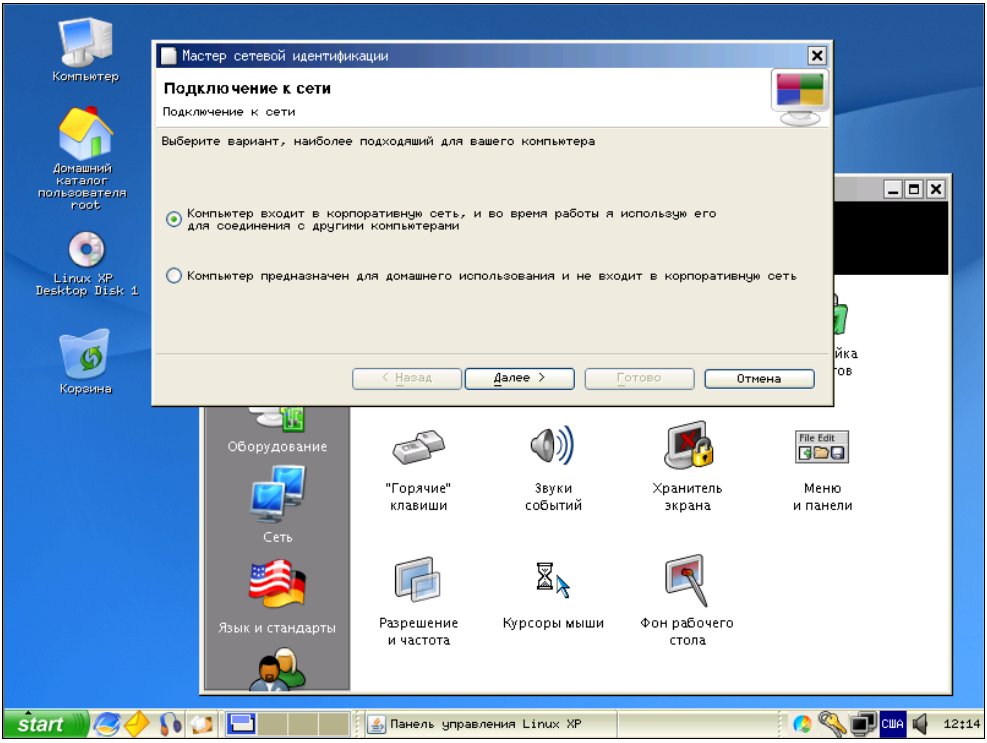


Рис. 2.2. Linux XP. Дистрибутив Linux XP специально подготовлен так, чтобы по внешнему виду максимально соответствовать операционной системе от Microsoft. Оформление окон, кнопка **Start**, содержимое рабочего стола и т. п., — все напоминает Windows XP

Примечание

Не случайно, что и базовая функциональность нового сервера от Microsoft — Windows Server 2008 — предполагает отказ от графического интерфейса и работу исключительно в режиме командной строки.

Безопасность в Linux и Windows

Очень много разговоров ведется о безопасности работы в операционных системах. При этом приводятся различные данные, которые должны показать преимущество той или иной операционной системы. Сейчас очень популярны цифры о количестве обнаруженных уязвимостей и сроках их устранения, причем в зависимости от критериев оценки лидером "становится" то одна, то другая система. Можно рассматривать количество обнаруженных уязвимо-

стей, можно оценивать степень их опасности и сроки реагирования разработчика. Любая такая оценка будет объективной, но насколько она отражает реальную жизнь?

Я бы советовал больше прислушиваться к мнению практикующих администраторов, сопровождающих системы на Linux. Для однажды установленной операционной системы и запущенного на ней программного обеспечения сам факт перезагрузки уже является нештатной ситуацией. Компьютер с Linux просто всегда работает и выполняет возложенные на него задачи.

Примечание

При освоении Linux необходимо сразу заставить себя отказаться от практики перезагрузок компьютера: в отличие от Windows, это не приносит никакого эффекта. Причины практически любых проблем нужно искать в системных настройках.

Стоимость владения

Очень популярная тема для обсуждения. Особенно мне запомнилось сравнение стоимости владения несколькими тысячами систем Linux на основе коммерческого обслуживания по сумме цен "за штуку"[1] со стоимостью корпоративного контракта для систем Windows, в котором скидка "за количество" снизила стоимость на порядок. Комментарии к подобным сравнениям излишни.

Абстрактной стоимости владения не существует. В каждом конкретном случае она должна оцениваться для условий конкретного предприятия. Не верьте тому, что администратора Linux надо обучать, а администратор Windows уже подготовлен "по определению". На первичном уровне администрирования любой специалист, имеющий некоторое знакомство с информационными системами, достаточно быстро сможет начать управлять как Linux, так и Windows. А если возникает необходимость серьезной подготовки, то без обучения не обойтись как одному, так и другому специалисту.

В Интернете представлен весьма большой объем документации по настройке Linux, и если возникла та или иная проблема, скорее всего, вы найдете необходимые рекомендации простым поиском в Сети.

Несколько моментов, о которых следует знать

Собственно сам Linux — это только *ядро*. Остальное — это приложения и службы, которые вы устанавливаете. Нечетные номера версий — экспериментальные, четные (2.8 и т. п.) представляют собой стабильные сборки.

---

[1] Для оцениваемого продукта не существовало отдельного корпоративного тарифа.

В Linux не принято хранить файлы "где придется". Есть достаточно четкая структура размещения информации (см. табл. 2.1 в *разд. "Структура папок Linux" далее в этой главе*), поэтому, например, все пользовательские данные будут находиться только в папке соответствующего личного профиля.

При работе в консоли система позволяет автоматически дополнять ввод с клавиатуры по нажатию клавиши <Tab>. Например, если требуется скопировать файл, то достаточно набрать команду (`cp`), первые символы имени файла и нажать клавишу <Tab>. Если первые символы однозначно определяют имя файла или команды, то система автоматически допишет полное название. В противном случае никаких изменений на экране не будет, а повторное нажатие клавиши <Tab> выведет на экран полный перечень имен, начинающихся с введенных символов.

Примечание

Состав доступных команд зависит от учетной записи, под которой выполнен вход в систему. Если вы не видите в списке требуемой команды, попробуйте переключиться на учетную запись root.

Как правило, пользовательская работа в Linux ведется при помощи графического интерфейса, однако в любой момент можно начать работу в нескольких *консолях*. Для этого достаточно запустить новый сеанс с помощью нажатия клавиш <Ctrl>+<Alt>+<F1>, <Ctrl>+<Alt>+<F2>[1] и т. д. (графическому интерфейсу соответствует сочетание клавиш <Alt>+<F7>).

Работу в консоли существенно облегчит использование программы MidNight Commander — **mc** (рис. 2.3). Программа практически повторяет интерфейс и возможности Norton Commander, с которого начиналась вся работа на компьютерах под управлением операционной системы DOS. При помощи **mc** можно осуществлять любые файловые операции (копировать, переименовывать, удалять, создавать папки и т. д.), редактировать файлы, просматривать архивы, установочные пакеты и т. п. MidNight Commander по умолчанию не устанавливается, но входит в большинство дистрибутивов Linux. Думаю, что вы не пожалеете, если будете использовать возможности данной программы.

В Linux расширения имен файлов не используются для ассоциации выполняемых операций. Исполняемым может быть *любой* файл, необходимо только предоставить ему соответствующее разрешение. Кстати, это повышает безопасность системы.

Команды в Linux чувствительны к регистру. Например, ключи `R` и `r` могут обозначать различные операции.

---

[1] Клавиша <Ctrl> требуется только при запуске команды в графическом режиме. После переключения в режим консоли переходить в другой сеанс можно нажатием клавиш <Alt>+<F*n*>, возврат в графический режим также будет выполняться нажатием сочетания клавиш <Alt>+<F7>.

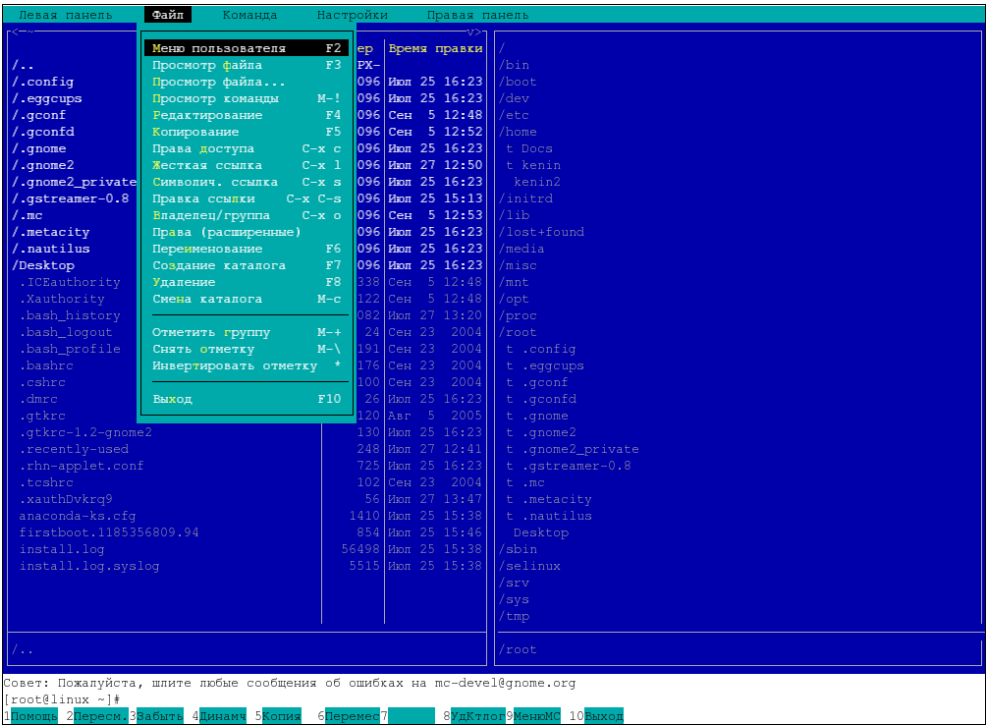


Рис. 2.3. Программа MidNight Commander

В Linux не принято подключать жесткие диски под именами логических дисков (C, D, E и т. д.). Обычно диски *монтируются*: добавляются в качестве новой папки в определенное место файловой структуры.

Так же, как и в Windows, в Linux создаются пользователи, которых можно объединять в группы. Учетные записи могут быть как локальными, так и храниться централизованно (и использоваться на нескольких компьютерах). В Linux есть один "суперпользователь", которому разрешено все. Его имя — root. Текущая работа в системе производится с правами обычного пользователя, в случае необходимости выполнения операции, требующей административных прав, система запрашивает пароль учетной записи root (и обычно сохраняет его некоторое время в памяти для удобства последующих административных операций).

Права доступа обычно отображаются в виде последовательности символов `-rwxr-x--x`. Первый символ указывает тип файла (`-` — обычный файл, `d` — папка, возможны также псевдофайлы), следующие три символа определяют права владельца файла, следующие три — права группы, к которой принадлежит владелец, и последние три обозначают права для всех остальных поль-

зователей. В каждой тройке первый символ свидетельствует о наличии права чтения (`r`) или его отсутствии (дефис), второй — право записи (`w`) и третий — исполнения (`x`). Часто права записывают также в виде трех цифр, например, 753. Если представить каждую цифру в двоичном виде, то получится 111101011, что соответствует `rwxr-x-wx`.

Структура папок Linux

Linux предполагает четкую структуру расположения папок и файлов. В табл. 2.1 приведены наиболее "значимые" папки системы.

Таблица 2.1. *Типовая структура папок в Linux*

Папка	Назначение
/sbin	Папка с программами редактирования и проверки структуры диска, а также изменения состояния системы
/dev	Содержит записи, соответствующие устройствам, подключенным к системе
/usr/bin	Папка программ работы с учетными записями. В этой же папке хранятся программы демонов
/etc	В этой папке находится основная часть файлов локальной конфигурации системы
/etc/init.d	Скрипты запуска системы. Часто указывают, в свою очередь, на папки /etc/rc?.d (? — цифра от 0 до 6, соответствует уровню запуска)
/home/*username*	Домашняя папка пользователя *username*
/usr	Папка с общими программами; доступна только для чтения
/usr/local	В эту папку должны устанавливаться прикладные программы
/usr/share/doc	Папка, в которую обычно копируется справочная документация по установленным программам
/lib	Папка с программными библиотеками
/mnt	Обычно используется для подключения устройств (диски, CD-ROM и т. д.)
/opt	Папка, в которой обычно размещаются устанавливаемые программы, имеющие большой объем
/proc	Папка для хранения специальных файлов, формируемых ядром системы
/var	Папка для изменяемых данных. Содержит, в том числе, папки журналов системы

Текстовый редактор vi

В Linux существует очень мощный текстовый редактор, который запускается командой `vi`. Поскольку большинство настроек сохранено в виде текстовых файлов, то умение воспользоваться редактором vi может быть очень полезным в случае проблем с графическим интерфейсом.

Для запуска редактора достаточно набрать в окне терминала `vi` и указать через пробел имя файла, открываемого для редактирования.

Текстовый редактор vi имеет два режима работы: командный и редактирования. При открытии файла вы попадаете в командный режим, в котором можно выполнять такие операции, как поиск, замена, сохранение файла, вызов внешней команды и т. п. Чтобы начать ввод текста, следует перейти в режим редактирования. Переход из режима редактирования в командный режим осуществляется по нажатию клавиши <Esc>.

В редакторе доступно много команд, мы приведем лишь самые основные, которые позволят вам выполнить простейшие операции с текстом.

Таблица 2.2. *Команды текстового редактора vi*

Команда	Действие
`a`	*Добавить*. Переход в режим ввода текста *справа* от курсора
`i`	*Вставить*. Переход в режим ввода текста *слева* от курсора
Клавиши перемещения курсора	Перемещение курсора по документу. Для перемещения курсора используются также четыре расположенные в ряд клавиши h (влево), l (вправо), j (вниз) и k (вверх). Можно использовать их вместе с цифрами: например, ввод команды 9k переместит курсор на 9 строк вверх
<Ctrl>+<F>/<Ctrl>+<B>	Перемещение на одну страницу вперед/назад
`G`	Переход на последнюю строку документа
`nG`	Переход на строку с номером *n*
`x`	Удаление символа над курсором
`X`	Удаление слова, в котором находится курсор
`dw`	Удаление символов, начиная с текущего, до конца слова; ввод команды 4dw приведет к удалению *четырех* слов
`d$`	Удаление символов, начиная с текущего, до конца строки
`/слово`	Поиск символов *слово* вперед
`?слово`	Поиск символов *слово* назад
`:g/поиск/s/замена/g`	Замена сочетания символов, указанного в строке *поиск*, на сочетание, указанное в строке *замена*, во всем тексте документа
`u`	Отмена последней операции (можно отменить несколько шагов)

Таблица 2.2 *(окончание)*

Команда	Действие
<Ctrl>+<R>	Восстановление последней отмененной операции
`:w`	Сохранение файла
`:wq`	Сохранение файла и выход из режима редактирования
`ZZ`	То же, что и :wq — сохранение файла и выход
`:q`	Выход из редактора (операция выполнится, только если все внесенные изменения сохранены)
`:q!`	Выход без сохранения изменений
`:! command`	Выполнение внешней команды (*command*)
<Ctrl>+<G>	Вывод информации об имени редактируемого файла и текущей позиции в нем

Проблемы с графической средой

При возникновении проблем с графической средой X11 в случае невозможности работы с окнами программ может помочь редактирование файлов конфигурации графической подсистемы.

Файл конфигурации обычно находится по следующему пути: /etc/X11 /xorg.conf. В случае использования среды X86 файл имеет аналогичную структуру, но называется XF86Config. Выключить X11 можно нажатием клавиш <Ctrl>+<Alt>+<Backspace>.

Часто система имеет настройки, вновь запускающие X11 после его закрытия. В этом случае перейдите в режим терминала, нажав <Ctrl>+<Alt>+<F2>, войдите в систему под учетной записью суперпользователя (root) и загрузите Linux в неграфическом режиме, выполнив команду `init 3`.

Новую конфигурацию можно создать автоматически, выполнив следующую команду:

```
Xorg –configure
```

Для проверки ее работоспособности выполните команду (для новой конфигурации создается файл с именем xorg.conf.new):

```
X –xf86config /root/xorg.conf.new
```

Если запуск сервера X11 прошел корректно и вы видите серый экран[1] с курсором X, то конфигурацию можно скопировать в качестве рабочей. Для этого закройте сервер X11 (**Ctrl+Alt+Backspace**) и скопируйте файл

```
cp /root/xorg.conf.new /etc/X11/xorg.conf
```

[1] Полный запуск графической подсистемы с менеджером окон осуществляется командой `startx`.

При необходимости вы можете откорректировать конфигурацию вручную. Структура файла достаточно понятна и снабжена необходимыми комментариями.

Выполнение команд с правами другого пользователя

Для выполнения программ с правами другого пользователя служит команда `su`. При выполнении команды[1]

```
su -
```

система запросит пароль. Введите пароль пользователя root, и вы получите его права (обратите внимание, что при этом изменяется символ приветствия).

Для возвращения введите команду `exit` или нажмите клавиши <Ctrl>+<D>.

Помимо переключения на суперпользователя эта же команда, введенная с указанием какой-либо другой учетной записи в качестве параметра, позволяет переключиться на нее, если далее по запросу системы ввести ее имя и пароль:

```
su — user1
```

Примечание

При переходе от суперпользователя к другому пользователю пароль вводить не требуется.

Программное обеспечение рабочего места

Операционная система — это только "основа", позволяющая работать в прикладных программах, ради которых и включают компьютер. Если вы планируете переход с Windows на Linux, то одной из первых задач станет определение используемых прикладных программ и поиск соответствующих решений для новой платформы.

Сегодняшний Linux включает в себя большое количество бесплатного прикладного программного обеспечения. Это текстовые и графические редакторы, аудио- и видеопроигрыватели, утилиты записи CD/DVD, почтовые клиенты и обозреватели Интернета, серверы баз данных и т. п. На портале **http://SourceForge.net** вы можете найти тысячи проектов, среди которых есть и программы управления предприятием (ERP-системы), CRM-системы, сис-

[1] Можно не использовать дефис в качестве параметра: в этом случае вы также получите права администратора, но параметры окружения (например, текущая папка) останутся прежними. При вводе дефиса команда переведет вас в новое окружение.

темы электронного документооборота и т. п. С большой вероятностью необходимое типовое программное обеспечение будет присутствовать в бесплатных версиях.

Среди коммерческого программного обеспечения можно отметить тенденцию постоянного увеличения числа вендоров, разрабатывающих свои продукты как для систем на основе Windows, так и для использования в Linux. Если примерами крупных западных разработчиков уже вряд ли кого удивишь (например, система документооборота Documentum, причем ее версия для Linux характеризуется большей надежностью и повышенной производительностью), то пример российской фирмы 1С, выпустившей версию своей программы для Linux, говорит о многом.

Если вам не удалось подобрать замену для какого-либо уникального продукта, то можно попытаться воспользоваться одним из следующих способов. Первый заключается в запуске программ Windows под Linux при помощи специального разработанного продукта WINE (**www.winehq.org**): судя по отзывам, таким образом успешно запускались даже программы 1С.

Примечание

WINE особенно подходит для тех программ, которые могут быть запущены в режиме совместимости с Windows 98.

Второе решение состоит в использовании виртуальной машины. Вы устанавливаете виртуальную машину, в которой запускаете операционную систему Windows и проблемное приложение. Данный способ гарантированно позволит продолжать использовать прикладную программу, но потребует приобретения лицензионной копии Windows.

Установка Linux

Установка Linux и ее первоначальная настройка не составляют никакой сложности. Операции выполняются в графической среде при помощи мастера установки (рис. 2.4), который в процессе инсталляции запрашивает основные параметры (часовой пояс, раскладку клавиатуры, путь установки и т. п.). Если какие-то параметры вам не понятны, можно просто согласиться с вариантом, предложенным мастером по умолчанию.

Многовариантная загрузка

На одном компьютере можно использовать несколько операционных систем. Лучше всего устанавливать их на различные логические диски. Но часто желание попробовать новую операционную систему возникает, когда компьютер уже используется и свободных дисков нет.

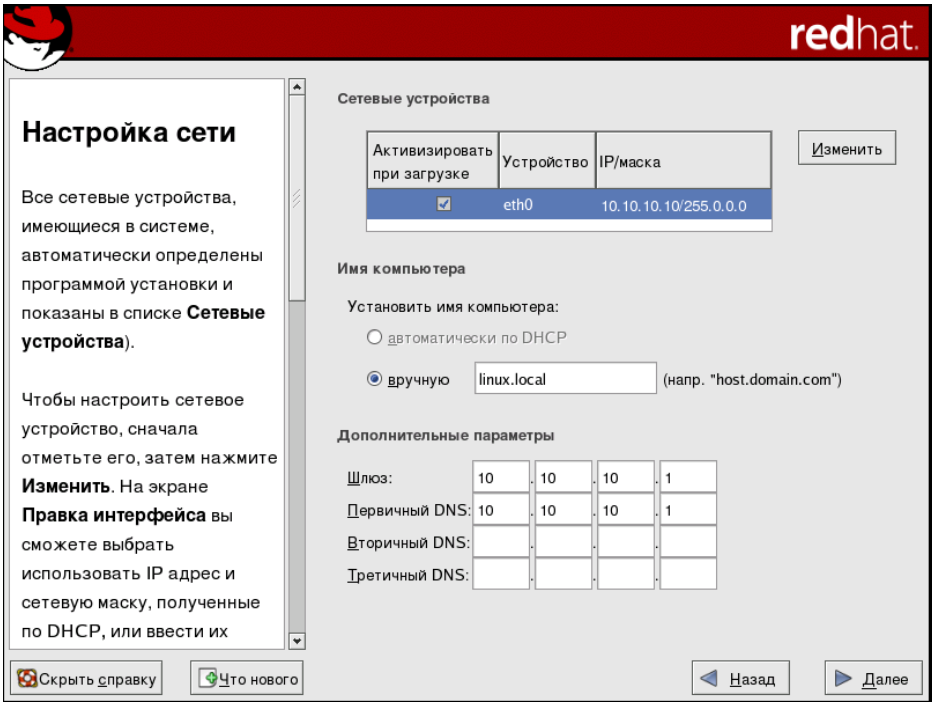


Рис. 2.4 Установка Linux происходит в графическом режиме

Установщики Linux позволяют изменить конфигурацию разделов существующей системы *без потери данных*. Мастер установки предложит создать на существующем диске новый раздел, при этом вы можете указать желаемый объем нового раздела (по умолчанию обычно предлагается использовать половину имеющегося свободного пространства). Операция займет некоторое время (зависит от объема жесткого диска), после чего установка Linux продолжится.

Естественно, что подобный вариант действий возможен только тогда, когда первой установленной системой была Windows. Современные установщики Linux "знают" практически все используемые операционные системы других вендоров.

Примечание

После установки Linux на раздел Windows и последующей загрузки Windows система предупредит о возможных неисправностях диска и предложит выполнить его проверку. При этом возможна и перезагрузка Windows (после установки новых устройств). Это стандартная реакция системы на изменение раздела диска. Данные не потеряны, надо просто один раз согласиться на выполнение предложенных шагов.

Выбор варианта загрузки по умолчанию

После установки Linux на компьютер с операционной системой Windows при включении необходимо выбрать вариант загрузки. Возможно, вы захотите изменить предлагаемый системой выбор по умолчанию.

Обычно в Linux для загрузки применяется пакет GRUB. В этом случае для изменения последовательности загрузки необходимо отредактировать файл /boot/grub/menu.lst. Откройте его в любом текстовом редакторе (для операции редактирования необходимы права пользователя root) и укажите для параметра default номер загрузки, которая будет выполняться по умолчанию (по умолчанию для каждой из загрузок установлено значение 0). Имейте в виду, что список вариантов нумеруется с нуля, поэтому для выбора третьего значения необходимо установить параметр default равным двум.

Тестирование Linux на виртуальной машине

Если вы хотите предварительно протестировать и ознакомиться с системой Linux, можно воспользоваться ее установкой на виртуальную машину. Хотя Linux можно достаточно легко настроить для работы, например, в Virtual PC, но для самой первой встречи с новой операционной системой данная операция будет затруднительна: в процессе установки необходимо вручную указать тип монитора. Обычно на этот параметр не обращают внимания, однако его отсутствие не позволит сразу же использовать графическую оболочку Linux в виртуальной среде. Исправлять конфигурацию придется в режиме командной строки Linux, что далеко не всегда под силу пользователю, в первый раз запускающему данную операционную систему.

Учитывая вышесказанное, лучше применить виртуальную машину от Vmware, поскольку виртуальная машина от Microsoft не столь дружественна к "чужим" операционным системам.

Работа с Linux-системами на виртуальной машине VMware имеет одну особенность: для повышения производительности, улучшения графического отображения, отсутствия блокировки курсора мыши в виртуальной машине (необходимости "освобождать" курсор нажатием правых клавиш <Alt>+ +<Ctrl>), копирования данных между виртуальными машинами следует установить VWware Tools. Если в виртуальной машине для Windows соответствующая установка происходит автоматически, то для Linux следует ее сделать вручную. Чтобы выполнить данную установку, подключите виртуальный образ CD-диска, который содержит установочный пакет утилит, соответствующий операционной системе виртуальной машины. Образы диска с утилитами находятся в папке установки VMware — обычно Program Files\VMware\VMware Workstation — и называются freebsd.iso, linux.iso, solaris.iso. Начните его установку в соответствии с правилами операционной

системы (например, для систем с инсталляционными пакетами RPM достаточно просто выбрать пакет, чтобы его установка была начата).

После установки пакета нужно запустить скрипт конфигурации утилит, который добавит необходимые модули в ядро системы. Имя исполняемого файла для образа linux.iso — vmware-config-tools.pl. Выполните эту операцию с правами суперпользователя.

Далее желательно запустить средство управления утилитами VMware (/usr/bin/vmware-toolbox) и включить синхронизацию времени виртуальной машины (по умолчанию она не включена, рис. 2.5).

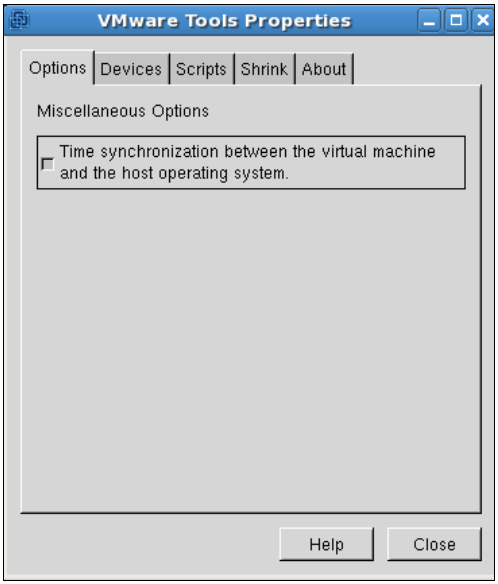


Рис. 2.5. Настройка опций VMware Tools в операционной системе Linux

Есть еще одна особенность в работе на виртуальной машине Linux от VMware: если вы подключаете к Linux совместно используемую папку на хосте, то по умолчанию она будет подмонтирована в каталог /mnt/hgfs.

Работа с ресурсами домена: Samba

Для работы в составе домена Windows (использование единой базы учетных записей пользователей, подключение/предоставление общих ресурсов и т. п.) предусмотрен пакет Samba. Этот пакет входит во все дистрибутивы Linux, и обычно нет необходимости загружать инсталляционные файлы с сайта **www.samba.org**.

Установка

По умолчанию Samba, как правило, однако может быть не запущен. Как правило, в Linux есть средства настройки параметров основных сетевых служб (рис. 2.6).

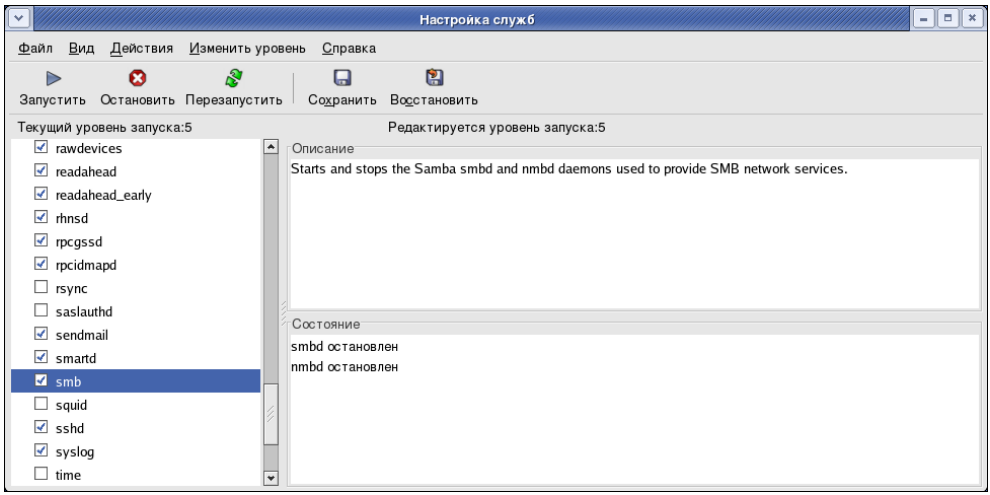


Рис. 2.6. Настройка автоматического запуска Samba графическими средствами

Проверить, работает ли демон Samba, можно, перечислив все активные процессы и отфильтровав вывод команды по названию службы:

```
ps -A | grep smb
```

Если Samba работает, то вы должны увидеть приблизительно такую информацию:

```
3200 ?        00:00:00 smbd
 4207 ?        00:00:00 smbd
```

Для перезапуска службы (необходимая операция в случае изменения конфигурации демона) можно использовать команду

```
service smb restart
```

Кроме сервиса smbd, если вам понадобятся пользовательские учетные записи домена Windows, необходимо установить в режим автоматической загрузки и демон Winbind (имя winbindd). Команда его запуска и перезагрузки выполняется аналогично.

Подключение к домену (Kerberos)

Примечание

Red Hat Linux имеет настройки Security Level Configuration. Если выбран уровень безопасности системы High или Medium, то аутентификация в домене Windows будет невозможна. Поэтому включите вариант No Firewall (через меню **Main | System Settings** или в режиме терминала командой `redhat-config-securitylevel`).

Настроить работу в домене Windows можно в одном из двух режимов: либо на основе NTLM-аутентификации (традиционный вариант, совместим с доменами Windows NT), либо на основе Kerberos (поддерживается в Windows 200*x*). Далее мы рассмотрим варианты настроек при использовании протокола Kerberos; другие варианты вы легко сможете найти в Интернете.

Настройка Kerberos

Kerberos обычно уже установлен в системе. Вам необходимо только отредактировать файл его конфигурации, указав адреса серверов аутентификации домена.

Примечание

Протокол Kerberos будет работать только в том случае, если рассогласование времени между компьютером пользователя и контроллером домена составляет меньше 5 минут. Чтобы обеспечить его корректную работу, предварительно синхронизуйте время на компьютерах и проверьте идентичность установленных часовых поясов.

Настройки Kerberos можно выполнить с помощью имеющихся в системе графических утилит (рис. 2.7), но проще вручную отредактировать файл конфигурации, расположенный по следующему пути: /etc/krb5.conf. В этом файле обычно достаточно отредактировать только параметры доменной области (realm) и центра выдачи ключей (KDC)[1]:

```
[realms]
LOCAL.DOMAIN = {
kdc = tcp/dc1.local.domain:88 tcp/dc2.local.domain:88
admin_server = dc1.local.domain
default_domain = local.domain
}
```

[1] В данном примере DNS-имя домена — local.domain, а контроллеры домена имеют имена dc1 и dc2.

```
[domain_realm]
.local.domain = LOCAL.DOMAIN
local.domain = LOCAL.DOMAIN

[kdc]
enable-kerberos4 = false
```

Примечание

Записи в этом файле чувствительны к регистру. Рекомендуется вводить имена *только* в верхнем регистре, так, как это сделано в данном примере.

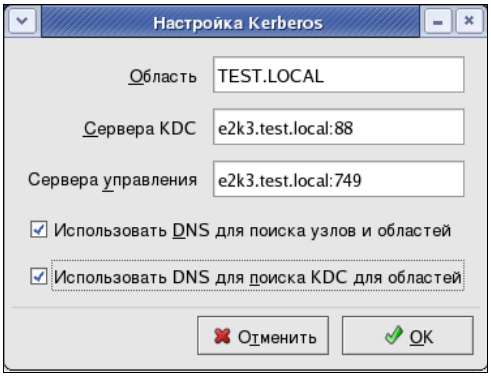


Рис. 2.7. Настройка параметров Kerberos в графическом режиме в Red Hat

После того как вы отредактируете конфигурацию, необходимо получить билет Kerberos. Чтобы получить для пользователя с правами администратора домена Windows, выполните следующую команду:

```
kinit administrator@LOCAL.DOMAIN
```

Обратите внимание, что имя домена должно быть набрано прописными буквами.

Команда должна отработать без ошибок. Самая распространенная ошибка возникает в случае, если время системы Linux отличается от времени контроллера домена. В этом случае синхронизуйте время и повторите команду.

Проверить полученный билет можно, выполнив команду

```
klist
```

Она должна показать параметры полученного билета (имя учетной записи, срок действия билета).

Настройки Samba

Настройки Samba содержатся в файле конфигурации, который расположен по следующему пути: /usr/samba/lib/smb.conf.

Файл состоит из нескольких разделов: `[globals]` — глобальные настройки, `[homes]` — домашние папки пользователей, `[printers]` — настройки печати и пользовательских разделов, в которых определяются сетевые папки. Имена разделов заключаются в квадратные скобки, параметры определяются в виде `key = value`. Файл конфигурации снабжен комментариями, так что для вас не составит особого труда разобраться с правилами его редактирования. Вы можете просто снять комментарии с тех строк, которые описывают наиболее подходящую конфигурацию сервера, и настроить по образцу совместный доступ к ресурсам.

Примечание

Отсутствие ошибок в файле можно проверить с помощью команды `testparm`. Если она сообщит об ошибке, следует перепроверить внесенные настройки.

Настройка nsswitch.conf

В файле /etc/nsswitch.conf определяется, какие источники будут использованы для получения данных о пользователях. Иногда настройки по умолчанию ограничиваются только локальными параметрами (в строках упомянуто только `files`). Поэтому проверьте, чтобы содержимое файла /etc/nsswitch.conf включало параметры как `files`, так и `winbind`. Например, так:

```
group: files winbind
hosts: files dns nis winbind
networks: files winbind
passwd: files winbind
shadow: files winbind
shells: files winbind
```

Подключение к домену

Для включения компьютера с Linux в домен Windows по протоколу Kerberos необходимо выполнить следующую команду (подключение происходит к домену, указанному в параметрах по умолчанию):

```
net ads join -U administrator%password
```

В этой строке `administrator` и `password` соответственно имя пользователя, имеющего право подключения компьютеров к домену (лучше всего, если это будет администратор домена), и его пароль. В ответ вы должны получить сообщение об удачном выполнении операции.

Проверка подключения

Проверить возможности работы в домене можно, попытавшись отобразить перечень учетных записей. Сначала следует протестировать наличие подключения командой

```
wbinfo -t
```

Эта команда должна выдать сообщение, аналогичное приведенному ниже:

```
[root@linux ~]# wbinfo -t
checking the trust secret via RPC calls succeeded
```

Командой `wbinfo -u` можно отобразить список пользователей, а применив ее с ключом `-g` — список групп.

Проверьте, что служба winbind успешно получает пароли с контроллера домена. Для этого выполните команду

```
getent passwd
```

В списке паролей вы должны увидеть записи, относящиеся к домену (имена пользователей будут показаны в начале строки в виде домен\пользователь).

Предоставление ресурсов в общий доступ

Операцию можно осуществить как с использованием графического интерфейса (рис. 2.8), так и путем правки конфигурации программы. Приведенный ниже краткий пример иллюстрирует основные параметры предоставления ресурса в общий доступ:

```
[Documents]
   comment = Архив документов
   path = /usr/local/docs
   valid users = @"domain\domain users" domain\user1
   admin users = @ domain\group2
   writable=yes
   browseable=yes
```

Необходимые дополнительные параметры (настройку протоколирования доступа, корзины, варианты предоставления ресурса с произвольной маской доступа и т. п.) легко уточнить по справочной документации.

Обратите внимание, что в секции `[global]` файла конфигурации можно установить, для каких диапазонов адресов будут предоставляться в совместное использование ресурсы, максимальное число одновременно открытых файлов и т. п.:

```
[global]
   workgroup = TEST
   realm = DOMAIN.LOCAL
```

```
preferred master = no
server string = Linux Machine
security = ADS
encrypt passwords = yes
log level = 3
log file = /var/log/samba/%m
max log size = 50
max open files = 100000
printcap name = cups
printing = cups
winbind enum users = Yes
winbind enum groups = Yes
winbind use default domain = Yes
winbind nested groups = Yes
winbind separator = +
idmap uid = 600-20000
idmap gid = 600-20000
hosts allow = 192.168.0.
```

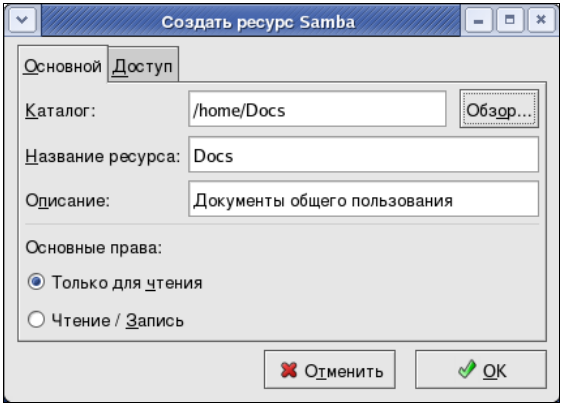


Рис. 2.8. Графический интерфейс управления службой Samba

При предоставлении ресурсов в доступ пользователям домена следует учитывать, что пользователь, подключающийся к ресурсу, будет иметь на компьютере личную папку. Можно настроить ее автоматическое создание при первом подключении, если добавить в /etc/pam.d/sshd следующую строку:

```
session required /lib/security/pam_mkhomedir.so
```

Другой вариант заключается в создании пользовательских папок вручную. При этом следует учитывать, что папки должны создаваться по следующему пути, учитывающему название домена:

```
/home/DOMAIN/username
```

Далее необходимо предоставить права доступа к данной папке соответствующим пользователям, запустив выполнение команды `chown -R`.

Учетная запись *Гость*

Учетной записи **Гость** (Guest) в Windows соответствует учетная запись nobody в Linux. По умолчанию анонимный доступ к ресурсам запрещен. Если вы хотите его разрешить, то удостоверьтесь в существовании в системе учетной записи nobody и откорректируйте конфигурацию Samba по следующему образцу:

```
[global]
  security = user
  map to guest = Bad Password

 [share_definition]
  guest ok = yes
```

Другой способ состоит в использовании параметра `security = share`. В этом случае доступ к ресурсу будет осуществляться только с параметрами гостевой учетной записи.

Подключение к общим ресурсам

Использование командной строки для подключения к ресурсам домена практически повторяет команды Windows. Для подключения ресурса нужно выполнить команду

```
net use m: \\servername\service
```

или, для подключения сетевого принтера

```
net use lpt1: \\servername\spoolservice
```

Если нужно подключить ресурсы *nix компьютеров, то используется команда `smbclient`:

```
smbclient  //hostname/service
```

Эту же команду следует выполнить для того, чтобы отобразить ресурсы, предоставленные в совместное использование с компьютера:

```
smbclient -L hostname
```

Сервер Linux в качестве контроллера домена

Сервер Linux может выступать в качестве контроллера домена Windows. Соответствующие настройки вносятся в конфигурацию сервера Samba; их описание легко найти в Интернете.

В качестве контроллера домена сервер Linux хранит учетные записи пользователей. При этом вы можете применять сценарии, исполняемые при входе пользователей в домен, однако вам недоступны групповые политики, активно используемые при управлении доменом Windows 200*x*. Групповые политики предполагается реализовать в версии Samba 4, которая в настоящее время проходит тестирование.

Возможный выход в такой ситуации заключается в применении дополнительных пакетов для реализации необходимых функций. Например, для автоматизации установки и удаления программ Windows можно применить WPKG (**http://wpkg.org**).

Межсетевой экран iptables

Операционные системы Linux включают в себя межсетевой экран. Наиболее широко используется межсетевой экран iptables. Программа позволяет осуществить настройки фильтрации пакетов существенно более точно, чем межсетевые экраны в Windows. Это объясняется тем, что в Linux имеется больше возможностей управления трафиком на низком уровне, чем доступно пользователям Windows.

Настройки запуска

Межсетевой экран iptables входит в состав практически всех современных выпусков Linux. Обычно при установке операционной системы задается вопрос, хотите ли вы задействовать сетевой экран по умолчанию или нет. В зависимости от вашего выбора, программа будет либо запущена, либо выключена[1]. При этом набор правил фильтрации пакетов по умолчанию запретит доступ к ресурсам компьютера извне и ограничит некоторые функции работы в локальной сети.

Запуск межсетевого экрана можно осуществить командой

```
/sbin/service iptables start
```

Для остановки демона в качестве параметра следует указать `stop`, для перезапуска (необходимо после редактирования конфигурации) — `restart`.

[1] Для того чтобы узнать, работает программа межсетевого экрана или нет, достаточно вывести на экран список процессов командой `ps -A` и отфильтровать его по названию службы командой `grep`.

Для автоматического запуска программы межсетевого экрана при каждом старте системы достаточно выполнить команду

```
/sbin/chkconfig --level 345 iptables on
```[1]

Примечание

В зависимости от используемого дистрибутива вы можете выполнить настройку служб специальными утилитами. Например, на рис. 2.9 представлен вариант настройки запуска службы утилитой `ntsysv` в Red Hat.

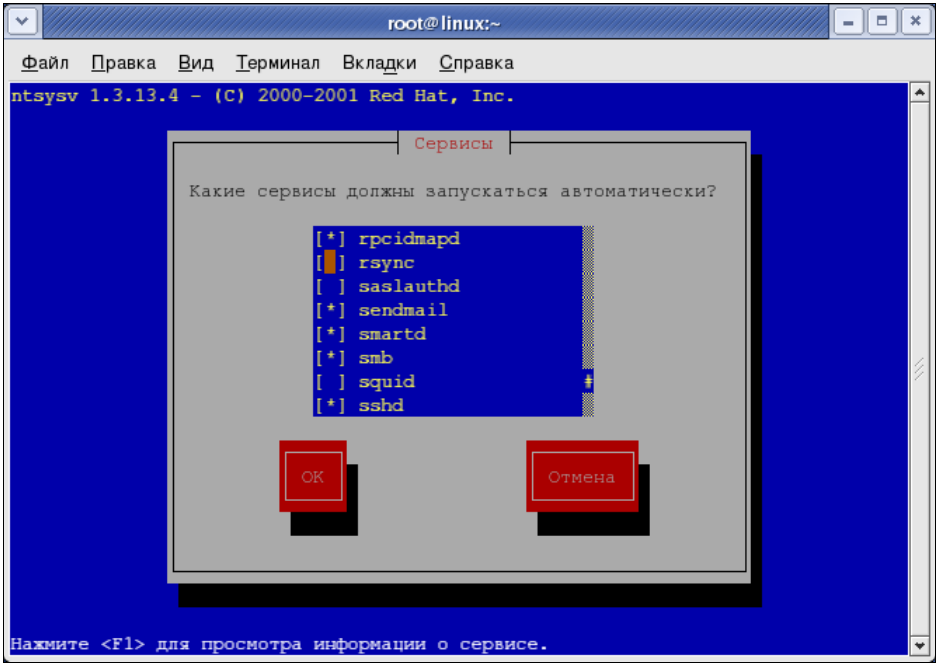


Рис. 2.9. Утилита для настройки параметров служб, работающая в текстовом режиме

Программы графического управления iptables

Для точной настройки межсетевого экрана требуется обращение к командной строке и добавление соответствующих правил с полным набором параметров — условий, которым должен удовлетворять пакет, чтобы к нему было

[1] В Linux существует несколько вариантов (уровней) загрузки. Они определяют, будет система стартовать в однопользовательском режиме, надо ли загружать графическую среду и т. п. Нормальному режиму работы соответствуют уровни 3 и 5; отличие между ними состоит только в том, что на уровне 3 не загружается графическая подсистема.

применено данное правило. Для пользователя, только начинающего работать в Linux, подобная настройка может вызвать существенные затруднения.

В большинстве случаев, чтобы обеспечить необходимый уровень безопасной работы в сети, достаточно применить стандартные ограничения. В таких

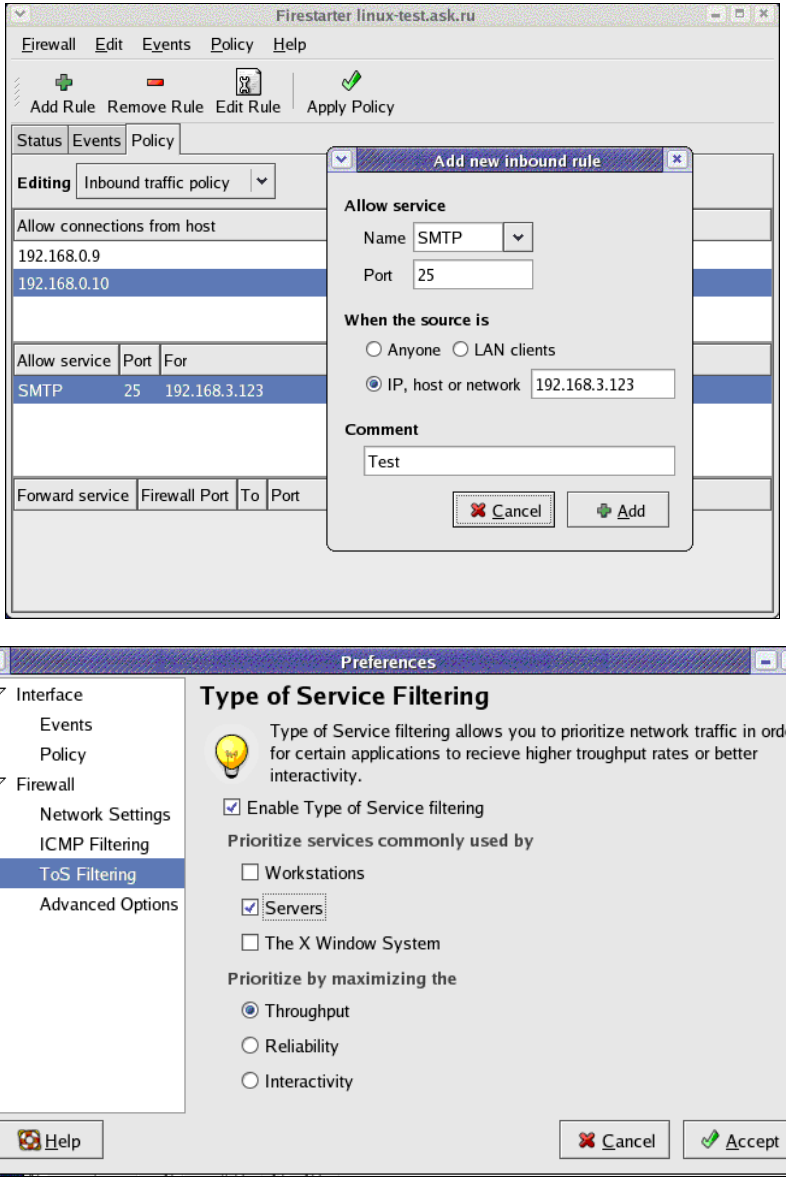


Рис. 2.10. Графическая настройка параметров межсетевого экрана

ситуациях можно рекомендовать использовать для настройки межсетевого экрана графические утилиты. Их легко найти среди бесплатного программного обеспечения на сайте Surceforge.net. В качестве примера на рис. 2.10 показан интерфейс одной из таких программ.

На рисунке представлены экраны программы FireStarter. С ее помощью легко настроить часто используемые на практике параметры межсетевого экрана в графическом режиме. На рисунке слева показано окно настройки правила публикации службы, справа — включение возможностей приоретизации трафика. Программа позволяет наблюдать события межсетевого экрана, создавать правила входящего и исходящего трафика, настраивать режим совместного использования подключения и т. п.

Принципы работы iptables

Любой пакет несколько раз анализируется на соответствие некоторым условиям каждым сетевым интерфейсом компьютера. При удовлетворении условиям к пакету применяется соответствующее правило и дальнейший анализ на данном этапе не производится. Если ни одно из правил не содержит условий, соответствующих пакету, к нему применяются правила по умолчанию. Подобные наборы правил носят названия *таблиц*.

Существует три таблицы правил: filter — основная таблица, nat — используется для пакетов, создающих новое подключение (можно менять адреса источника и назначения пакета), и mangle, применяемая для специального типа пакетов.

Один и тот же пакет может анализироваться межсетевым экраном несколько раз на различных этапах его обработки. Так, в таблице filter можно создавать правила, применяемые при *приеме* пакетов данным интерфейсом — INPUT, при *передаче* пакета тем же интерфейсом, которым он принят, — OUTPUT и при *пересылке* пакетов на другой сетевой интерфейс — FORWARD. Для таблицы nat предусмотрены варианты PREROUTING — при приеме пакета данным интерфейсом, OUTPUT — применяется к пакетам *перед* маршрутизацией через данный интерфейс и POSTROUTING — правило применяется перед передачей пакета с данного интерфейса. Таблица mangle имеет только два варианта: PREROUTING и OUTPUT. Их смысл аналогичен одноименным цепочкам таблицы nat.

К пакетам, удовлетворяющим условиям фильтров, можно применить несколько действий: они могут быть пропущены (ACCEPT), удалены с сообщением источнику об ошибке передачи данных (REJECT) или уничтожены без оповещения (DROP). Существует также возможность настройки и применения пользовательского варианта обработки (QUEUE).

Создание правил межсетевого экрана

Существует несколько вариантов настройки межсетевого экрана. Во-первых, можно отредактировать файл конфигурации iptables, расположенный по адресу /etc/sysconfig/iptables, и перезапустить соответствующего демона /sbin/service iptables restart. Второй способ заключается в последовательном добавлении или удалении правил. Он более сложен для недостаточно подготовленного администратора, зато гарантирует отсутствие ошибок во вносимых изменениях, поскольку при таком добавлении правил проверяется корректность команд.

После добавления правил необходимо сохранить конфигурацию командой /sbin/service iptables save. В противном случае внесенные вами изменения будут действительны только в течение текущего сеанса работы и потеряются при перезагрузке системы.

В общем виде команда редактирования правил межсетевого экрана выглядит следующим образом:

```
iptables [-t table-name ] command chain-name parameter-1 option-1
parameter-n option-n
```

Параметр `table-name` позволяет выбрать используемую таблицу. `Command` определяет выполняемое действие: добавление или исключение правила. `Chain-name` — это название соответствующего правила. Далее следует набор пар `parameter-n option-n`, которые, собственно говоря, и определяют конкретные действия программы.

Команды

Часть команд, часто применяемых при создании правил межсетевого экрана, представлена в табл. 2.3. Полный перечень данных команд можно просмотреть, вызвав на экран справку по команде `iptables`.

Таблица 2.3. *Команды* `iptables`

Команда	Означает
`-L`	Выводит список действующих правил (для отображения подробного списка используйте параметр `-v`)
`-F`	Удаляет цепочку, имя которой приведено далее в качестве параметра. Если имя не указано, то *удаляет все правила* межсетевого экрана
`-A`	Добавляет новое правило в *конец* списка
`-D`	Удаляет правило с указанным номером
`-I`	Добавляет правило и размещает его в списке в соответствии с указанным номером. Если номер правила не указан, то оно становится *первым*

Параметры

Список параметров, часто используемых при создании правил межсетевого экрана, приведен в табл. 2.4. Полный перечень возможных параметров можно просмотреть в справке по команде `iptables`.

Таблица 2.4. *Параметры команды* `iptables`

Параметр	Означает
`-d`	Определяет назначение пакета. Можно указывать имя хоста, IP-адрес или подсеть (либо как 192.168.0.0/255.255.255.0, либо как 192.168.0.0/24)
`-s`	Определяет источник пакета. Синтаксис аналогичен параметру `-d`
`-f`	Правило будет применено только к фрагментированным пакетам. Символ ! после данного параметра определяет область применения для нефрагментированных пакетов
`-i`	Определяет интерфейс (eth0, ppp0 и т. п.). Если параметр опущен, то правило будет применяться ко всем интерфейсам. Знак + используется в качестве маски: eth+ обозначает *все* интерфейсы Ethernet
`-o`	Определяет выходной интерфейс в правилах с OUTPUT и FORWARD
`-j`	Определяет правило (ACCEPT, DROP, QUEUE, и т. д.). Применение без указания опции используется в правилах с подсчетом пакетов (каждый пакет увеличивает значение счетчика на единицу)
`-p`	Определяет протокол IP: icmp, tcp, udp или all. Может использоваться протокол, определенный в /etc/protocols

Опции

Список опций, наиболее часто используемых при создании межсетевого экрана, приведен в табл. 2.5. Полный перечень опций отображается в справке по команде `iptables`.

Таблица 2.5. *Опции команды* `iptables`

Опция	Означает
`--dport`	Определяет порт назначения. Диапазон допустимых значений — 0:65535. Для указания интервала портов используется символ : (например, `--dport 3000:3200`), для исключения портов или их диапазонов — символ !
`--sport`	Определяет порт источника. Синтаксис аналогичен `--dport`
`--syn`	Определяет тип пакетов SYN. Можно использовать символ ! для указания всех остальных пакетов
`--tcp-flags`	Определяет пакеты со специальными флагами: ACK, FIN, PSH, RST, SYN и URG. Допускается использование обозначений ALL и NONE

Таблица 2.5 *(окончание)*

Опция	Означает
`--tcp-option`	Определяет дополнительные опции пакетов протокола IP
`--icmp-type`	Определяет имя или номер протокола ICMP. Допустимые имена можно вывести на экран командой `iptables -p icmp -h`

Ряд опций может использоваться при указании в командной строке `iptables` дополнительно загружаемых модулей. Так, при загрузке модуля limit (`-m n limit`) можно указывать максимальное число пакетов за единицу времени, например, `--limit 5/hour` ограничивает количество передаваемых пакетов данного типа до 5 в час. Модуль state позволяет использовать в правилах состояние соединения: `--state ESTABLISHED`, `--state INVALID`, `--state NEW`, `--state RELATED`. Модуль mac позволяет включить в правила проверку MAC-адресов (опция `--mac-source`). Полный список дополнительных модулей доступен в справочной подсистеме.

Настройка NAT

Рассмотрим пример настройки iptables для работы в качестве сервера NAT. Предполагается, что eth0 — это интерфейс Интернета, eth1 — интерфейс локальной сети.

Сначала необходимо разрешить маршрутизацию в ядре Linux при помощи команды

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

После этого в настройку iptables достаточно добавить только две строки:

```
iptables --table nat --append POSTROUTING --out-interface eth0 -j MASQUERADE
iptables --append FORWARD --in-interface eth1 -j ACCEPT
```

Первая строка разрешает пересылку пакетов с трансляцией адресов, вторая разрешает пересылку на внешний интерфейс пакетов, принимаемых внутренним интерфейсом.

Аутентификация доступа в Интернет

Встроенные межсетевые экраны Linux позволяют очень точно настроить правила фильтрации, но они не работают на уровне сессии. Поэтому в случае использования такой защиты в корпоративной среде у злоумышленников остается возможность присвоения себе адресов других компьютеров для обхода защиты. Выходом в такой ситуации является аутентификация *любой* попытки доступа в Интернет.

Подобные межсетевые экраны предлагают, как правило, коммерческие клиенты для систем на основе Windows. Вы можете приобрести такой продукт, но существуют и иные способы решения.

Один из них основан на подключении пользователя домена к совместно используемому ресурсу на межсетевом экране (такое подключение может быть легко настроено в сценариях входа в домен). Наличие подключения и его параметры используются в сценариях обработки запросов.

Другой способ заключается в предоставлении доступа к Интернет путем организации VPN-подключения к межсетевому экрану. Такой подход часто используется небольшими интернет-провайдерами, поскольку дает возможность легко подсчитать объем трафика каждого клиента.

Squid

Можно настроить доступ к Интернету с использованием аутентификации Windows, если установить прокси-сервер. Преимущество такого решения состоит в кэшировании трафика и, соответственно, снижении расходов организации. Недостаток данного метода заключается в том, что прокси-сервер работает только с трафиком HTTP/HTTPS, поэтому настройку специальных протоколов (например, для онлайн-работы с банком) все равно придется производить на основе IP-адресов источника и назначения[1].

При работе через прокси-сервер пользователь аутентифицируется на нем, а все запросы во внешний мир формируются от имени этого сервера и только с его адреса. Наиболее распространенным прокси для Linux является Squid (**www.squid-cache.org**). Выполнить настройку сервера для любой конфигурации вам поможет информация, которую можно найти на сайте **http://wiki.squid-cache.org/**. Отметим только, что включение аутентификации Windows осуществляется добавлением в конфигурацию следующих строк[2]:

```
auth_param ntlm program /usr/bin/ntlm_auth --helper-protocol=
squid-2.5-ntlmssp
auth_param ntlm children 10
#auth_param ntlm max_challenge_reuses 0
#auth_param ntlm max_challenge_lifetime 2 minutes
#auth_param ntlm use_ntlm_negotiate off
auth_param basic program /usr/bin/ntlm_auth --helper-protocol=
squid-2.5-basic
```

[1] Вообще говоря, в таких ситуациях нет особого риска: в правилах можно точно указать адреса доступа, так что использование данной возможности злоумышленником для работы в сети Интернет практически нереально.

[2] См. **http://wiki.squid-cache.org/ConfigExamples/WindowsAuthenticationNTLM**.

```
auth_param basic children 5
auth_param basic realm Domain Proxy Server
auth_param basic credentialsttl 2 hours
auth_param basic casesensitive off
authenticate_cache_garbage_interval 10 seconds

# Credentials past their TTL are removed from memory
authenticate_ttl 0 seconds
acl lcl src 192.168.0.0/16
acl auth  proxy_auth REQUIRED

http_access allow lcl auth
http_access deny all
miss_access allow all
icp_access deny all
```

Некоторые дополнительные настройки iptables

Выше упоминалось, что межсетевой экран на основе Linux имеет существенно большие возможности по настройке правил фильтрации по сравнению с системами Windows. Чтобы не быть голословным, приведу несколько экзотических примеров, подтверждающих это утверждение.

Создание ловушек

У специалистов по информационной безопасности существует такой метод противодействия атакам, как создание ловушек. Ловушка — это порт, соединение с которым после его установки обычным образом завершается только по тайм-ауту (обычно этот период составляет более 10 минут). Атакующая система все это время будет ожидать ответов и расходовать ресурсы на поддержание соединения.

Например, таким образом можно ввести злоумышленника в заблуждение, если поставить ловушки на порты NetBIOS:

```
iptables -A INPUT -p tcp -m tcp -m mport --dports 135,139 -j TARPIT
```

Балансировка каналов

Iptables позволяет использовать в правилах вероятностный критерий. Таким способом можно заставить систему отправлять пакеты частями на разные адреса. Это не балансировка нагрузки в строгом смысле, но достаточно простой метод распределения трафика по нескольким каналам штатными средствами системы.

Фильтрация по содержимому пакета

В правилах можно использовать критерий для нахождения заданной последовательности символов в передаваемой информации. При этом допускается анализировать как служебные данные пакетов, так и передаваемую внутри них информацию. Таким образом можно, например, запретить передачу файлов определенного типа, задав в качестве критерия поиска характерные для них последовательности символов[1].

Открытие портов по специальным запросам

Iptables позволяет выполнить такие специфические настройки, как открытие порта после принятия определенной последовательности пакетов.

Идея заключается в том, что в настройках межсетевого экрана установление соединения разрешается только после получения определенной последовательности входных пакетов. Таким способом легко предотвращается доступ к серверу сети Интернет: злоумышленник не сможет даже создать подключение, если не знает алгоритма входа. Некоторые варианты реализации такой технологии можно найти по следующим адресам: **http://www.opennet.ru/base/sec/port_knocking.txt.html**, **http://gentoo-wiki.com/HOWTO_Port_Knocking** и т. п.

Почтовый сервер

Один из самых известных почтовых серверов для Linux — это программа Postfix, входящая в состав практически всех дистрибутивных дисков. Почтовые серверы в Linux обеспечивают обмен сообщениями, работу со списками рассылки, а также позволяют создавать правила обработки почты. К ним легко подключаются пакеты, обеспечивающие антивирусную проверку сообщений и фильтрацию спама. При этом существенную часть программ почтовых серверов можно использовать на основе открытой лицензии.

В последнее время от почтового сервера ждут не только обмена сообщениями, но и поддержки функциональности организации групповой работы: наличие календаря и планирования встреч, общих папок хранения сообщений и документов, единых списков контактов и т. п. Возможности групповой работы поддерживаются некоторыми бесплатными продуктами, в частности:

- eGroupware (**http://www.egroupware.org/**);
- Group-Office (**http://www.group-office.com**);
- Open-Xchange (**http://mirror.open-xchange.org/ox/EN/community/**);

[1] Многие форматы можно однозначно определить по содержащимся в файлах служебных заголовках. Такие последовательности несложно найти в Интернете.

- Scalix (**http://www.scalix.com**, бесплатная версия имеет некоторые ограничения функциональности по сравнению с коммерческим вариантом);
- Kolab (**http://www.kolab.org**);
- OGo-OpenGroupware (**http://www.opengroupware.org/**);
- Zimbra (**http://www.zimbra.com/**);
- Open Source Outlook MAPI Connector (**http://www.openconnector.org/**).

Кроме того, существует большое количество коммерческих пакетов для организации групповой работы, например:

- Novell Groupwise (**http://www.novell.com/products/groupwise/**);
- BynariInsightManager (**http://bynari.net/index.php?id=7**);
- Communigate Pro (**http://www.stalker.com/CommuniGatePro/**);
- OfficeCalendar (**http://www.officecalendar.com/**);
- Zarafa (**http://www.zarafa.com/**);
- PostPath (**http://www.postpath.com/**, до 12 пользователей лицензия бесплатна).

Удаленное подключение к Linux

Linux изначально является многопользовательской системой с возможностью удаленного подключения и исполнения команд. Для него не требуется никаких дополнительных программ или режимов.

Наиболее безопасным способом удаленной работы с Linux является использование протокола OpenSSH. При этом на Linux должен быть запущен OpenSSH-сервер, а подключение необходимо осуществлять при помощи OpenSSH-клиента.

OpenSSH-сервер

Вам необходимо убедиться, что сервер SSH установлен и находится в режиме автоматической загрузки. Настройки сервера следует произвести в соответствии с особенностями используемого вами дистрибутива Linux. Более никаких специальных действий производить не требуется.

Подключение OpenSSH-клиента

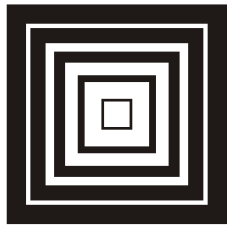
Существуют различные версии SSH-клиентов, разработанных как для Linux, так и для Windows. Использование SSH в принципе не отличается от работы в режиме telnet, но выполняется по шифрованному каналу.

При первом подключении к Linux программа запросит вашего согласия на включение удаленного хоста в число доверенных хостов. При желании вы можете предварительно скопировать открытый ключ хоста Linux для использования в программе SSH-клиента.

Использование графического режима

SSH-подключение обеспечивает работу с программами в режиме консоли. Для работы в графическом режиме нужно использовать программу-клиент. Наиболее распространенным является применение кроссплатформенного пакета VNC, который позволяет использовать в качестве сервера и клиента операционные системы Windows и Linux в любом сочетании (можно подключаться к Linux, работая в Windows, и наоборот).

Для обеспечения возможности подключения к Linux с использованием VNC вы должны проверить, что соответствующий пакет серверного программного обеспечения установлен и включена его автоматическая загрузка. Кроме того, следует настроить конфигурацию сервера VNC, определить допустимое число сессий, пароли и т. д. Эти действия выполняются в соответствии с описаниями справочной системы.



ГЛАВА 3

Структура сети

Информационная система предприятия начинается с соединений между различными устройствами. От качества этих каналов связи не в последнюю очередь зависит стабильность и надежность работы бизнес-приложений.

Структурированные кабельные сети

Согласно действующим правилам, *структурированные кабельные сети* (СКС) должны проектироваться и монтироваться специализированными организациями, имеющими государственную лицензию на данный вид деятельности. Однако на практике в силу высокой стоимости данных работ монтаж СКС в небольших организациях обычно выполняется собственными силами. Провода прокладываются вдоль плинтусов, а по стенам, в основном по эстетическим соображениям, устанавливаются специализированные короба. При этом далеко не всегда выполняются требования, предъявляемые стандартами СКС.

Категории СКС

Кабельные системы характеризуются *категорией*, определяющей качество линии связи (табл. 3.1).

Таблица 3.1. *Категории кабельных систем*

Категория	Максимальная частота сигнала, МГц	Область применения
3	16	Телефонные каналы, локальные сети Ethernet 10Base-T
5	100	Локальные сети со скоростью передачи до 100 Мбит/с
5e	100	Локальные сети со скоростью передачи до 1000 Мбит/с

Таблица 3.1 *(окончание)*

Категория	Максимальная частота сигнала, МГц	Область применения
6	250	Локальные сети со скоростью передачи до 1000 Мбит/с
7	600	Локальные сети со скоростью передачи до 1000 Мбит/с, сети ATM, кабельное телевидение

Кабельную сеть можно отнести к определенной категории, только если при ее создании использованы элементы (розетки, разъемы, кабели и т. п.), удовлетворяющие требованиям данной или более высокой категории, а проектирование и монтаж выполнены в соответствии с требованиями стандартов (ограничения на длины, число точек коммутации и т. д.).

В настоящее время большинство эксплуатируемых кабельных систем относятся к категории 5, которая допускает передачу данных по сети со скоростью до 100 Мбит/с. Категория 5e вводит небольшие дополнительные ограничения, которые позволяют использовать каналы передачи данных с гигабитными сетевыми картами. На практике аккуратно выполненная проводка на элементах категории 5 позволяет осуществлять передачу на скорости до 1 Гбит/с.

Волоконно-оптические сети

При построении кабельной системы предприятия часто возникает необходимость подключения устройств, разнесенных на большие расстояния. В этом случае успешно применяются волоконно-оптические линии связи.

Обычно одно волокно кабеля используется для передачи сигнала, другое — для приема. Существует оборудование, позволяющее за счет использования различных диапазонов излучения передавать и принимать данные по одному волокну, но оно используется не часто: обычно оптические кабели проектируются с большим запасом по числу волокон.

При расстояниях 100—200 метров применяются *многомодовые* оптические кабели. Стоимость прокладки и эксплуатации такой линии практически соизмерима со стоимостью линии на витой паре. При длинах соединений свыше 200 метров используется *одномодовый* оптический кабель. Соответствующее оборудование (приемники и передатчики оптического сигнала) по стоимости в несколько раз дороже, чем модели для многомодового кабеля.

Если расстояние, на которое предполагается передавать данные, измеряется десятками километров, то необходимо использовать передатчики повышенной мощности (они присутствуют в линейках продукции практически всех изготовителей).

Для подключения волоконно-оптических линий применяются специальные модули. Существуют различные модели такого оборудования, на практике в последнее время наиболее распространены SFP-модули[1], подключаемые в соответствующие порты активного оборудования (рис. 3.1). Но поскольку на практике эксплуатируются различные технологии, при проектировании расширения сети следует обращать внимание на совместимость используемых решений[2].

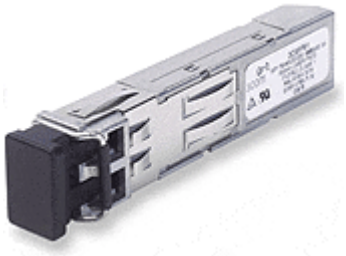


Рис. 3.1. SFP-модуль для подключения оптического канала связи

Эксплуатация волоконно-оптических каналов связи требует повышенной аккуратности со стороны пользователей. Не допускается резко изгибать кабель, следует оберегать оптические поверхности от засорения (не трогать их руками, всегда закрывать концы кабеля и гнезда в модуле подключения специальными заглушками и т. д.). В случае повреждения кабеля обычно требуется приглашение монтажных фирм, поскольку приобретение оборудования для поиска и определения мест неисправности (рефлектометры и т. п.) доступно только специализированным организациям.

Сети 10G

Увеличение объемов информации заставляет постоянно повышать скорости передачи данных. Внедрение мультимедийных приложений (ip-телефония, видеоконференции, системы видеонаблюдения и т. п.) приводит к тому, что величина скорости передачи в 1 Гбит/сек становится недостаточной для магистральных каналов предприятия. Объединение каналов *(см. разд. "Использование “агрегированных” каналов" этой главы)* не позволяет увеличить это значение на порядок.

---

[1] SFP (small form-factor pluggable) — компактный сменный приемопередатчик, регламентирован международным стандартом. В конструктиве SFP выпускаются модули для подключения как витой пары, так и оптических каналов (одномодовых и многомодовых) на различные частоты линии связи.

[2] Например, следует учитывать типы оптических разъемов, которые могут отличаться на оборудовании различных вендоров. Нужно принимать во внимание тип оптического кабеля (выпускаются более чем по 5 стандартам), длину волны и т. п.

Результатом усилий ряда предприятий стала технология передачи на частоте 10 Гбит/сек. В настоящее время стандартизовано использование в данных целях как медного кабеля (витой пары), предназначенного для небольших расстояний, так и оптического. На практике соединения 10G применяются для связи коммутаторов уровня ядра предприятия или при оснащении датацентров, где имеют место самые высокие требования к объемам и скорости передачи данных.

Примечание

Существуют технологии оптического уплотнения (CWDM), позволяющие по одному волокну передавать несколько каналов данных. Но они оправданы только в случае сверхдлинных линий связи и не применяются на уровне предприятий.

Схема разъема RJ45

Для подключения компьютера к коммутатору обычно используется расшивка разъема, показанная на рис. 3.2.

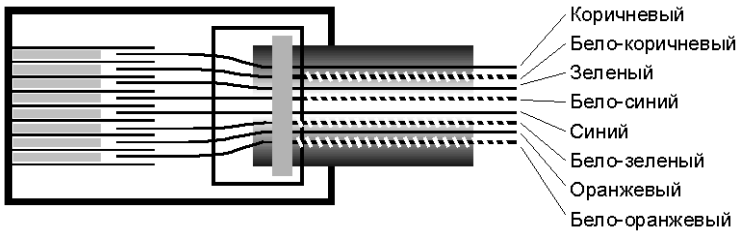


Рис. 3.2. Расшивка разъема RJ45

На практике применяются два варианта расшивки кабеля — A и B. Один (B, показан на рисунке) используется в основном в странах Америки, другой — A — в странах Европы. Варианты отличаются только "переменой мест" зеленой и оранжевой пар.

Однако даже в условиях одной организации можно встретить оба варианта разделки разъема, например, вследствие выполнения работ разными исполнителями или в результате поставок патч-кордов различных исполнений. Вообще говоря, разделка разъема не сказывается на работе оборудования за исключением случая, когда один конец кабеля разделан по варианту A, а другой — по варианту B. На практике такая ситуация чаще всего возникает при использовании розеток и кросс-шкафов (когда разводку в шкафу делает один человек, а розеток — другой) или при укорачивании существующего кабеля (если исполнитель не проверит тип расшивки отрезаемого разъема).

Для передачи сигналов используются только две[1] пары из четырех, имеющихся в кабеле. Хотя это и не разрешается стандартами, администратор может задействовать оставшиеся пары, например использовать средние контакты (пара *голубой — бело-голубой* провода) под телефон, а коричневую пару в качестве замены одной из сигнальных при обнаружении обрыва в кабеле.

Два компьютера можно соединить витой парой *без коммутатора*. Для этого необходима специальная расшивка разъема, которая называется *перекрещенной* (crossover). При такой расшивке на одной из сторон кабеля меняются местами входные и выходные провода (первая и третья пары, см. табл. 3.2). К использованию перекрещенных кабелей приходится прибегать не только в случае соединения "компьютер — компьютер", но и, например, при подключении ADSL-модема непосредственно к сетевой плате компьютера[2] или соединении двух коммутаторов ранних моделей выпуска.

Итоговая расшивка такого кабеля представлена в табл. 3.2.

Таблица 3.2. *Перекрещенная схема разделки разъемов RJ45*

Разъем 1: цвет жилы	**Разъем 2: цвет жилы**
Бело-оранжевый	Бело-зеленый
Оранжевый	Зеленый
Бело-зеленый	Бело-оранжевый
Синий	Синий
Бело-синий	Бело-синий
Зеленый	Оранжевый
Бело-коричневый	Бело-коричневый
Коричневый	Коричневый

Примечание

Современные модели коммутаторов обладают возможностью определения типа расшивки кабеля и автоматически переключаются на нужный вариант. У ранее выпускавшихся моделей такой функции нет, поэтому, например, для соединения двух таких устройств между собой также необходимо использовать crossover-кабель[3].

---

[1] В Gigabit Ethernet на скорости 1000 Мбит/с задействованы все четыре пары.

[2] ADSL-модемы, как правило, имеют порты, предназначенные для подключения к коммутаторам локальной сети.

[3] На некоторых моделях имеется либо кнопка переключения типа одного из портов, либо два разъема для одного порта, соответствующих тому или иному варианту подключения (называемым MDI и MDIX).

Варианты исполнения СКС

Кабельная система предприятия может быть выполнена различными способами: по технологии скрытой проводки, в накладных каналах, в пространстве под фальшполом или над навесным потолком и т. п. Собственными силами прокладка кабелей обычно производится без трудоемких строительных работ — в накладных каналах, при этом переходы между отдельными помещениями осуществляются либо через отверстия в стенах, либо над накладным потолком коридора.

Внимание: патч-корды

Часто в условиях предприятия экономят на кабелях, при помощи которых осуществляется подключение компьютера в розетку кабельной сети. Следует отметить, что эти кабели, называемые *патч-кордами*, часто являются причиной снижения скорости передачи данных. Они подвергаются наибольшему механическому воздействию, в то время как бывают изготовлены специалистом недостаточной квалификации. С течением времени их параметры ухудшаются, что приводит к ошибкам передачи данных, появление которых достаточно трудно заметить.

Обратите внимание, что, по данным одного из производителей патч-кордов, две трети их не проходят тестирования. Трудно ожидать стабильности характеристик от изделий, изготовленных в кустарных условиях, поэтому стоит комплектовать рабочие места только профессионально выполненными патч-кордами.

Составные линии

Стандарты СКС не предусматривают возможности составления линий передачи данных из нескольких участков. Это значит, что соединение компьютера с коммутатором должно состоять из патч-корда, информационной розетки, кабеля, коммутационной панели (на которую "расшит" кабель), патч-корда до разъема на коммутаторе. Если по каким-либо причинам длины кабеля недостаточно (кабель поврежден или сотруднику выделено другое место), то наращивать его *нельзя*.

Однако на практике достаточно часто приходится сталкиваться с необходимостью удлинения кабеля. Ни в коем случае не рекомендуя применять на практике нижесказанное, должен отметить, что на 100-мегабитных сетях кабели вполне удовлетворительно функционируют при наличии скрутки (или, что еще лучше, паяного соединения) двух кусков. При этом следует минимизировать длину участка кабеля, на котором нарушен шаг витой пары. И, поскольку качество контактов скрутки может существенно снизиться через некоторый промежуток времени из-за воздействия внешних условий (например,

окисления под воздействием влаги), следует позаботиться о надежной изоляции такого соединения.

Прокладка силовых кабелей

Каждое рабочее место пользователя должно быть оборудовано розеткой электропитания с заземлением и информационными розетками. В небольших организациях обычно используют розетки существующей электропроводки. При этом следует учитывать, что расстояние между силовой и информационными розетками одного рабочего места по стандарту не должно превышать 1 м. Кроме того, в целях снижения уровня помех и повышения пожароустойчивости в стандартах определяется минимальное расстояние между силовым и информационными кабелями: оно зависит от потребляемой мощности, но обычно можно ориентироваться на значение в 10—15 см. На практике редко удается выдержать такие расстояния, поэтому, чтобы минимизировать влияние силового кабеля, часто используют специальные кабели с экранированием.

При размещении большого числа пользователей в помещении, не оборудованном достаточным количеством силовых розеток, часто осуществляется проводка силовых и информационных кабелей до рабочего места в одном канале. Согласно стандарту, если оба кабеля прокладываются в общем канале, то должна быть предусмотрена сплошная перегородка между силовыми и информационным отсеками.

Примечание

Одним из мощных источников электропомех являются люминесцентные лампы. При прокладке информационных кабелей часто не обращают внимания на их близость к таким лампам, например, при монтаже новых трасс над фальшпотолком. Для снижения влияния данного источника помех не следует допускать прокладку информационного кабеля ближе 15 см от люминесцентной лампы.

Питание по сети Ethernet

Современное оборудование, подключаемое к компьютерным сетям, часто потребляет совсем немного мощности. Учитывая, что в стандартах передачи данных 10/100 Мбит/сек используются только две пары проводников витой пары из четырех имеющихся, часто можно существенно сэкономить на прокладке кабелей, если применить технологию *питания оборудования по кабелю Ethernet* (Power over Ethernet, PoE)).

Какое оборудование запитывают по технологии PoE? Обычно это IP-телефоны, точки беспроводного доступа, камеры видеонаблюдения и т. п.

Существует несколько вариантов обеспечения PoE. Первый состоит в использовании специальных коммутаторов либо уже имеющих функцию PoE,

либо поддерживающих ее (коммутаторы допускают установку дополнительного блока питания, после чего обеспечивается предоставление услуги PoE). Данный способ применяется при наличии значительного числа портов с функцией PoE, например, при эксплуатации в организации IP-телефонов.

Примечание

Администраторы могут использовать управление портами PoE для того, чтобы, например, перегрузить зависшее устройство: достаточно снять напряжение с соответствующего порта, а потом снова подать его при помощи команд управления коммутатором.

Второй способ подачи питания через сеть Ethernet заключается в приобретении специальных блоков питания, включаемых в "разрыв" сетевого кабеля (для подачи напряжения 48 В используется коричневая пара проводников). Такое решение оправдано при подключении единичных устройств.

В PoE-коммутаторах применяется специальная технология для проверки порта. Перед подачей питания на порт производится специальное тестирование, замеряются параметры подключенного оборудования и, если оно соответствует требованиям технологии PoE, коммутатор включает питание. Таким образом, в порты PoE можно безопасно включать обычные устройства. При использовании же "врезных" блоков питания, особенно самых дешевых их вариантов, следует исключить возможность случайного подключения другого оборудования.

В соответствии со стандартом 802.3af максимальная мощность, которая может быть получена устройством с PoE-порта, составляет 12,95 Вт (при этом порт должен обеспечить мощность до 15,4 Вт). Подключаемые устройства часто потребляют меньшую мощность, например, типовая точка беспроводного доступа потребляет около 11 Вт, IP-телефоны — от 2 до 14 Вт в зависимости от модели. В целях экономии на большинстве моделей коммутаторов суммарно допустимая мощность питания по портам Ethernet меньше величины 15,4 × <количество портов> Вт. В случае превышения допустимого значения потребляемой мощности коммутатор начинает *отключать* питание отдельных портов, учитывая *приоритеты* портов для PoE, которые администратору необходимо назначить вручную в соответствии с предназначением подключенного оборудования.

Требования пожарной безопасности

Основные требования пожарной безопасности при прокладке кабелей в офисе заключаются в следующем:

- кабели, каналы, розетки и т. п. должны соответствовать определенной категории пожароустойчивости; обычно это выполняется при помощи современных элементов СКС;

- силовые и информационные кабели при прокладке в одном канале должны быть разделены сплошной перегородкой. Минимальное расстояние от силовых кабелей до информационных определяется по специальным нормативам в зависимости от нагрузки, но обычно не должно быть менее 12—15 см;
- отверстия, выполненные для прокладки кабелей между помещениями, должны быть закрыты легкоудаляемым негорючим материалом, например, цементом или гипсом низкой прочности, минеральной ватой и т. п.;
- при прокладке кабелей в пространстве над навесным потолком недопустимо использовать горючие материалы[1].

Физическая топология сети здания

Размеры сегментов сети на витой паре

Длина кабеля от одного элемента активного оборудования до другого, например от компьютера до коммутатора, в сети Ethernet не должна превышать 100 м. Обычно стандартами предусмотрена максимальная длина самого кабеля 90 м, а 10 м отводится на соединительные кабели[2].

Для локальной 10-мегабитной сети, построенной на *концентраторах*, существует "правило 5/4": между любыми двумя сетевыми устройствами должно быть не более 5 сегментов сети с четырьмя концентраторами *(хабами)*. Это требование ограничивает размер сети с концентраторами, построенной на витой паре, диаметром 500 м. Ограничение на длины обусловлено самой природой Ethernet, принципами, на которых строится такая сеть, и не зависит от совершенствования элементной базы. В сети Ethernet каждая система может начать передачу данных в произвольный момент времени, независимо от других устройств. Если во время передачи система обнаруживает чужую посылку данных, то эта ситуация[3] детектируется и данные будут повторно переданы каждой из этих систем через некоторый случайный промежуток вре-

---

[1] В случае монтажа кабельной системы под фальшполом нормативами налагаются более строгие ограничения. Например, разделение пространства под фальшполом на зоны, отделяемые друг от друга несгораемыми материалами и т. п.

[2] На практике длина патч-кордов обычно составляет 1 м и более. Обратите внимание, что не имеет смысла применять самодельные короткие патч-корды, например, для подключения сервера к патч-панели, если оба этих элемента расположены рядом ("фирменные" кабели не могут быть короче ~60 см). При малой длине кабеля возрастает уровень помех, возникающих при отражении высокочастотных сигналов от точки соединения кабеля и розетки. Это может привести к увеличению числа ошибок в линии.

[3] Одновременная передача информации несколькими системами называется *коллизией*.

мени. При больших размерах участка сети такая коллизия может быть не обнаружена (система "не услышит" чужой пакет во время попытки своей передачи), что приведет к потере данных, повторам передачи и результирующему снижению пропускной способности сети.

Хотя в 100-мегабитной сети обычно используются только коммутаторы, на практике в ряде организаций эксплуатируются и концентраторы. Стандартом предусмотрено в этом случае использование максимум *двух* концентраторов с расстоянием между ними *не более 5 м*.

Типовая структура сети предприятия

На практике существует два подхода к построению каналов передачи данных. В первом случае развитие начинается от комнаты системного администратора, в которой устанавливается коммутирующее оборудование, становящееся центром сети. В дальнейшем, по мере увеличения числа рабочих мест, к сети подключаются новые коммутаторы, и структура сети принимает достаточно хаотичный вид (рис. 3.3).

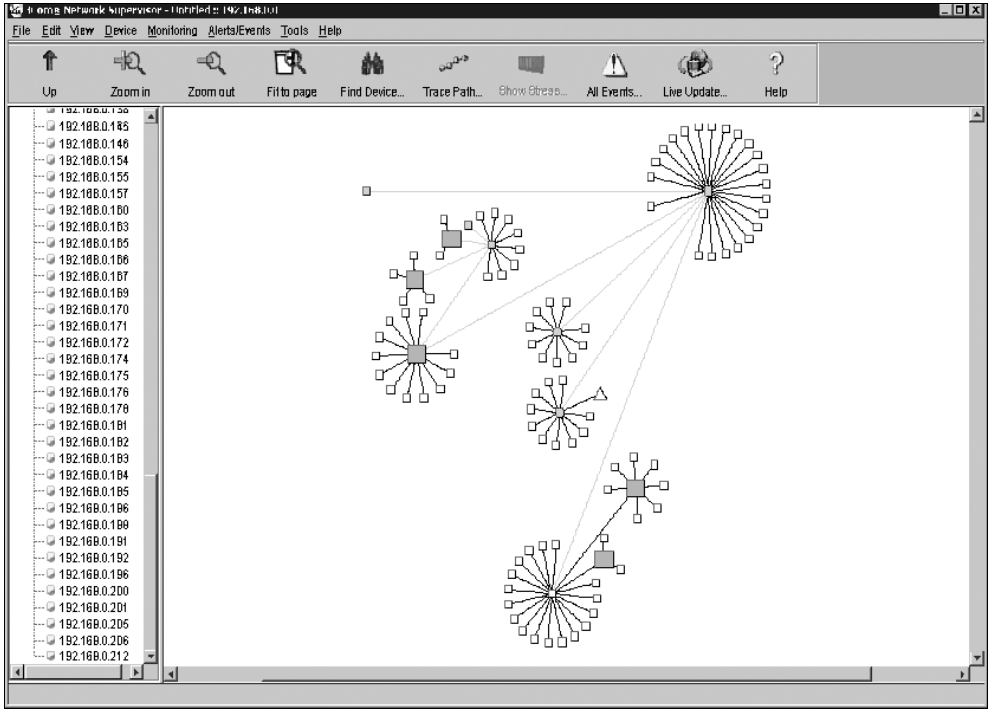


Рис. 3.3. Структура локальной сети небольшого предприятия после некоторого периода неуправляемого развития

Подобная сеть, хотя и обеспечивает текущее функционирование сетевых приложений, не является отказоустойчивой и часто не позволяет внедрить современные решения, критичные к параметрам инфраструктуры.

Если предприятие въезжает в новый офис, то, как правило, структура сети проектируется "с нуля". Принято выделять несколько *уровней* структуры.

Уровни ядра, распределения и доступа

Современная сеть создается на основе трех уровней: ядра (Core), распределения (Distribution) и доступа (Access), как это показано на рис. 3.4. На уровне доступа обеспечивается подключение конечных рабочих станций. На уровне распределения реализуется маршрутизация пакетов и их фильтрация (на основе списков доступа и т. п.). Задача оборудования уровня ядра — максимально быстро передать трафик между оборудованием уровня распределения.

Если рассматривать типовую сеть небольшой организации, занимающей несколько этажей одного здания, то уровень распределения будет соответствовать оборудованию, объединяющему коммутаторы каждого этажа, а уровень ядра — активному оборудованию, размещаемому обычно в главной серверной.

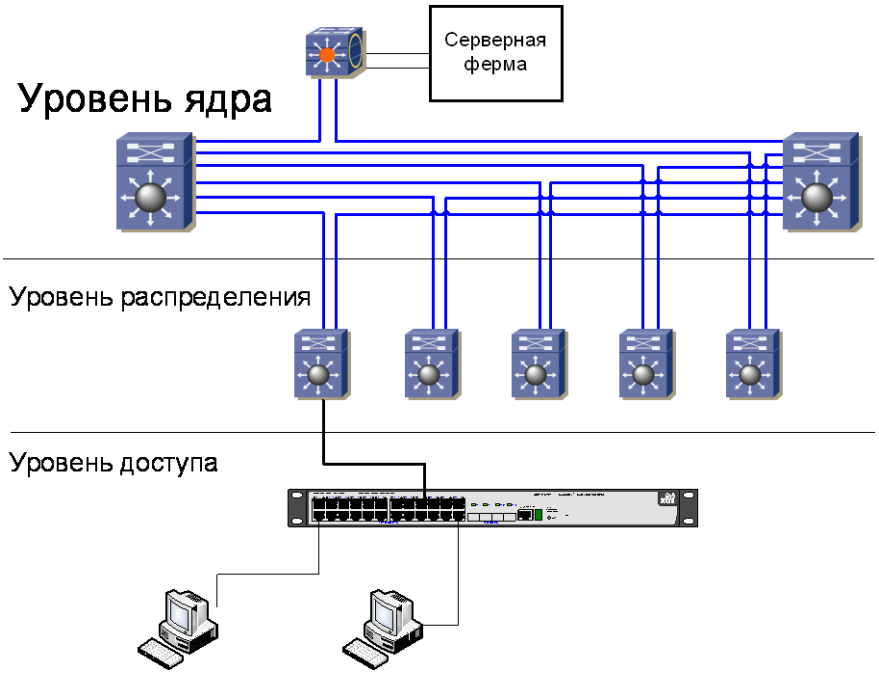


Рис. 3.4. Трехуровневая структура сети

Это классическая схема иерархической структуры, которая на практике часто модифицируется с учетом специфики организации, оборудования и т. д. Так, в зависимости от размеров предприятия, может отсутствовать какой-либо уровень, и структура сети станет двухуровневой. Маршрутизацию данных можно реализовать на уровне ядра, а оборудование уровня распределения будет только пересылать данные внутри сегмента сети. Все зависит от решаемых задач, распределения потоков информации и предъявляемых к информационной системе требований.

Часто в схеме сети выделяют *серверную ферму*. Принципиально серверная ферма представляет собой обычный узел распределения, но реализованный на быстродействующем оборудовании и, как правило, со 100%-ным резервированным решением. В малых организациях часто практикуется подключение серверов непосредственно к ядру сети передачи данных.

Трехуровневая схема больше свойственна крупным сетям. Для средних и небольших предприятий чаще всего создается двухуровневая схема: существует один, обычно самый мощный коммутатор, к которому подключаются как серверы, так и рабочие станции. К этому коммутатору подключены коммутаторы второго уровня, распределяющие данные на остальные рабочие станции.

На практике структуру сети администраторам обычно приходится "примерять" на уже существующие линии связи, ограничиваться возможностями по созданию новых соединений (учитывая, по какой трассе можно проложить линию связи собственными силами) и т. д. Поэтому одной из основных рекомендаций при изменении топологии сети должна быть минимизация количества коммутаторов между любыми двумя точками подключения компьютеров.

Топология каналов сети распределенного предприятия

Если при построении сети внутри здания обычно удается придерживаться иерархии связей "здание — этаж — рабочее место", то в случае размещения предприятия в нескольких зданиях структура сети в значительной степени определяется возможностями прокладки внешних кабелей. Наличие кабельной канализации, воздушных линий связи, кабельных эстакад и т. п. достаточно жестко определяют возможные направления каналов передачи данных.

Поскольку стоимость прокладки кабелей между зданиями достаточно высока, обычно прокладывается лишь минимум связей, которые обеспечат отказоустойчивость сетевой структуры. При этом весьма часто используется *кольцевая* структура, иногда снабжаемая "перемычкой" для снижения числа промежуточных узлов между двумя узлами распределения. На рис. 3.5 приведен вариант подобной структуры сети крупного распределенного предприятия.

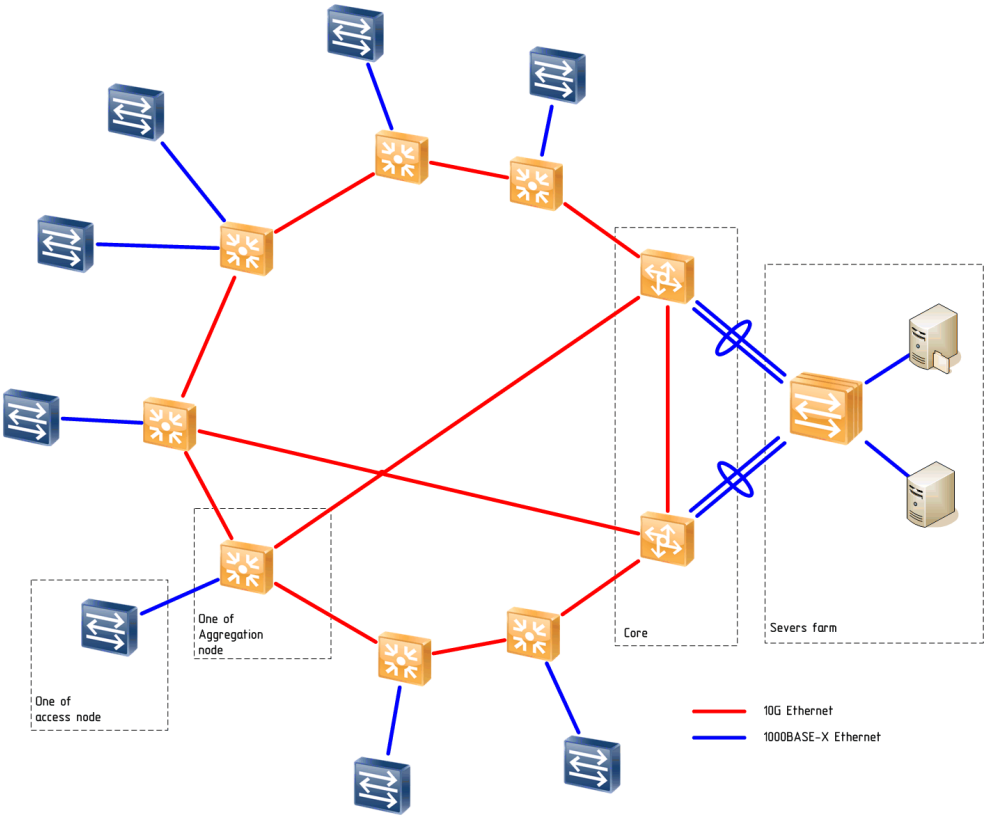


Рис. 3.5. Вариант структурной схемы связей территориально распределенной информационной системы

Документирование структуры каналов связи

Традиционной проблемой большинства организаций является документирование своей кабельной подсистемы. Специализированные программные продукты, позволяющие поддерживать схемы сети с учетом вносимых в нее изменений в актуальном состоянии, стоят весьма дорого, а исходная документация быстро становится неактуальной после нескольких перемещений сотрудников и прокладки дополнительных каналов связи.

Существует много программ, которые позволяют автоматически воспроизвести структуру сети. Окно одной из таких программ — 3 Com Network Supervisor — представлено на рис. 3.3. С помощью данных, собираемых программой, легко находить точки подключения компьютеров к коммутаторам, обнаруживать те или иные неисправности конкретной конфигурации.

Естественно, что получаемая диаграмма тем точнее, чем более интеллектуальные активные устройства используются в сети. В случае эксплуатации неуправляемых устройств возможностей у администратора существенно меньше.

Логическая структура сети

Разбиение сети на сегменты

СКС — самая "консервативная" часть информационной системы предприятия. Любое ее изменение сопряжено с существенными материальными затратами. Однако возможность переконфигурирования инфраструктуры часто может существенно повысить управляемость и надежность всей системы. Например, объединение портов управляемых по сети устройств (коммутаторы, аварийные источники питания и т. п.) в "физически обособленную" сеть существенно повышает уровень безопасности системы, исключая доступ к таким элементам с произвольных рабочих станций. Кроме того, выделение, например, компьютеров бухгалтерии в отдельную сеть исключает доступ к ним по сети всех остальных пользователей.

Подобная возможность изменения конфигурации реализуется путем создания *виртуальных сетей* (Virtual local area network, VLAN). VLAN представляет собой логически (программно) обособленный сегмент основной сети. Обмен данными происходит *только* в пределах одной[1] VLAN. Устройства разных VLAN *не видят* друг друга. Самое главное, что из одной VLAN в другую не передаются широковещательные сообщения.

VLAN можно создать *только* на управляемых устройствах; самые дешевые модели (часто их называют *офисными*) такую возможность не поддерживают.

Варианты создания VLAN

На практике существует несколько технологий создания VLAN. В простейшем случае порт коммутатора приписывается к VLAN определенного номера (port based VLAN или *группировка портов*). При этом одно физическое устройство логически разбивается на несколько: для каждой VLAN создается "отдельный" коммутатор. Очевидно, что число портов такого коммутатора можно легко изменить: достаточно добавить или исключить из VLAN соответствующий физический порт.

Второй часто используемый способ заключается в отнесении устройства к той или иной VLAN на основе MAC-адреса. Например, так можно обосабливать камеры видеонаблюдения, IP-телефоны и т. п. При переносе устройства

[1] Одна VLAN может объединять порты нескольких коммутаторов (VLAN с одинаковым номером на разных коммутаторах считаются одной и той же VLAN).

из одной точки подключения в другую оно останется в прежней VLAN, никакие параметры настройки менять не придется.

Третий способ заключается в объединении устройств в сеть VLAN по сетевым протоколам. Например, можно "отделить" протокол IPX от IP, "поместить" их в разные VLAN и направить по различным путям.

Четвертый способ создания VLAN состоит в многоадресной группировке.

Примечание

Обычно рекомендуется включать магистральные порты коммутаторов (порты, соединяющие коммутаторы) во все VLAN, существующие в системе. Это значительно облегчает администрирование сетевой структуры, поскольку иначе в случае отказа какого-либо сегмента и последующего автоматического изменения маршрута придется анализировать все варианты передачи данных VLAN. Важно помнить, что ошибка в таком анализе, неправильный учет какого-либо фактора приведет к разрыву VLAN.

VLAN открывают практически безграничные возможности для конфигурирования сетевой инфраструктуры, соответствующей требованиям конкретной организации. Один и тот же порт коммутатора может принадлежать одновременно нескольким виртуальным сетям, порты различных коммутаторов — быть включенными в одну VLAN и т. п.

На рис. 3.6 показан пример построения VLAN из компьютеров, подключенных к различным коммутаторам. Обратите внимание, что при использовании

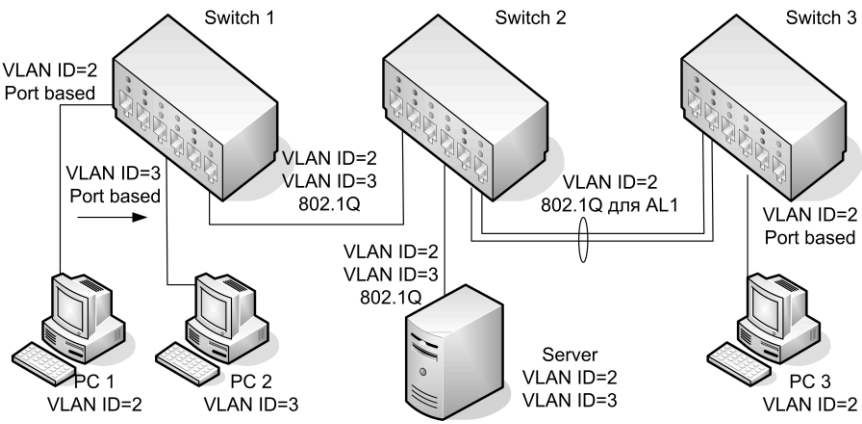


Рис. 3.6. Пример построения VLAN на нескольких коммутаторах.
Поскольку предполагается, что сервер подключается к нескольким VLAN и серверный сетевой адаптер поддерживает создание tagged VLAN, то в этом случае используется настройка серверного порта коммутатора по стандарту 802.1q. Для реализации возможности передачи данных VLAN между коммутаторами соответствующие порты, подключенные к связующей линии, в режиме 802.1q настраиваются на членство в тех виртуальных сетях, данные которых должны передаваться через эту линию связи. Для простоты VLAN по умолчанию (ID = 1) не отображена

агрегированных каналов (на рисунке для связи устройств Switch 2 и Switch 3) в состав VLAN на каждом коммутаторе должны включаться именно *агрегированные порты* (обычно получают названия AL1, AL2 и т. д.).

Теги 802.1q

В соответствии со стандартом 802.1q номер VLAN передается в специальном поле кадра Ethernet, которое носит название TAG. Поэтому пакеты, содержащие такое поле, стали называть *тегированными* (tagged), а пакеты без этого поля — *нетегированными* (untagged). Поле TAG включает в себя данные QoS (поэтому все пакеты, содержащие информацию о качестве обслуживания, являются тегированными) и номер VLAN, на который отведено 12 бит. Таким образом, максимально возможное число VLAN составляет 4096.

Сетевые адаптеры рабочих станций обычно не поддерживают теги, поэтому порты коммутаторов уровня доступа настраиваются в варианте untagged. Для того чтобы через один порт (обычно это магистральные порты или порты соединения двух коммутаторов) можно было передать пакеты *нескольких* VLAN, он включается в соответствующие VLAN в режиме tagged. Коммутатор будет анализировать поля TAG принятых пакетов и пересылать данные только в ту VLAN, номер которой содержится в поле. Таким образом через один порт можно безопасно передавать информацию нескольких VLAN.

Примечание

При соединениях "точка — точка" порты для одинаковых VLAN должны быть либо оба tagged, либо оба untagged.

VLAN 1

При создании VLAN следует учитывать тот факт, что служебная сетевая информация пересылается нетегированными пакетами. Для правильной работы сети администратору необходимо обеспечить передачу таких пакетов по всем направлениям. Самый простой способ настройки заключается в использовании VLAN по умолчанию (VLAN 1). Соответственно, все порты компьютеров необходимо включать в VLAN с другими номерами.

В VLAN 1 по умолчанию находятся интерфейсы управления коммутаторами, причем ранее выпускавшиеся модели коммутаторов не позволяют сменить номер для VLAN управления. Поэтому администратору следует тщательно продумать систему разбиения на VLAN, чтобы не допустить случайного доступа к управлению коммутаторами посторонних лиц, например, можно переместить *все* порты доступа коммутатора в другую VLAN, оставив для VLAN 1 только магистральный порт. Таким образом, пользователи не смогут подключиться к управлению коммутатором.

GVRP

Протокол GVRP[1] предназначен для автоматического создания VLAN. С его помощью можно автоматически назначать порты во все вновь создаваемые VLAN. Несмотря на определенные удобства, такое решение является существенной брешью в системе обеспечения сетевой безопасности. Администратор должен представлять структуру VLAN и производить назначения портов ручными операциями.

Маршрутизация в сетях предприятий

Информация внутри локальной сети, которая определяется IP-адресом и маской подсети, пересылается от одного компьютера к другому: отправитель посылает пакет непосредственно на физический адрес получателя. Если отправитель и получатель данных находятся в различных сетях, то данные, предназначенные для компьютера другой сети, передаются на специальное устройство — *маршрутизатор*, которое должно обеспечить пересылку информации. В малых организациях обычно существует только одна точка подключения к глобальной сети, поэтому правила пересылки данных крайне просты: информация для внешней сети должна пересылаться на один компьютер (обычно назначаемый *шлюзом по умолчанию*), который пересылает все такие данные на один адрес во внешней сети.

Как уже говорилось, отдельные VLAN изолированы друг от друга. На практике обычно возникает необходимость *управляемой* передачи данных из одной VLAN в другую, для того чтобы, например, обеспечить доступ компьютеров к серверам организации или в Интернет. В этих случаях необходимо настроить *машрутизацию*.

Обычно маршрутизация выполняется средствами активного оборудования сети передачи данных. Коммутаторы, которые могут передавать пакеты из одной сети в другую, называют коммутаторами *уровня 3*[2]. Коммутаторы уровня 2 могут только разбить сеть на несколько VLAN; передать данные из одной VLAN в другую они не могут.

Примечание

Функцию маршрутизации могут выполнить программным образом как серверы, так и рабочие станции Windows[3]. Это допустимо в небольших сетях, но требует установки дополнительных сетевых адаптеров и соответствующей настройки. Обычно функцию маршрутизации возлагают на активное сетевое оборудование, поскольку это более надежное и производительное решение.

---

[1] Generic VLAN Registration Protocol.

[2] *См. разд. "Модель OSI" далее в этой главе.*

[3] Для включения маршрутизации в Windows XP требуется ручная настройка параметров реестра.

Для использования функций маршрутизации на коммутаторах третьего уровня для VLAN необходимо создать *интерфейсы* и присвоить им IP-адреса. После этого между таким VLAN может быть осуществлена пересылка пакетов.

Если на одном коммутаторе создано несколько интерфейсов VLAN и им присвоены IP-адреса, то такие интерфейсы станут считаться *локальными*, маршрутизация между ними будет включена сразу же.

Автоматизация настроек маршрутизации

Обычно VLAN распределены по всей сети организации и информация, предназначенная для конкретной VLAN, должна "пройти" через несколько промежуточных сетей. Соответствующие пути могут быть определены вручную *(статическая маршрутизация)*. Но при большом числе VLAN вручную отслеживать изменения, тем более автоматически перестраивать пути в случае повреждения каналов связи, становится практически нереальным. На помощь приходят протоколы автоматической маршрутизации.

В относительно небольших организациях применяются два протокола: RIP и OSPF.

RIP

RIP[1] — самый простой в использовании протокол автоматической маршрутизации. Он не требует никакой настройки от администратора. Достаточно только включить использование RIP для всего маршрутизатора и для каждого отдельного интерфейса VLAN.

RIP периодически рассылает широковещательным (RIP версии 1) или мультикастовым (RIP версии 2) образом информацию о собственной таблице маршрутизации. Приняв аналогичный пакет от другого маршрутизатора, RIP производит изменение локальной таблицы маршрутизации. В результате через некоторый промежуток времени коммутаторы будут "знать" маршруты, присутствующие на каждом устройстве.

Недостатками RIP являются излишняя "шумливость" (постоянная рассылка большого количества информации) и плохая масштабируемость для крупных сетей.

OSPF

Протокол OSPF[2] позволяет создавать таблицы маршрутизации больших сетей. Он требует предварительной настройки, хотя в случае не очень крупной сети эти операции не являются сколько-нибудь сложными.

---

[1] Routing Information Protocol.

[2] Open Shortest Path First.

В самой минимальной конфигурации достаточно включить использование протокола OSPF на коммутаторе, создать одну область (обычно ее называют *областью 0* — area 0) и активизировать протокол OSPF для каждого интерфейса VLAN.

Протокол OSPF позволяет настроить безопасную передачу данных о таблицах маршрутизации (данные будут приниматься, например, только после идентификации маршрутизатора безопасным способом).

Различным линиям связи можно назначить *весовые коэффициенты*, что позволит администратору более точно настроить выбираемые коммутатором пути передачи данных. В случае сложной структуры сети можно создать несколько различных зон и настроить их параметры так, чтобы минимизировать служебный трафик и ускорить сходимость таблиц маршрутизации в случае изменения топологии.

DHCP-relay

Запросы на получение IP-адреса являются широковещательными и рассылаются только в пределах одной VLAN. Создание надежной службы DHCP для каждой VLAN обычно нерационально, поскольку один DHCP-сервер может обслуживать большое число сетей.

Для передачи запроса на получение IP-адреса из одной сети в другую необходимо использовать специальную программу, называемую агентом DHCP, которая будет проверять наличие в сети запросов на получение IP-адреса и переправлять их на сервер DHCP уже от своего IP-адреса. Такие пакеты маршрутизируются между сетями, поскольку являются одноадресными (приходит с адреса агента на адрес DHCP-сервера). Сервер DHCP, получив такой запрос, "знает", что нужно предоставить IP-адрес из диапазона адресов, соответствующего адресу агента, сообщает всю информацию агенту и процесс завершается обычным для аренды адреса образом.

DHCP-агента можно реализовать как программным образом на сервере Windows в настройке службы маршрутизации и удаленного доступа, так и на коммутаторах третьего уровня.

В случае настройки коммутатора достаточно включить данную функцию и для каждого интерфейса VLAN указать адреса DHCP-серверов, на которые следует пересылать запросы аренды адреса.

Программная маршрутизация

Рабочие станции Windows могут выступать в качестве маршрутизаторов только при установке специализированных программ третьих фирм, например, WinRoute. Существует большое количество аналогичных программ

(многие из которых бесплатны), используемых даже в системах на Windows 9*x*. Серверы Windows уже включают в себя возможность маршрутизации — в их составе присутствует Служба маршрутизации и удаленного доступа (Routing and Remote Access Server, RRAS).

RRAS

Служба RRAS осуществляет многопротокольную[1] маршрутизацию пакетов, позволяет создавать соединения по требованию и осуществлять для них маршрутизацию данных. Начиная с Windows 2000, служба RRAS устанавливается автоматически, но находится в *отключенном состоянии*. Для ее запуска следует открыть консоль управления RRAS и выполнить задачу **Настроить и включить маршрутизацию и удаленный доступ**.

Сервер RRAS может выполнять как *статическую*, так и *динамическую* маршрутизацию. Настройка статической маршрутизации через оснастку RRAS — это просто использование графического интерфейса вместо утилиты `route`. Больший интерес представляет возможность включения динамических протоколов маршрутизации — Routing Information Protocol (RIP) и Open Shortest Path First (OSPF).

Мост

Частным случаем взаимодействия двух сетей является такой вариант объединения сегментов, когда сигналы из одного сегмента должны без всякого ограничения попадать в другой, и наоборот. Реализовать эту функцию легко даже на рабочих станциях путем создания *мостов* (bridges).

Создание моста на рабочих станциях Windows XP позволяет "прозрачно" объединить несколько Ethernet-сетей. Например, обеспечить передачу пакетов из беспроводного сегмента сети в локальную сеть или соединить несколько сегментов сети, к которым подключен данный компьютер.

Для создания *моста* между сегментами следует открыть задачу **Сетевые подключения**, выделить два соответствующих Ethernet-адаптера и в меню свойств выбрать команду **Создать мост**.

Примечание

При создании моста используются алгоритм spanning tree algorithm, который предупреждает зацикливание пересылки пакетов, если соединяемые мостом сегменты имеют и другие точки взаимного подключения.

[1] Служба маршрутизирует протоколы IP, IPX, AppleTalk.

Поскольку мост обеспечивает передачу *всех* пакетов из одного сегмента сети в другой, то данное решение не следует использовать для интерфейсов доступа в Интернет.

Надежность сетевой инфраструктуры

Необходимым условием надежной работы информационной системы является безотказное функционирование каналов связи. Данная задача решается путем *дублирования* как собственно каналов связи, так и активного оборудования (коммутаторов). Понятно, что на практике отказоустойчивая конфигурация сети создается только в тех случаях, когда простои в работе информационной системы недопустимы и могут привести к существенным экономическим потерям.

Дублирование каналов связи и оборудования производят как в ядре сети (обязательно), так и на уровне распределения (рекомендуется). Подключение оконечных устройств (рабочих станций пользователей) не дублируется.

Отказоустойчивая топология сети передачи данных

На рис. 3.4 и 3.5 показаны варианты отказоустойчивой схемы сети передачи данных. Связи между коммутаторами уровня распределения и ядра дублированы, коммутаторы также дублированы. Серверы предприятия отказоустойчивым образом подключены к коммутаторам ядра (один сетевой интерфейс сервера подключен к одному коммутатору, второй — к другому).

Примечание

Отказоустойчивые схемы, несмотря на кажущуюся простоту, требуют тщательной настройки коммутаторов. При этом в зависимости от выбранного варианта конфигурации может потребоваться использование протоколов, которые не поддерживаются относительно дешевыми моделями оборудования.

Простое соединение двух коммутаторов двумя кабелями создаст кольцо, которое недопустимо в сети Ethernet. Результатом станет широковещательный шторм и практическая неработоспособность сегмента сети. Поэтому создание отказоустойчивых решений требует первоначальной настройки[1] активного оборудования.

Существует два варианта построения сети, использующей топологию соединений, изображенную на рисунках. Первый вариант использует протоколы,

[1] У коммутаторов, предназначенных для использования на уровне доступа, обычно по умолчанию включены протоколы, которые "разорвут" такое кольцо. Коммутаторы уровня ядра не имеют таких настроек, поэтому возникновение кольца быстро приведет к падению сегмента сети.

работающие на втором уровне модели OSI. Второй основан на протоколах маршрутизации третьего уровня модели OSI.

Построение отказоустойчивой сети на основе протоколов второго уровня

Отказоустойчивая конфигурация, построенная с использованием протоколов второго уровня, обеспечивает самое быстрое восстановление в случае аварии. Сеть может восстановиться за 13 секунд или даже еще быстрее в случае использования проприетарных протоколов[1].

Использование протоколов остовного дерева

Протоколы остовного дерева — Spanning Tree Protocol (STP, стандарт 802.1d) и Rapid Spanning Tree Protocol (RSTP, стандарт 802.1w) — используются для автоматического построения связей сетевой структуры. Коммутаторы пытаются вычислить оптимальные маршруты между всеми устройствами по определенным алгоритмам и автоматически блокируют (отключают) порты в случае обнаружения петель[2]. Для определения маршрутов и контроля соединений по специальным алгоритмам постоянно рассылаются служебные пакеты (Bridge Protocol Data Units, BPDU). В случае изменения структуры сети производится ее переконфигурирование. Этот процесс занимает от 30 секунд до нескольких минут в зависимости от размера сети для протокола STP. При использовании RSTP (усовершенствованной версии STP) время перестройки уменьшается до нескольких секунд.

Протоколы могут обеспечить связность сети без каких-либо ручных настроек. При построении структуры алгоритмы учитывают скорость соединения и количество коммутаторов между точками. Администратору нужно только включить данные протоколы на портах (часто это настройка по умолчанию для коммутаторов уровня доступа). На основании анализа рассылки пакетов BPDU коммутатор определяет существующие связи и автоматически отключает порты, к которым подключены вторые, резервные каналы.

Для оптимизации дерева связей целесообразно *вручную* назначить приоритеты коммутаторам: устройство в центре сети должно иметь самый малый

---

[1] Проприетарным называют протокол, не описываемый открытым стандартом, а являющийся уникальной технологией определенного вендора. Хотя использование проприетарных решений позволяет получить лучшие показатели по сравнению с открытыми стандартами, но такой выбор связан с ориентацией на использование оборудования только одного вендора и с вытекающими из этого рисками.

[2] Для этого достаточно воткнуть один патч-корд в два порта коммутатора (например, пользователь увидел свободный конец патч-корда, не проверил, что другой конец его включен в розетку, и подключил разъем в соседнюю свободную розетку).

"вес"[1] (Bridge ID или Bridge Priority); чем дальше от логического центра, тем большие веса нужно назначать коммутаторам. Кроме того, в случае использования протокола RSTP желательно настроить опцию быстрого старта порта (Fast Start) для тех портов, к которым подключены конечные устройства. Это исключит такие порты из процедуры определения маршрутов и ускорит сходимость.

Протоколы STP/RSTP поддерживаются всеми современными коммутаторами. Однако серьезным недостатком их применения является *отключение* резервных связей. Резервные связи не используются для передачи данных и включаются только в случае повреждения основного канала.

Примечание

Поддержку протоколов STP/RSTP следует включать не только при наличии избыточных каналов связи. Включение этой функции позволит сохранить функционирование сети в случае случайного или умышленного создания петель, которые без данных протоколов приведут к широковещательному шторму и практическому прекращению функционирования сегмента. Обычно протоколы STP/RSTP на коммутаторах уровня доступа включаются по умолчанию.

Использование стандарта MSTP

Протокол MSTP (Multi Spanning Tree Protocol описан в стандарте 802.1s) и является расширением протокола RSTP на сеть с VLAN[2].

В отличие от RSTP, MSTP строит дерево связей с учетом созданных на коммутаторах VLAN. Поэтому предупреждение петель происходит не путем отключения порта коммутатора, а через отключение передачи данных *только* для определенной VLAN. Иными словами, можно настроить MSTP таким образом, чтобы для части VLAN было заблокировано одно соединение из дублированных ссылок, а для других VLAN — второе[3]. Таким образом все соединения будут передавать данные. В случае повреждения канала связи MSTP обнаружит это событие и автоматически перестроит структуру.

Главный недостаток решения на протоколе MSTP заключается в сложности настройки такой структуры. Администратор должен четко представлять разбиение системы на VLAN, оценить потоки данных в каждом сегменте и пу-

---

[1] Алгоритм выбора приоритета коммутатора основан на MAC-адресе устройства, поэтому ранее установленное и, соответственно, более старое устройство, как имеющее меньший номер MAC, получит приоритет в процедуре выбора корневого коммутатора. На практике обычно происходит с точностью до наоборот: в центр сети целесообразно поместить самое новое и, следовательно, самое производительное устройство.

[2] Точнее, протокол RSTP стал частью протокола MSTP.

[3] Для этого в настройках протокола администратору вручную нужно назначить каналам различные веса: в одном случае первый канал будет основным, а второй — резервным; в другом — наоборот.

тем ручной настройки добиться относительно равномерного использования всех каналов связи.

Также следует учитывать, что во многих моделях коммутаторов (особенно бюджетного ряда) поддержка протокола MSTP не реализована.

Использование "агрегированных" каналов

Стандарт 802.3ad описывает агрегированные каналы. Агрегированный канал позволяет объединять несколько линий связи между коммутаторами в один общий канал передачи данных. Соответственно, агрегированный канал имеет пропускную способность, равную сумме пропускных способностей объединяемых каналов. При передаче данных задействованы оба канала[1], причем в случае отказа одного из соединений все данные начинают передаваться через оставшийся канал. Агрегированный канал может настраиваться как вручную явным указанием объединяемых портов, так и автоматически на основе специального протокола LACP — Link Aggregation Control Protocol. Соответствующие настройки выполняются в программе конфигурирования коммутаторов.

К сожалению, стандарт не описывает многоточечное подключение, т. е. соединение должно быть осуществлено *только* между двумя устройствами.

На практике многие вендоры создали решения, позволяющие "обойти" данное ограничение. Были разработаны технологии, в которых агрегированный канал создается из двух и более ссылок, соединяющих объединенные в один стек коммутаторы. При этом настройка такого решения выполняется аналогично созданию агрегированного канала в пределах одного коммутатора.

Подобные решения требуют специальной организации стека коммутаторов; они разработаны различными вендорами (3Com, Nortel, Cisco и т. п.), но могут в каждом случае иметь уникальные названия. При этом конкретные реализации могут быть совместимы между оборудованием различных вендоров (например, MLT от Nortel идентичен технологии EtherChannel от Cisco и т. д.). Самым главным для администраторов сетей является тот факт, что два канала подключения любого его устройства к различным коммутаторам могут быть объединены в один агрегированный канал на основе открытого стандарта — 802.3ad таким образом, как будто подключение осуществляется к одному коммутатору. Например, так можно осуществить отказоустойчивое

[1] Распределение данных по отдельным каналам производится на основе подсчета хэш-функции от MAC-адресов источника и назначения. В результате каналы загружаются относительно равномерно, но передача данных между компьютером А и компьютером Б всегда происходит только по одному каналу, поэтому максимальная скорость передачи данных между двумя устройствами всегда определяется только одним каналом передачи данных. При этом в целом происходит общее увеличение пропускной способности.

подключение сервера к ферме коммутаторов: достаточно, чтобы программное обеспечение было настроено на поддержку протокола LACP.

Добиться полной отказоустойчивости такого решения можно, объединив коммутаторы в *отказоустойчивый* стек. При его создании все коммутаторы объединяются в кольцо, последний коммутатор объединяется возвратным стековым кабелем с первым коммутатором. В результате отказ любого устройства стека сохранит возможность передачи данных на верхний уровень сети. Такая конфигурация стека возможна не во всех моделях оборудования, поэтому выбор моделей коммутаторов должен учитывать требования к системе передачи данных и позволять создать необходимые конфигурации.

Построение отказоустойчивой сети на основе протоколов третьего уровня

Основным используемым на практике вариантом создания отказоустойчивой конфигурации сети на сегодня являются решения, основанные на применении протоколов автоматической маршрутизации. Хотя протоколы маршрутизации имеют несколько худшие показатели времени перестроения сети (например, OSPF может перестроить сеть приблизительно за 3 секунды), однако трудоемкость настройки структуры сети существенно ниже, чем при использовании, например, протокола второго уровня MSTP.

С точки зрения протоколов маршрутизации, сеть с резервными каналами связи представляет собой отдельные подсети с несколькими возможными путями передачи данных из одной подсети в другую. В большинстве случаев администратору достаточно только включить протоколы автоматической маршрутизации, чтобы сеть "заработала". Причем переключение на другие пути передачи данных в случае повреждения каналов связи будет происходить за счет изменения таблиц маршрутизации.

VRRP

При маршрутизации между несколькими VLAN в качестве шлюза по умолчанию для рабочих станций используется адрес интерфейса коммутатора. Это является узким местом такого решения, поскольку в случае выхода из строя коммутатора со шлюзом компьютеры потеряют связь с другими сетями.

Для предупреждения подобных ситуаций необходимо использовать протокол VRRP (Virtual Routing Reduntance Protocol).

Примечание

Этот протокол реализован далеко не на всех моделях коммутаторов. Как правило, модели, приобретаемые малыми организациями, не имеют поддержки данного протокола.

Идея создания отказоустойчивого шлюза с использованием протокола VRRP состоит в следующем. В сети устанавливаются два коммутатора с поддержкой данного протокола. На каждом из них настраиваются сетевые интерфейсы и включается протокол VRRP. После этого производится настройка интерфейса с одним и тем же IP-адресом на *обоих* коммутаторах, причем один коммутатор определяется главным, а второй — ведомым. В нормальных условиях работы коммутаторы постоянно обмениваются между собой служебной информацией. Если они оба нормально работают, то по настроенному адресу шлюза "отвечает" только главный коммутатор. Если он выходит из строя, то второй коммутатор начинает принимать данные по адресу шлюза и передавать их в другие сети в соответствии с настройками.

Таким образом обеспечивается отказоустойчивая работа шлюза, не зависящая от состояния отдельного коммутатора или целостности связей.

Протокол VRRP является стандартом. В то же время существуют отдельные модификации его реализации на коммутаторах различных вендоров. Так, из описанного принципа работы VRRP следует, что в "нормальных условиях" передачу данных в другую сеть обеспечивает только главный коммутатор. Хотя физические связи в целях обеспечения отказоустойчивости имеют оба устройства. Поэтому, например, в коммутаторах Nortel реализовано расширение функциональности протокола VRRP. Оба коммутатора будут работать в качестве шлюза[1] и передавать данные в другие сети. Однако если один из них выйдет из строя, его трафик будет перенаправен в другой коммутатор. Этим достигается балансировка нагрузки на различные каналы связи и увеличение пропускной способности сети.

Время восстановления структуры сети

Добиться малого времени восстановления передачи данных после единичной аварии очень сложно. На основе использования открытых стандартов реально достичь восстановления обслуживания за период не более 3—5 секунд.

Использование проприетарных технологий может сократить данный период до менее чем одной секунды. Однако к подобным прогнозам следует относиться крайне осторожно: часто даже крупные вендоры в маркетинговых целях презентуют крайне низкие значения периода восстановления (например, 20 мсек), не делая акцента на тех условиях, при которых получен такой показатель. Если отказ внутри шассийного коммутатора может быть парирован за

[1] Мы не будет останавливаться подробно на реализации такой технологии. При ее использовании к одному IP-адресу шлюза привязываются два MAC-адреса: один для клиентов первого коммутатора, другой — для клиентов второго. В результате пакеты, переданные на один шлюз (один IP-адрес), достигают различных устройств.

данную величину, но на восстановление после другой неисправности требуется несколько секунд, то сеть в целом будет характеризоваться именно наихудшим показателем.

Что можно посоветовать администраторам? В первую очередь, больше проверять, чем доверять маркетинговым предложениям. Изучать базовые документы по используемым технологиям, читать технические описания оборудования, обращая внимания на любые оговариваемые особенности. Во-вторых, стараться быть в курсе тестов, проводимых независимыми лабораториями, такими как Tolly Group (**http://www.tolly.com/**), обращая при этом внимание на условия проведения теста.

В-третьих, просчитывать необходимые параметры для конфигурации именно вашей сети. Каждая конфигурация индивидуальна, и не факт, что лучшее решение для идеальной лаборатории окажется таковым в реальной ситуации.

Качество обслуживания в сетях предприятия

Тестирование каналов связи

Качество информационной системы начинается с качества комплектующих, использованных при построении сети. Несмотря на доступность инструментов для расшивки кабеля и монтажа элементов СКС, желательно привлечь к работам фирмы, имеющие опыт работы на этом рынке и обладающие необходимым уровнем компетенции. Например, даже такая мелочь, как лишний перехлест пары проводников при расшивании гигабитного соединения, может привести к тому, что ссылка по своим параметрам не будет соответствовать заданной категории.

Все линии связи должны быть протестированы сертифицированным оборудованием. Это позволит не только выявить ошибки, но и обнаружить ухудшение параметров линии, которое может привести к отказам только после некоторого периода эксплуатации. Наличие подобных тестов позволит быть уверенным в качестве построенной СКС, в том, что линия будет надежно работать как на момент создания, так и через несколько лет эксплуатации.

На рис. 3.7 в качестве примера представлен результат тестирования одной линии связи на соответствие требованиям категории 5e. Линия не прошла тест, поскольку в ней было перепутано подключение проводников. Подобные тесты должны быть проведены для всей кабельной системы, а их результаты — храниться в архиве администратора.

LINKWARE
CABLE TEST MANAGEMENT SOFTWARE

X

ID кабеля: R530-PP14-P07

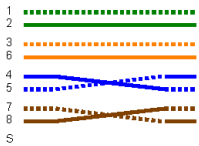
Суммарный результат: FAIL

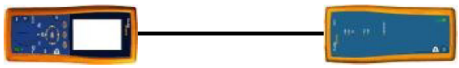
Дата / Время: 12/28/2006 01:16:10pm
Запас: 7.2 dB (NEXT 12-78)
Врем. предел: ISO11801 PL max Class D
Тип кабеля: Cat 5e UTP

Оператор: [illegible]
Версия программы: 1.3000
Версия лимитов: 1.0200
NVP: 67.0%

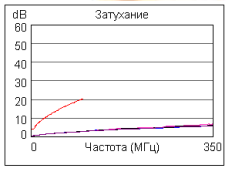
Модель: DTX-1800
Сер. номер гл. модуля: 8789145
Сер. номер удал модуля: 8789146
Главный модуль: DTX-PLA001
Удаленный модуль: DTX-CHA001

Карта проводов (T568A)
FAIL

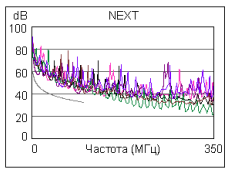


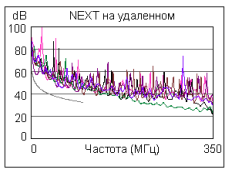


Длина (фт)	[Пара 36]	42
Обосн. задержка (ns), Лимит 498	[Пара 12]	65
Разн. задержок (ns), Лимит 44	[Пара 12]	1
Сопротивл. (ом), Лимит 21.0	[Пара 36]	2.7
Затухание Разница (dB)	[Пара 45]	17.5
Частота (МГц)	[Пара 45]	100.0
предел (dB)	[Пара 45]	20.4

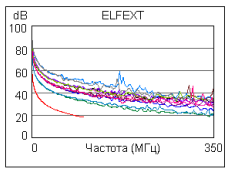


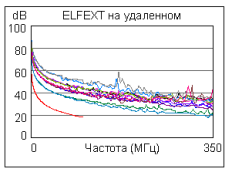
	Наихудш. разн		Наихудш. знач	
Неверн	Глав.	SR	Глав.	SR
Наихудш пара	12-78	36-78	12-78	36-78
NEXT (dB)	7.2	7.4	7.2	7.4
Част. (МГц)	88.8	100.0	88.8	100.0
предел (dB)	33.2	32.3	33.2	32.3
Наихудш пара	12	78	78	36
PSNEXT (dB)	8.2	8.7	8.3	9.3
Част. (МГц)	87.5	90.8	90.3	100.0
предел (dB)	30.3	30.0	30.0	29.3



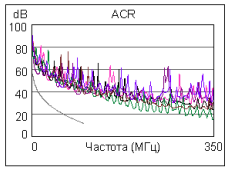


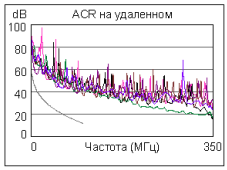
PASS	Глав.	SR	Глав.	SR
Наихудш пара	36-45	45-36	36-45	45-36
ELFEXT (dB)	13.7	13.6	14.2	13.6
Част. (МГц)	89.8	89.8	97.8	90.3
предел (dB)	19.6	19.6	18.8	19.5
Наихудш пара	36	36	36	36
PSELFEXT (dB)	15.9	15.5	16.6	15.9
Част. (МГц)	2.5	88.8	100.0	97.8
предел (dB)	47.7	16.7	15.6	15.8



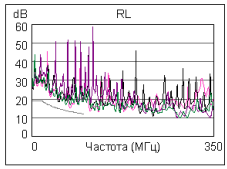


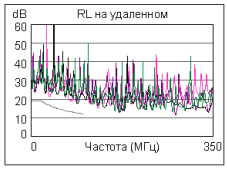
Неверн	Глав.	SR	Глав.	SR
Наихудш пара	12-78	12-78	12-78	36-78
ACR (dB)	13.9	13.3	23.8	25.1
Част. (МГц)	6.9	7.4	88.8	100.0
предел (dB)	46.0	45.4	14.0	11.9
Наихудш пара	12	78	36	36
PSACR (dB)	15.6	15.1	26.8	26.9
Част. (МГц)	6.6	7.4	100.0	100.0
предел (dB)	43.4	42.4	8.9	8.9





Неверн	Глав.	SR	Глав.	SR
Наихудш пара	12	45	12	36
RL (dB)	1.6	4.5	1.6	5.0
Част. (МГц)	73.3	7.8	73.5	89.3
предел (dB)	13.4	19.0	13.3	12.5





FLUKE networks

Рис. 3.7. Протокол испытания качества линии связи специализированным оборудованием

Приоритезация трафика

Построить сеть, которая гарантированно пропускала бы весь трафик в случае активной сетевой работы всех пользователей, практически нереально. Параметры пропускной способности рассчитываются по неким усредненным показателям с учетом предположений о характере использования сети (типы задач, наличие голосового и мультимедийного трафика и т. п.).

В большинстве сетей малых и средних предприятий пропускная способность сети используется менее чем на 10%, и ограничения в передаче данных из-за исчерпания полосы пропускания кажутся маловероятными. Но все каналы связи имеют свои пределы. С увеличением интенсивности использования сетевых приложений вероятность кратковременной перегрузки сети будет только повышаться.

Сама сеть *не гарантирует* доставку информации. Если пакет с данными не может быть передан, он удаляется и, естественно, теряется. Большинство приложений корректно обработает факты потери части передаваемых данных и запросит их повторно. Однако есть задачи, для которых любая потеря пакетов недопустима. Например, при передаче голоса подобная ситуация приведет к возникновению "провалов". В этом случае можно решить проблему, если предоставить передаче голоса более привилегированные условия, чем, например, протоколу пересылки почтовых сообщений.

Задача приоритезации трафика решается путем присвоения передаваемым по сети пакетам определенного *класса* обслуживания и обеспечения для них соответствующего *качества* обслуживания. Часто для простоты все эти технологии называют QoS — Quality of Service[1]. В общем случае данная задача является весьма сложной[2] и решается по-разному для локальной и магистральных сетей. Мы опишем основные подходы, используемые для ее решения.

Варианты приоритезации: QoS, ToS, DiffServ

Существует несколько возможностей определения необходимого качества обслуживания. На уровне кадров Ethernet (второй уровень модели OSI) существует возможность включения поля TAG, значение которого определяет требуемый уровень обслуживания. Поскольку протокол IP работает не только в сетях Ethernet, но и в сетях WAN, которые не обязательно основаны на кадре Ethernet, то и в IP-пакете было предусмотрено специальное поле ToS, при-

---

[1] Обращаю внимание читателя, что настраивать QoS имеет смысл только при возникновении подобных ситуаций. В случае достаточности полосы пропускания никаких дополнительных действий предпринимать не нужно.

[2] Подумайте хотя бы над теми параметрами, которые нужно обеспечить для качественной передачи данных. Это может быть и гарантия полосы пропускания, и отсутствие задержек пакетов более определенной величины, и максимально допустимый процент потери пакетов. Разные задачи будут определять отличающиеся требования.

нимающее данные о требуемом уровне обслуживания. Впоследствии был разработан новый протокол Differtiated Services (DS или DiffServ), который и используется в настоящее время для маркировки IP-пакетов в соответствии с уровнем обслуживания.

Коммутаторы, используемые на малых и средних предприятиях, а также коммутаторы уровня доступа в больших сетях обычно используют для приоритезации только поле QoS Ethernet-кадра. Коммутаторы уровня предприятия могут приоритезировать трафик с учетом всех действующих стандартов. Так, на рис. 3.8 показано окно настройки параметров качества обслуживания коммутатора фирмы Nortel, в котором можно "подстроить" метки DSCP к значениям приоритетов 802.1p.

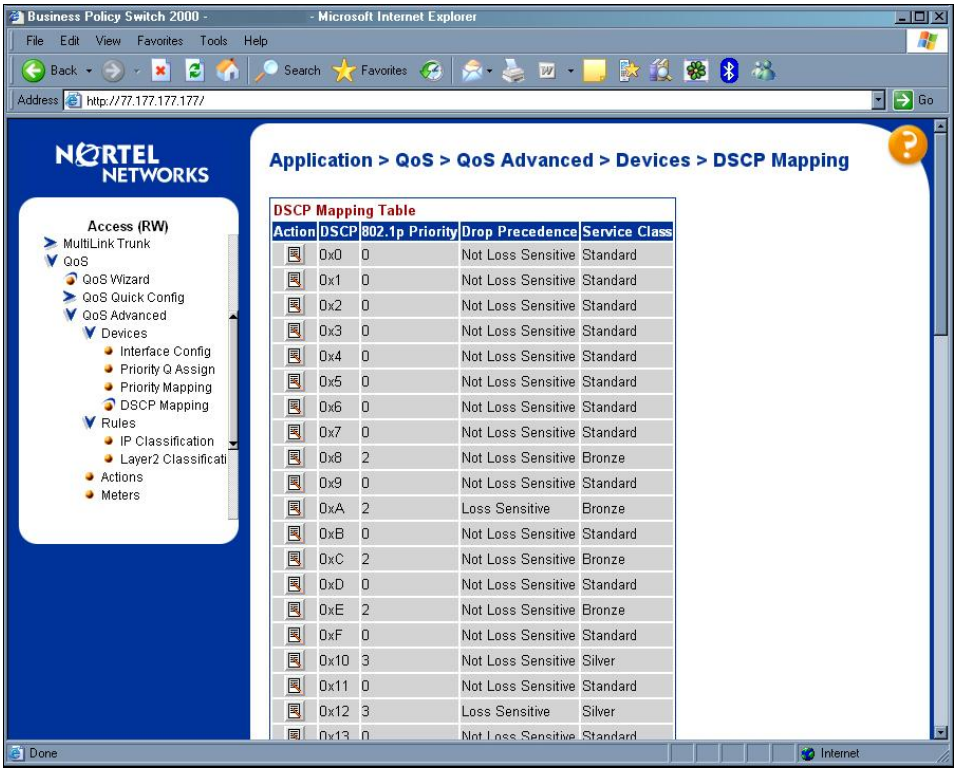


Рис. 3.8. Скриншот окна управления коммутатора фирмы Nortel

Пакеты данных в соответствии с протоколом 802.1p[1] имеют специальное поле приоритета из трех битов. Таким образом, данные в локальной сети могут

[1] Точнее, само поле определено в протоколе 802.1q, но назначение битов приоритета описано в протоколе 802.1p.

быть промаркированы одним из восьми *классов* обслуживания. Приоритет пакету должна "ставить" программа, создающая данный трафик, но его значение может быть изменено по пути следования (например, на некоторых моделях коммутаторов[1]).

В DiffServ на описание приоритета выделено 6 бит, что позволяет иметь до 64 возможных классификаций приоритезации. Реально используется существенно меньше уровней сервиса. В табл. 3.3 приведены основные применяемые на практике уровни сервиса DiffServ.

Таблица 3.3. *Часто используемые на практике уровни сервиса DiffServ*

Класс	**PHB (Per Hop Behavior)**	**Описание**	**Область применения**
Default		—	
Class-Selector		Используется для обратной совместимости с ToS	
Expedited Forwarding (EF)	EF	Используется при необходимости минимизации варьирующихся задержек и потери пакетов. Предполагает гарантированную полосу пропускания	Передача голоса
Assured Forwarding (AF)	AF11 High Priority Low Drop Precedence	Рекомендован для особо важных приложений	Сетевые службы, программы управления производством (SAP и т. п.)
	AF21 Medium Priority Low Drop Precedence		Службы обеспечения безопасности
	AF22 Medium Priority Medium Drop Precedence		Сообщений электронной почты
	AF22 Medium Priority High Drop Precedence		Фоновая репликация данных
	AF31 Low Priority Low Drop Precedence		HTTP

[1] Существуют и различные программы, позволяющие менять параметры качества обслуживания и назначать данным желаемые классы (приоритеты). Так, в состав пакета Resource Kit для сервера Windows входит программа Traffic Control, позволяющая назначать классы обслуживания на основе собственных фильтров и переопределять параметры качества обслуживания.

Классификация, маркировка, приоритезация

Для настройки приоритезации трафика необходимо выполнить несколько шагов. Во-первых, следует создать правила, по которым можно выделить часть трафика, требующую особых условий при передаче. Этот процесс называется *классификацией*. Например, вы хотите предоставить льготные условия для передачи данных какому-то приложению. Если оно работает по какому-либо протоколу, не используемому другими приложениями, то достаточно создать правило классификации на основе протокола. Можно определить правило, которое будет выделять трафик, отправленный устройством А устройству Б с 8 часов утра до 12 часов дня каждый понедельник (возможности классификации зависят, в первую очередь, от используемого оборудования) и т. д.

После того как данные классифицированы, передаваемый пакет следует *маркировать*. Поскольку по стандарту Ethernet реально существует восемь приоритетов, то вам необходимо составить правила, которые поставят в соответствие различные типы трафика существующим уровням[1]. Промаркированный пакет готов к применению правил приоритезации.

Классификацию с последующей маркировкой пакетов можно проводить на любом коммутаторе, поддерживающем управление приоритезацией. В том числе допускается и выполнение *перемаркировки* трафика, т. е. повторного назначения приоритетов на основании других правил. Однако более рационален иной подход: маркировку трафика следует выполнять там, где такой трафик *создается*, иными словами — на коммутаторах уровня доступа. Коммутаторы уровня распределения и ядра используют уже назначенную маркировку и производят на основании ее приоритезацию трафика по заданным на них правилам. Это оптимизирует нагрузку на активное оборудование сети, разгружая центральные коммутаторы от дополнительной работы по анализу трафика.

После того как выполнены классификация и маркировка, необходимо применить *правила приоретизации*. Стандарт предусматривает восемь уровней приоритета, но не описывает правила, которые могут быть применены к каждому из них. В этом отношении имеются только общие рекомендации, поэтому вам придется сформировать правила приоритезации самостоятельно. Например, вы можете создать правило, которое будет блокировать весь трафик, соответствующий определенному классу.

Реально процессы обеспечения различного уровня качества передачи реализуются путем направления пакетов на различные очереди в коммутаторе.

---

[1] Часто в целях удешевления модели коммутаторы, предназначенные для использования на уровне доступа, имеют меньше 8 очередей, используемых при приоритезации трафика. Соответственно сузятся ваши возможности по детализации процесса приоритезации.

Как работает приоритезация: очереди

Процесс приоретизированной передачи пакетов реализуется следующим образом. На коммутаторе создаются буферы для временного хранения пакетов на каждом порте. Их принято называть *очередью*.

Количество буферов — это количество очередей, которые поддерживает коммутатор. В идеале количество очередей должно быть равно количеству уровней приоритезации, а именно восьми. Меньшее их количество не позволит использовать все возможности протокола, большее — не имеет смысла за пределами данного коммутатора, хотя и позволяет более точно приоритезировать передачу трафика в конкретном коммутаторе. Размеры буфера обычно не одинаковы для разных очередей: чем выше приоритет очереди, тем больше памяти отводится для хранения ее пакетов[1].

Если канал связи свободен, то пакет данных сразу же передается по назначению. Если такой возможности нет, то коммутатор помещает пакет на временное хранение в очередь, определяемую по заданным правилам. Как только линия связи освободится, коммутатор начнет передачу пакетов из очередей. Существует несколько алгоритмов передачи данных (администратор может выбирать алгоритмы и настраивать их параметры). Наиболее популярны два алгоритма: Strict Priority Queuing (SPQ) и Weighted Round Robin (WRR).

При использовании SPQ сначала передаются пакеты из очереди, имеющей максимальный приоритет, и только когда она полностью освободится, коммутатор начнет передачу данных из следующей по приоритету. Данный алгоритм обеспечивает практически гарантированную доставку пакетов максимального приоритета, однако при существенном объеме высокоприоритетной информации другие пакеты могут теряться (коммутатор вообще не сможет приступить к обслуживанию очереди с низким приоритетом).

Алгоритм WRR использует специальные взвешенные процедуры для отправки пакетов. Каждой очереди выделяется определенный лимит для передачи: чем выше приоритет очереди, тем больше пакетов из нее передается, но в любом случае будут опрошены все очереди в порядке снижения приоритета: после истечения выделенного периода обслуживания одной очереди коммутатор перейдет к обработке пакетов очереди, следующей по приоритету. Данный алгоритм обеспечивает передачу *всех* типов пакетов.

Иногда используют смешанные алгоритмы. Например, самые критичные очереди (обычно имеющие приоритет 1 или 2) обслуживают на основе алгоритма SPQ, а для всех остальных применяют вариант WRR.

---

[1] Качество коммутатора определяется в том числе и объемом памяти, выделяемой для очередей: более дорогие модели имеют большие размеры буферов. Обычно расширенными настройками коммутатора можно распределять выделенную память между очередями по собственным критериям, однако на практике эти параметры по умолчанию обычно не изменяют.

Ограничение полосы пропускания трафика (Traffic shaping)

Коммутаторы, на которых реализована возможность приоритезации трафика, часто имеют возможность ограничивать полосу пропускания для того или иного типа данных. Например, можно ограничить выделяемую полосу для загрузки данных по протоколу FTP или для протоколов видеопросмотра в рабочее время значением, обеспечивающим достаточный свободный объем для основных производственных приложений.

Данная настрйка выполняется в соответствии с правилами конфигурирования конкретной модели коммутатора.

Беспроводные сети

Выполнение полного цикла работ по проектированию и монтажу СКС является весьма затратной операцией. Стоимость проектирования, стоимость самих материалов, оплата монтажных работ — эти расходы могут составить весьма значительную сумму. Даже в небольших организациях для создания сети необходимо приобрести несколько сотен метров кабеля. Для средних и крупных организаций счет уже ведется на тонны "меди". Кроме того, достаточно велики стоимости розеток, каналов и других элементов. При этом в силу большой трудоемкости в проекты обычно закладываются необходимые резервы, рабочие места, которые только могут быть созданы в перспективе, и т. п.

Для небольших офисов существует решение, которое уже сейчас успешно конкурирует с существующими кабельными сетями — *беспроводные линии связи*.

Для создания такой сети каждый компьютер должен быть оборудован беспроводным адаптером, а в офисе необходимо установить специальные устройства — так называемые *точки доступа*, выполняющие, кроме того, роль хабов сети.

В настоящее время большая часть ноутбуков комплектуется устройствами доступа к беспроводной сети, а стоимость адаптера, устанавливаемого в "обычный" компьютер, сравнима со стоимостью стандартной сетевой платы. Если учесть, что стоимость точки доступа аналогична стоимости небольшого коммутатора, то переход на беспроводную сеть может быть экономически оправдан для многих организаций, а в некоторых случаях (например, аренда помещения без права выполнения монтажно-строительных работ, наличие мобильных сотрудников[1]) использование беспроводной сети может стать и единственным приемлемым решением.

[1] Например, официанты могут использовать мобильные компьютеры для приема заказов, врачи иметь с собой ноутбуки при проведении обхода и т. д.

Стандарты беспроводной сети

В настоящее время устройства для беспроводной сети выпускаются на основе нескольких стандартов, некоторые параметры которых приведены в табл. 3.4.

Таблица 3.4. *Некоторые параметры стандартов беспроводной сети*

Параметр	Стандарт		
	802.11a	**802.11b**	**802.11g**
Диапазон частот, ГГц	5	2,4	2,4
Число каналов	8	3	3
Максимальная скорость передачи, Мбит/сек	54	11	54 (108 с аппаратным сжатием)
Совместимость		802.11.g	802.11.b

На практике лучше выбрать один стандарт беспроводного оборудования, а при необходимости использования совместимых режимов — проверять наличие сертификации соответствующего решения.

Проектирование беспроводной сети предприятия

С помощью беспроводных технологий можно соединять компьютеры (по принципу "точка — точка"), отдельные сегменты сетей и т. п. Наиболее часто в локальных сетях устройства беспроводного доступа ставятся в качестве *точки доступа* (Wireless Access Point, AP). В этом случае персональные компьютеры подключаются к точкам доступа, через которые осуществляют доступ как в локальную сеть организации, так и в Интернет, при этом точка доступа выступает аналогом концентратора локальной сети.

После выбора стандарта беспроводной сети следует определить *зоны покрытия*. Одно стандартное устройство AP "покрывает" в помещении зону радиусом около 75—100 м. Хотя существуют различные оценки для расчетов диаграмм зон покрытия, эти величины существенно зависят от конкретных условий: планировки помещений, материала стен и т. п. Лучшим способом является проведение тестовых измерений на местности с использованием соответствующего оборудования. Как правило, это весьма дорогостоящая операция, поэтому часто ограничиваются тестированием уровня сигнала встроенными средствами беспроводного адаптера (штатными средствами Windows XP). При этом следует учесть, что существующее на предприятии оборудование при своей работе может создать помехи беспроводной сети, и предусмотреть необходимые технологические резервы. И даже при отсутствии по-

стоянных помех используемые в беспроводной сети программы должны быть устойчивы к кратковременному исчезновению связи[1].

На количество устанавливаемых точек доступа будут влиять также требования к скорости передачи данных. Указанные в табл. 3.4 значения скорости передачи данных являются максимальными, а полоса пропускания *делится* между всеми устройствами, которые подключены к данному каналу. Также следует учитывать, что скорость передачи данных снижается на максимальных расстояниях при слабом уровне сигнала. Установка дополнительных точек доступа позволит распределить между ними пользователей[2] и повысить

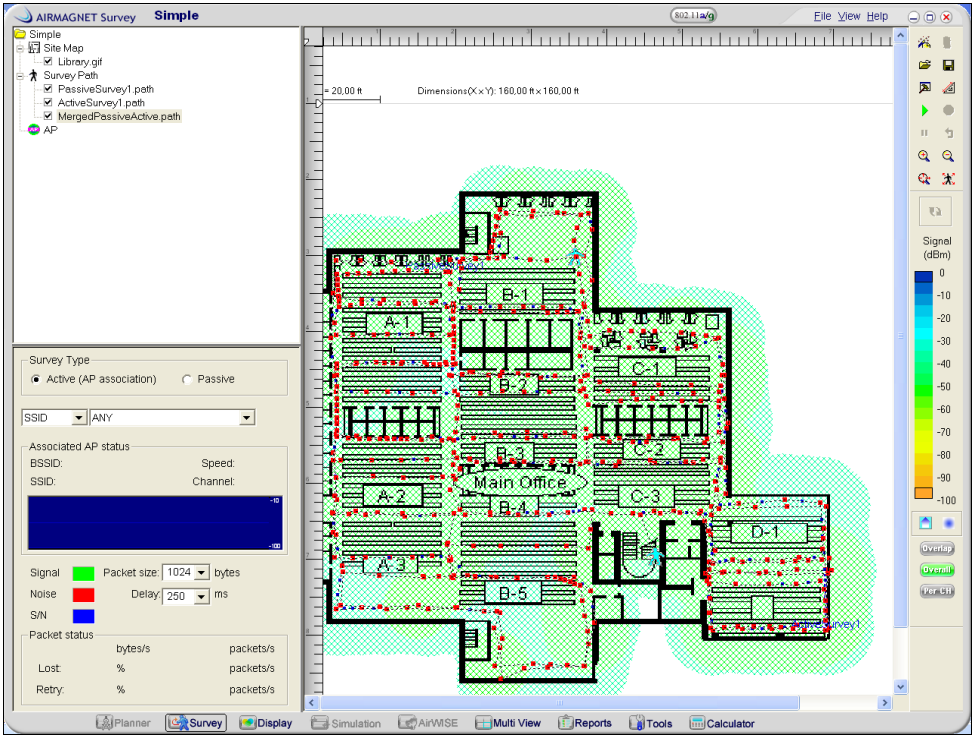


Рис. 3.9. Проектирование установки беспроводных точек доступа.
Для обеспечения работы в любой точке здания в беспроводной сети необходимо учесть многие факторы. Специализированное программное обеспечение позволяет построить возможные зоны покрытия на основе замеров и анализа параметров радиосигнала.
На рисунке представлен пример от AirMagnet, Inc.

[1] Например, при работе в 1С могут наблюдаться случаи аварийного завершения программы из-за кратковременной потери связи с сервером.

[2] В связи с этим обычно рекомендуется устанавливать одну точку доступа приблизительно на 10 клиентов, хотя технический предел подключений беспроводных устройств, как правило, составляет не одну сотню систем.

скорость обмена данными. Поскольку правильное расположение точек доступа требует учета многих факторов, на практике беспроводные сети часто проектируются на основе анализа замеров параметров радиочастотного сигнала в реальных условиях (рис. 3.9).

Если нужно спроектировать связь между двумя зданиями, то следует использовать специализированные беспроводные *мосты* и, возможно, направленные антенны.

Примечание

Если режим работы системы предполагает мобильность устройств (перемещение их во время работы с системой с переключением между различными точками доступа), то такое решение требует использования специального программного обеспечения.

Безопасность беспроводной сети

Точку доступа можно сравнить с концентратором локальной сети, который поставлен в общедоступное помещение. Любой может "подключиться" к данному сегменту и прослушивать передаваемую информацию. Поэтому правильной настройке подключения клиентов необходимо уделить особое внимание.

Шифрование трафика беспроводной сети

Для защиты передаваемой по беспроводной сети информации все данные *шифруются*. Исторически первый стандарт безопасности для Wi-Fi — WEP (Wired Equivalent Privacy) — предусматривает шифрование с помощью статичного ключа, известного как пользователю, так и администратору точки доступа. К сожалению, в практической реализации этого документа были найдены ошибки, которые позволяют за короткое время (порядка нескольких часов) вычислить данный ключ. Поэтому протоколы WEP, даже с увеличенной длиной ключа, не могут считаться безопасными при создании корпоративной беспроводной сети.

Примечание

Если примененные при создании беспроводной сети устройства не поддерживают новых протоколов безопасности, то администраторы могут защитить передаваемую информацию путем создания виртуальных частных сетей (VPN).

Новый стандарт безопасности WPA (Wi-Fi Protected Access) предусматривает как использование динамических (изменяемых) ключей шифрования, так и аутентификацию пользователя при входе в беспроводную сеть. Проектируя беспроводной сегмент сети, следует приобретать только устройства, удовлетворяющие данному стандарту.

Аутентификация пользователей и устройств Wi-Fi

В беспроводных сетях применяются два способа проверки пользователей и устройств при их подключении. Первый — это проверка MAC-адресов устройств, подключаемых к данной точке доступа. В этом случае администратор вручную должен настроить для *каждой* точки доступа соответствующий список MAC-адресов устройств, которым разрешено беспроводное подключение.

Способ не может считаться безопасным, поскольку MAC-адреса легко определяются при прослушивании беспроводного сегмента, а "подмена" MAC-адреса не представляет никакой сложности даже для не совсем опытного пользователя.

Второй способ основан на протоколе двухточечного соединения с надежной аутентификацией — EAP (Extensible Authentication Protocol). Для предприятий следует рекомендовать аутентификацию на основе стандарта 802.1x с использованием сервера RADIUS.

Наиболее безопасен способ, при котором для аутентификации вместо паролей используются сертификаты. Однако он требует наличия на предприятии настроенной системы PKI *(см. главу 12)*. Настройка беспроводных устройств для аутентификации с использованием сертификатов по протоколу 802.1x

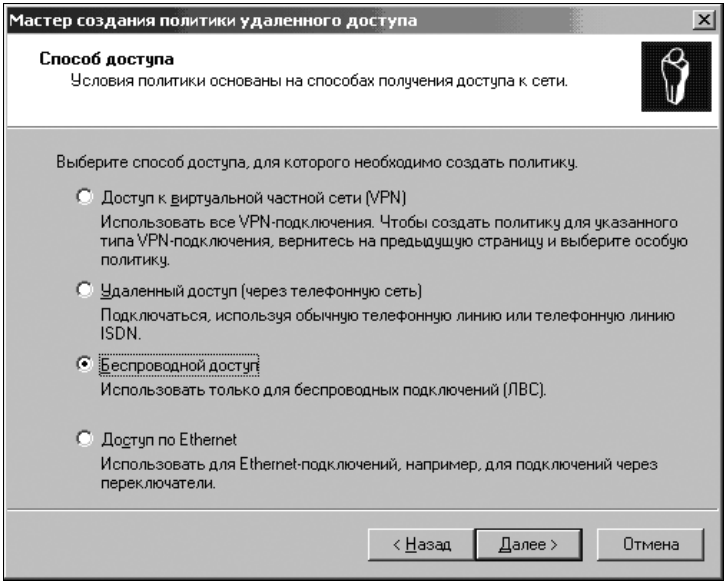


Рис. 3.10. Создание политики RADIUS-сервера для беспроводной сети. При создании политики удаленного доступа для сервера RADIUS должен быть выбран шаблон **Беспроводной доступ**

практически идентична примеру, описанному в *главе 9* в *разд. "Настройка протокола 802.1x"*. Единственное отличие заключается в выборе шаблона политики, используемой на сервере RADIUS (рис. 3.10).

Примечание

При такой настройке клиенты, ранее не работавшие в составе домена, не могут быть подключены к нему по беспроводной сети, поскольку на них не установлены необходимые сертификаты. Вам следует либо заранее осуществить подсоединение компьютера к домену с помощью проводной сети, либо настроить особую политику для временного подключения гостевых записей (введя в этом случае временные ограничения сессии в политике подключения сервера RADIUS). При краткосрочном подключении к сети клиент получит сертификат и в дальнейшем будет работать в соответствии с постоянной политикой беспроводного доступа.

Безопасность клиента

При подключении компьютера к публичной беспроводной сети следует принимать те же меры безопасности, что и при работе в Интернете. Прежде всего

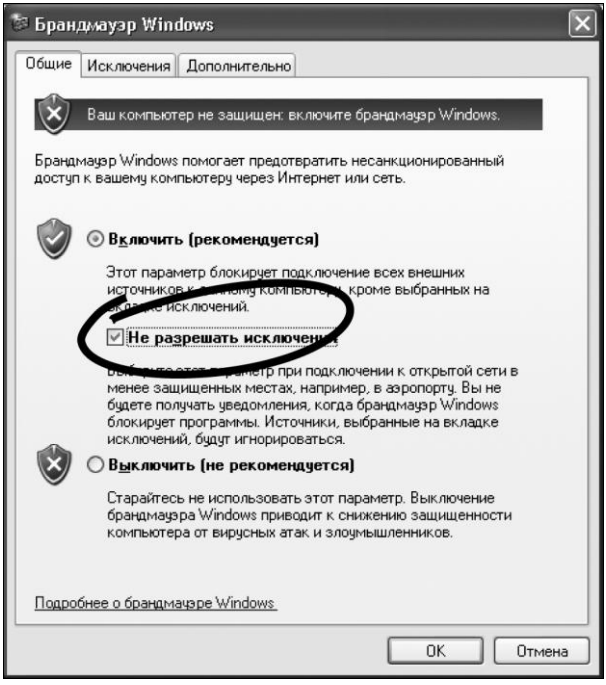


Рис. 3.11. Настройка брандмауэра Windows XP SP2.
В межсетевом экране Windows XP имеются так называемые исключения, предназначенные для работы в локальной доверенной сети, которые позволяют подключиться к защищенному компьютеру извне. Не нужно забывать, что в публичных сетях допущенные по умолчанию исключения должны быть *запрещены* (выделено на рисунке)

следует обязательно защитить подключение брандмауэром (например, встроенный брандмауэр Windows XP — опция **Защитить подключение к Интернету** в свойствах беспроводного подключения). Этим вы блокируете доступ к данным, хранимым на локальном компьютере, из внешней сети.

Включение этой опции обеспечивает защиту системы Windows XP с первым сервис-паком. На компьютерах с Windows XP при установленном втором сервис-паке необходимо *в обязательном порядке* запретить допущенные разработчиком по умолчанию разрешения доступа к компьютеру извне (осуществляется через настройку брандмауэра отключением исключений, рис. 3.11).

Терминология компьютерной сети

Протоколы

Сетевой протокол — это набор программно реализованных правил общения компьютеров, подключенных к сети. Практически это "язык", на котором компьютеры разговаривают друг с другом. В настоящее время стандартом стало использование *только* протокола TCP/IP. В предыдущих версиях Windows по умолчанию устанавливалось несколько протоколов, обычно это NetBEUI, NWLink IPX/SPX, TCP/IP.

- **NetBEUI.**

  Компактный и эффективный протокол для взаимодействия в малых сетях (до 200 компьютеров). Используется в самых разнообразных системах: Microsoft LAN Manager, Windows 3.1/3.11 for Workgroups/95/98/NT 4.0, IBM PCLAN, LAN Server и т. п. В Windows 2000 и старше применяется новая спецификация этого протокола, которая получила название NetBIOS Frame Protocol (NBFP). NetBEUI (NBFP) не требует никаких дополнительных настроек. Если нужно быстро создать сеть и вы не чувствуете себя уверенными в понимании дополнительных настроек, которых, например, требует протокол TCP/IP, то включите протокол NBFP. Вы получите простую и весьма быстро функционирующую локальную сеть.

- **NWLink IPX/SPX.**

  Если в сети есть серверы Novell NetWare[1], то этот протокол необходим для организации с ними связи. В противном случае данный протокол следует исключить из числа используемых в системе.

- **TCP/IP.**

  Основной рекомендуемый протокол как для больших сетей предприятий и малых офисов, так и для соединения домашних компьютеров в частную

[1] В последних версиях Netware по умолчанию используется протокол TCP/IP.

сеть. В отличие от других протоколов требует ряда предварительных настроек.

Примечание

Не следует использовать в сети больше служб и протоколов, чем требуется для нормальной работы в конкретной ситуации. Во-первых, при этом будут непроизводительно использоваться ресурсы компьютера. Во-вторых, любая дополнительная служба и неиспользуемый протокол — это еще один "вход" в систему, который надо защищать. Поэтому проще не предоставлять дополнительных возможностей хакерам, чем постоянно следить за обнаруживаемыми в этих службах уязвимостями, устанавливать необходимые обновления и т. п.

Модель OSI

С целью систематизации часто используется *модель OSI*, условно разбивающая сетевое взаимодействие на семь уровней (табл. 3.5).

Знание уровней OSI обычно требуется при сдаче тех или иных сертификационных экзаменов, но на практике такое деление потеряло свое значение. Если первые три уровня еще можно достаточно хорошо вычленить при анализе того или иного сетевого проекта, то классифицировать функциональность оборудования по остальным уровням достаточно сложно. В маркетинговых целях часто указывают в описаниях коммутаторов, что они работают, например, на уровне 4 или 7. На практике это означает только, что при реализации определенного функционала в коммутаторах производится анализ пакета данных по характеристикам, относящимся к соответствующим уровням. Например, это происходит при операциях маршрутизации группового трафика (коммутатор анализирует пакет на принадлежность той или иной программе), приоритезации пакетов и т. п.

Таблица 3.5. *Модель OSI*

Уровень OSI	Назначение	Примеры	Необходимое сетевое оборудование
Application (7)	Обеспечение служб сетевых приложений	Протоколы SMTP, HTTP, FTP и т. п.	
Presentation (6)	Службы кодирования и преобразования данных, используемых на уровне приложений	Стандарты кодирования изображений (GIF, JPEG, TIFF и т. п.), аудио и видео (MPEG) и т. п.	
Session (5)	Обеспечение коммуникаций между приложениями более высокого уровня (согласование, поддержка, завершение сессий)	Session Control Protocol (SPC) Remote Procedure Call Zone Information Protocol (AppleTalk)	

Таблица 3.5 *(окончание)*

Уровень OSI	Назначение	Примеры	Необходимое сетевое оборудование
Transport (4)	Обеспечивает передачу данных от одной точки до другой	TCP (используются соединения) UDP (передача данных без создания соединения)	
Network (3)	Обеспечивает логическую структуру сети (сетевые адреса)	IP	Маршрутизаторы Маршрутизирующие коммутаторы
Data Link (2)	Обеспечивает передачу данных по тем или иным *физическим* каналам связи	Ethernet Token Ring FDDI Point-to-Point Protocol Frame Relay	Коммутаторы Мосты
Physical (1)	Определяет физические, механические, электрические и другие параметры физических каналов связи (напряжение, частота, максимальные длины участков и т. п.)	LAN категории 3 LAN категории 5 V.35	Концентраторы

Стек протоколов TCP/IP

Когда говорят о TCP/IP, то обычно подразумевают под этим именем множество различных протоколов, использующих в своей основе TCP/IP. Существует большое количество различных стандартов, которые определяют те или иные варианты взаимодействия в сети Интернет.

Так, есть правила, по которым осуществляется обмен сообщениями между почтовыми серверами, и есть правила, по которым конечные пользователи могут получать в свой ящик письма. Имеются правила для проведения широковещательных видео- и аудиотрансляций, правила для организации телефонных переговоров по Интернету. Существуют правила, которые определяют поведение участников передачи данных в случае возникновения ошибки и т. п.

Логично, что при разработке правил пересылки файла никто не создает новых механизмов пересылки единичного пакета данных и что протокол пересылки файлов основан на более простом протоколе передачи пакетов.

Поэтому принято говорить, что существуют уровни протокола IP, а на каждом уровне — различные варианты специальных протоколов. Весь этот набор протоколов называют *стеком протоколов TCP/IP*.

Протоколы UPD, TCP, ICMP

Для передачи данных используются протоколы TCP (Transmission Control Protocol, протокол управления передачей данных) и UDP (User Datagram Protocol, протокол пользовательских дейтаграмм). UDP применяется в тех случаях, когда не требуется подтверждения приема (например, DNS-запросы, IP-телефония). Передача данных по протоколу TCP предусматривает наличие подтверждений получения информации. Если передающая сторона не получит в установленные сроки необходимого подтверждения, то данные будут переданы повторно. Поэтому протокол TCP относят к протоколам, предусматривающим соединение (connection oriented), а UDP — нет (connection less).

Протокол Internet Control Message Protocol (ICMP, протокол управляющих сообщений Интернета) используется для передачи данных о параметрах сети. Он включает такие типы пакетов, как ping, destination unreachable, TTL exceeded и т. д.

IPv6

Бурное развитие Интернета привело к тому, что параметры, заложенные при создании протоколов IP, стали сдерживать дальнейшее развитие глобальной сети. Поэтому многочисленные группы постоянно разрабатывают возможные модификации данного протокола. Наиболее "признанной" на данный момент разработкой считается проект группы IETF (Internet Engineering Task Force, проблемная группа проектирования Интернета), который называют IPv6 (другие проекты объединяют общим названием IP Next Generation или IPng).

К основным особенностям данного проекта относятся:

- сохранение неизменными основных действующих принципов построения протокола IP;
- использование более длинных адресов (128-битные);
- применение встроенного 64-битного алгоритма шифрования;
- учет механизма резервирования пропускной способности протокола (ранее проблема решалась введением классов обслуживания);
- наличие больших возможностей дальнейшего расширения функций: строго описана только часть характеристик, остальные допускают дальнейшее развитие.

Хотя большинство участников Интернета поддерживает разработку этого протокола, однако реальное внедрение данной разработки потребует длительного времени и существенных инвестиций, поскольку влечет за собой модернизацию большого количества уже установленного оборудования.

Поддержка протокола IPv6 заложена в операционные системы Windows, начиная с Windows XP. Чтобы ее включить[1] в Windows XP, необходимо выполнить команду `ipv6 install`. Но использование `ipv6` пока еще не имеет практического значения. По разным оценкам нехватка адресного пространства протокола IPv4 может возникнуть не ранее чем через 5—10 лет. Это достаточный срок для разработки уже следующей спецификации протокола IP.

Параметры TCP/IP протокола

IP-адрес

Каждый компьютер, работающий по протоколу TCP/IP, обязательно имеет *IP-адрес* — 32-битное число, используемое для идентификации узла (компьютера) в сети. Адрес принято записывать десятичными значениями каждого октета этого числа с разделением полученных значений точками. Например: 192.168.101.36.

IP-адреса уникальны. Это значит, что каждый компьютер имеет свое сочетание цифр, и в сети не может быть двух компьютеров с одинаковыми адресами. IP-адреса распределяются централизованно. Интернет-провайдеры делают заявки в национальные центры в соответствии со своими потребностями. Полученные провайдерами диапазоны адресов распределяются далее между клиентами. Клиенты сами могут выступать в роли интернет-провайдера и распределять полученные IP-адреса между субклиентами и т. д. При таком способе распределения IP-адресов компьютерная система точно знает "расположение" компьютера, имеющего уникальный IP-адрес; ей достаточно переслать данные в сеть "владельца". Провайдер в свою очередь проанализирует пункт назначения и, зная, кому отдана эта часть адресов, отправит информацию следующему владельцу поддиапазона IP-адресов, пока данные не поступят на компьютер назначения.

Выделение диапазона адресов осуществляется бесплатно, но организация, получившая адреса, должна реально подтвердить их использование через определенный промежуток времени.

Для построения *локальных сетей* организаций выделены специальные диапазоны адресов. Это адреса 10.x.x.x, 192.168.x.x, 10.x.x.x, с 172.16.x.x по

[1] В Windows Vista IPv6 включен по умолчанию. Учитывая, что реализация данного протокола неизбежно несет в себе определенное количество ошибок, следует отключить IPv6 в случае его неиспользования.

172.31.x.x, 169.254.x.x[1]. Пакеты, передаваемые с указанных адресов, *не маршрутизируются* (иными словами, не пересылаются) через Интернет, поэтому в различных локальных сетях компьютеры могут иметь совпадающие адреса из указанных диапазонов. Для пересылки информации с таких компьютеров в Интернет и обратно используются специальные программы, "на лету" заменяющие локальные адреса реальными при работе с Интернетом. Иными словами, данные в Сеть пересылаются от реального IP-адреса. Этот процесс происходит "незаметно" для пользователя. Такая технология называется *трансляцией адресов* и более подробно описана в *главе 8*.

Групповые адреса

Если данные должны быть переданы на несколько устройств (например, просмотр видео с одной Web-камеры на различных компьютерах или одновременное разворачивание образа операционной системы на несколько систем), то уменьшить нагрузку на сеть может использование *групповых рассылок*.

Для этого компьютеру присваивается еще один IP-адрес из специального диапазона: с 224.0.0.0 по 239.255.255.255[2], причем диапазоны 224.0.0.0—224.0.0.255 и 239.0.0.0—239.255.255.255 не могут быть использованы в приложениях и предназначены для протоколов маршрутизации[3] и т. п. Назначение адресов групповой рассылки производится соответствующим программным обеспечением.

Если коммутатор имеет функции работы с групповыми рассылками (поддержка IGMP snoophing, PIM DM/PIM SM), то передаваемые на адреса групповой рассылки данные будут поступать только на те порты, к которым подключены устройства, подписавшиеся на соответствующие рассылки. В результате сетевой трафик может быть существенно снижен по сравнению с вариантом передачи таких данных каждому устройству сети независимо.

Распределение IP-адресов сети малого офиса

В сетях предприятий обычно задействованы диапазоны IP-адресов, выделенные для локального использования. Часть адресов закрепляется статически, часть — раздается динамически с помощью DHCP (Dynamic Host Configuration Protocol, динамический протокол конфигурации сервера).

---

[1] Под x подразумевается любое число от 0 до 254.

[2] Multicast-адрес присваивается динамически. Это делает соответствующая программа, использующая многоадресную рассылку.

[3] Например, адрес 224.0.0.1 принадлежит всем системам сегмента сети; адрес 224.0.0.2 — всем маршрутизаторам сегмента и т. д.

Статические адреса закрепляются:

- за шлюзом, для которого обычно используют адрес xxx.xxx.xxx.1, но это традиция, а не правило;
- за серверами DNS, DHCP, WINS;
- за контроллерами домена;
- за серверами сети (например, централизованные файловые ресурсы, почтовый сервер и т. п.);
- за станциями печати, имеющими непосредственное подключение к сети;
- за управляемыми сетевыми устройствами (например, сетевыми переключателями, SNMP-управляемыми источниками аварийного питания и т. п.).

Рабочие станции традиционно используют *динамические адреса*. При этом часть динамических адресов выдается для локального использования, а часть предназначается для внешних клиентов, "гостей" сети.

Примечание

Обычно для компьютеров, получающих гостевые адреса, устанавливаются определенные ограничения прав доступа к внутренним ресурсам.

Для упрощения администрирования сети рекомендуется выработать план распределения диапазона адресов и предусмотреть в нем некоторый запас для будущего развития информационной системы.

Маска адреса

Понятие *подсети* введено, чтобы можно было выделить часть IP-адресов одной организации, часть другой и т. д. Подсеть представляет собой диапазон IP-адресов, которые считаются принадлежащими одной локальной сети. При работе в локальной сети информация пересылается непосредственно получателю. Если данные предназначены компьютеру с IP-адресом, не принадлежащим локальной сети, то к ним применяются специальные правила для вычисления маршрута пересылки из одной сети в другую. Поэтому при использовании протокола TCP/IP важно знать, к какой сети принадлежит получатель информации: к локальной или удаленной.

Маска — это параметр, который "сообщает" программному обеспечению о том, сколько компьютеров объединено в данную группу ("подсеть"). Маска адреса имеет такую же структуру, как и сам IP-адрес: это набор из четырех групп чисел, каждое из которых может быть в диапазоне от 0 до 255. При этом чем меньше значение маски, тем больше компьютеров объединено в данную подсеть. Для сетей небольших предприятий маска обычно имеет вид 255.255.255.x (например, 255.255.255.224). Маска сети присваивается компьютеру одновременно с IP-адресом.

Так, сеть 192.168.0.0 с маской 255.255.255.0 (иначе можно записать 192.168.0.0/24[1]) может содержать хосты с адресами от 192.168.0.1 до 192.168.0.254. Адрес 192.168.0.255 — это адрес широковещательной рассылки для данной сети. А сеть 192.168.0.0 с маской 255.255.255.128 (192.168.0.0/25) допускает адреса от 192.168.0.1 до 192.168.0.127 (адрес 192.168.0.128 используется при этом в качестве широковещательного).

На практике сети с небольшим возможным числом хостов используются интернет-провайдерами (с целью экономии IP-адресов). Например, клиенту может быть назначен адрес с маской 255.255.255.252. Такая подсеть содержит только два хоста. При разбиении сети организации используют диапазоны локальных адресов сетей класса C. Сеть класса C имеет маску адреса 255.255.255.0 и может содеражать до 254 хостов. Применение сетей класса C при разбиении на VLAN в условиях предприятия связано с тем, что протоколы автоматической маршрутизации используют именно такие подсети.

При создании подсетей в организации рекомендуется придерживаться следующего правила: подсети, относящиеся к определенному узлу распределения, должны входить в одну сеть. Это упрощает таблицы маршрутизации и экономит ресурсы коммутаторов. Например, если к данному коммутатору подключены подсети 192.168.0.0/255.255.255.0, 192.168.1.0/255.255.255.0, 192.168.3.0/255.255.255.0, то другому коммутатору достаточно знать, что в этом направлении следует пересылать пакеты для сети 192.168.0.0/255.255.252.0.

Эта рекомендация несущественна для сетей малых и средних организаций, поскольку ресурсов современных коммутаторов достаточно для хранения настроек такого объема.

Примечание

Хотя многие сертификационные экзамены содержат вопросы, так или иначе связанные с разбиением на подсети (правильный подсчет маски сети, числа адресов и т. п.), на практике проводить ручной подсчет вряд ли придется. Существует много онлайновых ресурсов, которые предлагают различные варианты калькуляторов сетевых адресов (Network Calculator), например **http://www.globalstrata.com/services/network/bscnetcalc.asp**.

После того как компьютер получил IP-адрес и ему стало "известно" значение маски подсети, программа может начать работу в данной локальной подсети. Чтобы обмениваться информацией с другими компьютерами в глобальной сети, необходимо знать правила, куда пересылать информацию для внешней сети. Для этого служит такая характеристика IP-протокола, как адрес шлюза.

---

[1] 24 соответствует длине маски, используемой для адресации подсетей. Если записать маску 255.255.255.0 в двоичном виде, то получится последовательность из 24 единиц и 8 нулей. Маска 255.255.255.128 будет представлять собой последовательность из 25 единиц и 7 нулей. Поэтому ее записывают также в виде /25 и т. д.

Шлюз (Gateway, default gateway)

Шлюз (gateway) — это устройство (компьютер), которое обеспечивает пересылку информации между различными IP-подсетями. Если программа определяет (по IP-адресу и маске), что адрес назначения *не входит* в состав локальной подсети, то она отправляет эти данные на устройство, выполняющее функции шлюза. В настройках протокола указывают IP-адрес такого устройства.

Для работы *только* в локальной сети шлюз может не назначаться[1].

Для индивидуальных пользователей, подключающихся к Интернету, или для небольших предприятий, имеющих единственный канал подключения, в системе должен быть только один адрес шлюза — это адрес того устройства, которое имеет подключение к Сети. При наличии нескольких маршрутов (путей пересылки данных в другие сети) будет существовать несколько шлюзов. В этом случае для определения пути передачи данных используется таблица маршрутизации.

Таблицы маршрутизации

Организация может иметь несколько точек подключения к Интернету (например, в целях резервирования каналов передачи данных или использования более дешевых каналов и т. п.) или содержать в своей структуре несколько IP-сетей. В этом случае, чтобы система "знала", каким путем (через какой шлюз) посылать ту или иную информацию, используются *таблицы маршрутизации* (routing). В таблицах маршрутизации для каждого шлюза указывают те подсети Интернета, для которых через них должна передаваться информация. При этом для нескольких шлюзов можно задать одинаковые диапазоны назначения, но с разной стоимостью передачи данных: информация будет отсылаться по каналу, имеющему самую низкую стоимость, а в случае его выхода из строя по тем или иным причинам автоматически будет использоваться следующее наиболее "дешевое" подсоединение.

Таблицы маршрутизации имеются на каждом устройстве, использующем протокол IP. Администраторы в основном работают с таблицами маршрутизации коммутирующего оборудования. Настройка таблиц маршрутизации компьютеров имеет смысл только в случае наличия нескольких сетевых адаптеров, подключенных к различным сегментам сети. Если у компьютера есть только одна сетевая карта (одно подключение к Интернету), таблица маршрутизации имеет наиболее простой вид: в ней записано, что все сигналы должны отправляться на шлюз, назначенный *по умолчанию* (default gateway).

---

[1] Если для доступа в Интернет используется прокси-сервер, то компьютерам локальной сети адрес шлюза также может не назначаться.

Просмотреть таблицу маршрутизации протокола TCP/IP можно при помощи команды `route print`. С помощью команды `route` можно также добавить новый статический маршрут (`route add`) или постоянный маршрут — `route add -p` (маршрут сохраняется в настройках после перезагрузки системы).

Покажем на примере, как можно использовать модификации таблицы маршрутизации. Предположим, что на компьютере имеются две сетевых карты, одна из которых непосредственно подключена к Интернету (имеет реальный адрес), а вторая используется для работы во внутренней сети (локальный адрес). Доступ в Интернет производится по умолчанию через шлюз в локальной сети. В этом случае таблица маршрутизации, отображаемая по команде `route print`, выглядит примерно так:

```
Активные маршруты:
Сетевой адрес     Маска сети       Адрес шлюза    Интерфейс   Метрика
0.0.0.0           0.0.0.0          192.168.0.4    192.168.0.29   1
127.0.0.0         255.0.0.0        127.0.0.1      127.0.0.1      1
192.168.0.0       255.255.255.0    192.168.0.29   192.168.0.29   1
192.168.0.29      255.255.255.255  127.0.0.1      127.0.0.1      1
192.168.0.255     255.255.255.255  192.168.0.29   192.168.0.29   1
195.161.192.0     255.255.255.224  195.161.192.2  195.161.192.2  1
195.161.192.2     255.255.255.255  127.0.0.1      127.0.0.1      1
195.161.192.255   255.255.255.255  195.161.192.2  195.161.192.2  1
224.0.0.0         240.0.0.0        192.168.0.29   192.168.0.29   1
224.0.0.0         240.0.0.0        195.161.192.2  195.161.192.2  1
255.255.255.255   255.255.255.255  192.168.0.29   192.168.0.29   1
255.255.255.255   255.255.255.255  195.161.192.2  195.161.192.2  1
Основной шлюз:         192.168.0.4
===========================================
Постоянные маршруты: Отсутствует
```

Проверим путь прохождения пакетов на адрес Интернета, например 109.84.231.210, с помощью команды `tracert`[1]:

```
tracert 109.84.231.210 -d
```

В итоге получаем примерно такую картину (листинг ограничен первыми четырьмя узлами):

```
Трассировка маршрута к 109.84.231.210 с максимальным числом прыжков 30
1    <1 мс    <1 мс    <1 мс   192.168.0.4
2    <1 мс    <1 мс     1 ms   195.12.72.145
3    15 ms     1 ms     1 ms   195.12.75.245
4    40 ms    57 ms    41 ms   195.12.75.241
...
```

[1] Ключ `-d` использован для ускорения операции, чтобы отключить запросы DNS-имен тех хостов, через которые передается пакет данных.

Предположим, что мы хотим изменить путь прохождения пакетов к выбранному нами хосту, направив информацию через вторую сетевую карту (а не через шлюз по умолчанию). Для этого с помощью команды `route add` нужно добавить желаемый нами маршрут:

```
route add 109.84.231.210 mask 255.255.255.255 195.161.192.2
```

В команде мы указали, что хотим назначить новый маршрут не для диапазона адресов, а только для конкретного значения (поэтому маска — 255.255.255.255). Кроме того, явно указали адрес сетевого интерфейса, через который нужно пересылать пакеты.

После исполнения данной команды (на экран система не выводит никаких итогов операции) можно просмотреть новую таблицу маршрутизации:

```
Активные маршруты:
Сетевой адрес    Маска сети       Адрес шлюза    Интерфейс     Метрика
...
109.84.231.210   255.255.255.255  195.161.192.2  195.161.192.2    1
...
Основной шлюз:         192.168.0.4
===================================
Постоянные маршруты: Отсутствует
```

По сравнению с исходным вариантом таблица маршрутизации дополнилась одной строкой, которая приведена в данном примере (остальные строки не изменились и опущены для наглядности).

Проверяем новый путь прохождения сигналов:

```
Трассировка маршрута к 109.84.231.210 с максимальным числом прыжков 30
1     1 ms     1 ms     1 ms     195.161.192.1
2    23 ms    22 ms    23 ms     195.161.94.137
3    23 ms    23 ms    23 ms     195.161.94.5
...
```

Видно, что пакеты пересылаются уже через *другой* интерфейс.

Эти изменения маршрутизации действуют до перезагрузки системы или до подачи обратной команды: удаления записей маршрутизации. Для восстановления параметров маршрутизации достаточно подать команду, указав тот маршрут, который требуется удалить[1]:

```
route delete 109.84.231.210
```

[1] Если подобные изменения необходимы постоянно, то следует использовать запуск команды с ключом `-p`, после чего добавленный маршрут будет отображен также в строке `Постоянные маршруты`.

При этом обычно можно не указывать параметры маски и интерфейса (если они однозначно определяются по вводимому в команде адресу).

Примечание

На практике автор встречался с ситуациями, когда изменение параметров маршрутизации в операционной системе Windows не сразу "отрабатывалось" корректно. Иногда после операций над таблицей маршрутизации для достижения успеха нужно было программно отключить и вновь включить тот сетевой интерфейс, для которого выполнялась настройка.

Понимание правил маршрутизации важно не только при построении маршрутов в Интернете, — задаче, которую вряд ли придется решать администраторам сетей некрупных предприятий. На практике для выделения обособленных участков локальной сети (например, по соображениям безопасности) достаточно широко используются виртуальные сети *(см. разд. "Создание виртуальных сетей" ранее в этой главе)*. А для того чтобы обеспечить избранный доступ в такие сети, администраторы должны уметь написать правильную таблицу маршрутизации для соответствующей VLAN[1].

Автоматическое присвоение параметров IP-протокола

Как уже отмечалось, параметры IP-протокола индивидуальны для каждого компьютера. Чтобы облегчить пользователям их назначение, были разработаны специальные механизмы, позволяющие автоматизировать данный процесс.

Серверы DHCP

В локальных сетях администраторы устанавливают так называемый сервер DHCP (Dynamic Host Configuration Protocol, динамический протокол конфигурации сервера). Сервер DHCP автоматически сообщает компьютерам, начинающим работу в составе сети, параметры настройки протокола TCP/IP: в первую очередь это IP-адрес, маска адреса, шлюз. Причем администраторы могут с помощью сервера DHCP сообщать клиенту различные настройки: адреса WINS- и DNS-серверов, серверов времени, указывать расположение данных автоматической настройки прокси-клиентов и т. п.

Примечание

На практике возможны различные варианты настройки DHCP. Так, автор неоднократно на практике сталкивался с ситуацией, когда адреса клиентам назначались фактически "по статике" (путем резервирования по MAC-адресам), а остальные параметры TCP/IP-протокола определялись динамически.

---

[1] Или создать список доступа — ACL (access control list), в котором правила записываются аналогично правилам маршрутизации.

Обычно IP-адрес от сервера DHCP выделяется компьютеру на определенный срок, заданный в настройках сервера (поэтому его называют также *динамическим IP-адресом*). Если компьютер не будет продолжать работу в данной сети, то этот адрес может быть переназначен другому устройству.

При добавлении IP-протокола в операционную систему его настройки по умолчанию предусматривают автоматическое получение параметров. Если в сети есть настроенный DHCP-сервер, то от пользователя локального компьютера в этом случае не потребуется никаких дополнительных действий по настройке TCP/IP-протокола.

Адресация APIPA

Для облегчения построения небольших сетей разработчики Microsoft включили в последние версии Windows возможность самостоятельного назначения адресов. Если в сети нет сервера DHCP, а протокол IP установлен с параметрами автоматического получения значений, то Windows присвоит сетевой плате адрес из диапазона от 169.254.0.1 по 169.254.255.254 (маска подсети 255.255.0.0), предварительно проверив, не используется ли уже такой адрес в системе. Данный механизм позволяет применять IP-протокол в небольших сетях при минимальных ручных настройках. Естественно, что никаких дополнительных параметров настройки операционная система в этом случае не получает. Например, она не будет знать, куда посылать запросы, чтобы получить данные с серверов Интернета. А если будет отключен NetBIOS поверх TCP/IP, то системы не смогут разрешить имена других компьютеров сети и т. п.

Примечание

Использование адреса из указанного выше диапазона (проверяется командами `ipconfig` или `winipcfg`) при наличии в сети сервера DHCP свидетельствует либо о неисправности последнего, либо о проблемах кабельного подключения данного компьютера.

Назначение адресов при совместном использовании подключения к Интернету

Особая ситуация возникает при настройке совместного использования подключения к Интернету. В этом случае тот компьютер, на котором создается данное подключение, начинает выполнять роль сервера DHCP с единственным ограничением: его адрес *жестко фиксирован* — 192.168.0.1. Клиенты, которые получают от данного сервера адреса из подсети 192.168.0.0/24, автоматически настраиваются на использование его в качестве шлюза по умолчанию и сервера имен.

Поскольку вариант совместного использования подключения присутствует как на серверных системах, так и на рабочих станциях, то такое решение яв-

ляется наиболее оптимальным для небольших организаций. Настройте подключение к Интернету, включите его совместное использование — и вы получите у себя в сети корректное назначение параметров TCP/IP-протокола для компьютерных систем.

Порт

При передаче данных кроме IP-адресов отправителя и получателя пакет информации содержит в себе номера *портов*. Порт — это некое число, которое используется при приеме и передаче данных для идентификации процесса (программы), который должен обработать данные. Так, если пакет послан на 80-й порт, то это свидетельствует, что информация предназначена серверу HTTP.

Номера портов с 1-го по 1023-й закреплены за конкретными программами (так называемые *well-known-порты*). Порты с номерами 1024—65 535 могут быть использованы в программах собственной разработки. При этом возможные конфликты должны разрешаться самими программами путем выбора свободного порта. Иными словами, порты будут распределяться динамически: возможно, что при следующем старте программа выберет иное значение порта.

Знание того, какие порты используют те или иные прикладные программы, важно при настройке брандмауэров. Часть настроек в таких программах для наиболее популярных протоколов предопределена, и вам достаточно только разрешить/запретить протоколы, руководствуясь их названиями. Однако в некоторых случаях придется обращаться к технической документации, чтобы определить, какие порты необходимо "открыть", чтобы обеспечить прохождение пакетов данной программы.

Примечание

При настройке брандмауэра следует учитывать, что многие программы при подключении к Интернету открывают не один порт, а используют некоторый диапазон значений. Один из возможных вариантов настройки брандмауэров для недокументированных программ — это анализ их реального трафика с помощью какой-либо программы перехвата передаваемых по сети пакетов.

Увидеть, какие порты реально задействованы на компьютере, можно с помощью команды `netstat`. В зависимости от версии операционной системы данная команда имеет различный набор ключей, позволяющих детализировать отчет (например, указать программы или процессы, использующие конкретные порты). В общем случае достаточно запустить команду с ключом `-a`:

```
>netstat -a
Активные подключения
  Имя     Локальный адрес       Внешний адрес          Состояние
  TCP     sasha:http            sasha.ask.ru:0         LISTENING
```

```
TCP    sasha:epmap          sasha.ask.ru:0           LISTENING
TCP    sasha:https          sasha.ask.ru:0           LISTENING
TCP    sasha:microsoft-ds   sasha.ask.ru:0           LISTENING
TCP    sasha:1025           sasha.ask.ru:0           LISTENING
TCP    sasha:1033           sasha.ask.ru:0           LISTENING
TCP    sasha:1064           ack-isa2.ask.ru:8080     CLOSE_WAIT
TCP    sasha:1067           ack-exchange.ask.ru:2703 ESTABLISHED
TCP    sasha:1070           ack-exchange.ask.ru:1025 ESTABLISHED
TCP    sasha:1078           ack-frw.ask.ru:8080      CLOSE_WAIT
UDP    sasha:microsoft-ds   *:*
UDP    sasha:isakmp         *:*
UDP    sasha:1041           *:*
UDP    sasha:1053           *:*
```

В данном примере на компьютере готовы к подключению несколько портов (состояние `LISTENING`): это порты http, epmap и т. д. — номера портов можно отобразить, если добавить ключ `-n`; порты 1067 и 1079 подключены (`ESTABILISHED`, программа показывает, с какой системой идет обмен данными); передача информации с портов 1064 и 1078 завершена и система находится в состоянии закрытия соединения (`CLOSE_WAIT`) и т. д.

Примечание

Для получения информации по удаленному компьютеру используются специальные программы *сканирования портов*. Данные по отдельному порту можно получить штатными средствами системы (например, с помощью команды telnet или утилиты PortQry из состава Support Tools).

Протокол ARP

Пакеты, пересылаемые в сети Ethernet, адресуются компьютерам не по их именам и не на IP-адрес. Пакет предназначается устройству с конкретным MAC-адресом.

MAC-адрес — это уникальный адрес сетевого устройства, который заложен в него изготовителем оборудования. Первая половина MAC-адреса представляет собой идентификатор изготовителя, вторая — уникальный номер данного устройства.

Примечание

MAC-адрес часто используется для идентификации систем, например, при создании фильтров допуска в Интернет. Однако следует знать, что этот способ не является полностью надежным: хотя MAC-адрес должен быть уникальным и является неотъемлемой характеристикой устройства, существуют способы его изменения. Например, в новых операционных системах его можно сменить даже через штатные свойства сетевого адаптера, поэтому хакеру для обхода та-

кого фильтра доступа достаточно вывести из строя действующую систему (или выбрать момент ее выключения) и продолжить работу от ее адреса.

Для получения MAC-адреса используется протокол ARP (Address Resolution Protocol, протокол разрешения адресов). В системе имеется специальная утилита, которая позволяет отобразить кэш известных данному компьютеру MAC-адресов — `arp`.

Утилита `arp` может быть использована, например, при создании резервированных адресов DHCP-сервера. Для такой настройки администратору необходимо ввести MAC-адрес соответствующей системы. Чтобы его узнать, достаточно выполнить команду `ping` на имя данной системы, после чего просмотреть кэш ARP (командой `arp -a`) и скопировать значение MAC-адреса в настройки DHCP.

Имена компьютеров в сети TCP/IP

Человеку удобнее работать с именем компьютера, чем запоминать цифры, составляющие его IP-адрес. В сети на основе протокола TCP/IP компьютеры могут иметь два имени: это NetBIOS-имя компьютера и имя *хоста* (DNS-имя). Обычно имя хоста и NetBIOS-имя совпадают, и к этому следует стремиться. Но принципиально эти имена могут быть разными. Например, длина NetBIOS-имени ограничена 15 символами, а хосту может быть присвоено более длинное название. Или, если при создании домена вы пытаетесь дать ему имя, совпадающее с именем будущего контроллера, то программа установки предложит выбрать другое имя данному хосту.

Имя хоста составляется из нескольких имен, разделяемых при написании точкой, например, так: **www.ask.ru**. Первая слева группа символов (до точки), в данном примере это **www**, является собственным именем компьютера. Следующая группа символов — от точки до точки — это имя группы компьютеров, которой принадлежит данная система. Следующая группа символов — имя группы компьютеров, которой в свою очередь принадлежат группы компьютеров, имена которых находятся левее. Данную цепочку можно продолжать сколь угодно долго. Для удобства обычно ограничиваются тремя-четырьмя группами символов.

На практике под *именем домена* понимают всю группу символов справа от имени компьютера. В зависимости от того, сколько групп символов входит в доменное имя, различают домены первого, второго, третьего и т. д. уровней.

Примечание

При создании нового домена Windows не следует давать ему имя домена первого уровня. В этом случае действуют некоторые ограничения, с которыми можно ознакомиться в базе данных Microsoft. Целесообразно дать домену Windows имя вида ***<название_организации>*.local**.

Самая правая группа символов имени (до первой точки) называется *доменом первого уровня*, вторая справа — *доменом второго уровня*, затем следует *домен третьего уровня* и т. д.

Примечание

Иногда употребляют термин FQDN — fully qualified domain name (обычно эту аббревиатуру употребляют без перевода; русский термин звучит как *полное имя узла*). Под FQDN понимают полную цепочку имен системы: от имени хоста до имени корневого домена. Чтобы подчеркнуть, что имеется в виду *полное* имя, в конце его ставят *точку*, которую принято считать *именем корневого домена*. Например, FQDN для Web-сайта будет писаться следующим образом: **www.ask.ru.** (последняя точка включается в имя).

Имена хостов внутри широковещательного домена Windows должны быть уникальны. При попытке запуска системы, имеющей такое же имя, как и у другого работающего компьютера, вы получите сообщение об ошибке.

Доменные имена Интернета

В Интернете за уникальностью присваиваемых имен следит организация (физическое лицо), отвечающая за домен, в рамках которого выдается имя. При присвоении имен используется принцип: если данное доменное имя свободно, то его можно получить. Приобретение доменного имени — это платная услуга, кроме того, необходимо ежегодно продлевать действие имени. "Отобрать" выданное доменное имя практически невозможно.

Такой способ гарантирует уникальность полного доменного имени компьютера и в то же время требует проверки на уникальность желаемого имени только в одном месте.

Организации и физические лица, регистрирующие для себя доменные имена, обычно стараются создать такое доменное имя, которое легко запоминается пользователем, при этом часто используется юридическое название. Сравните: Белый дом (США) — **whitehouse.gov**, корпорация Microsoft — **microsoft.com**, и т. д.

Существуют два направления создания доменных имен. Одно — по географическому принципу (каждая страна имеет свой домен первого уровня, в рамках которого создаются все имена компьютеров), второе — по типу деятельности организации. В России "географический" домен имеет имя ru.

Функции технического сопровождения системы регистрации и DNS-серверов зоны ru осуществляет Российский НИИ развития общественных сетей (РосНИИРОС). Со списком организаций, осуществляющих регистрацию в домене ru, можно ознакомиться на странице **http://www.ripn.net:8080/nic/dns/registry-all/reg_list.html**.

По состоянию на момент подготовки книги данные функции выполняли:

- Региональный Сетевой Информационный Центр (RU-CENTER, **http://www.nic.ru/**);
- Гарант-Парк-Телеком (**http://www.r01.ru/**);
- ООО "СЦС Совинтел" (**http://www.sovintel.ru/**);
- Объединение сетей Фринет (**http://www.free.net/**);
- Демос-Интернет (**http://www.demos-internet.ru/new/index.html**);
- ООО "Регтайм" (**http://www.webnames.ru/**).

Второе направление — это присвоение имени на основе типа деятельности. Среди подобных имен наиболее известен домен com для коммерческих организаций. Другие популярные домены — это edu (учебные организации), gov (правительственные), net (сетевые ресурсы), org (некоммерческие организации), info и т. п.

В настоящее время список доменов "по типу деятельности" существенно расширен, в том числе введено много доменов, в которых можно бесплатно зарегистрировать имя для общественных проектов.

Соотношение доменных имен и IP-адресов компьютеров

Каждый компьютер в глобальной сети должен иметь уникальный IP-адрес. Без наличия такого адреса работа просто невозможна. Наличие доменного имени для работы не обязательно. При необходимости в строках адреса программ, предназначенных для работы в Интернете, можно набирать IP-адрес.

Доменное имя может существовать, но не иметь IP-адреса (естественно, работа с такими узлами невозможна). Такая ситуация может возникнуть, если, например, организация заранее зарегистрировала за собой доменное имя, но не располагает в настоящий момент какими-либо ресурсами в сети Интернет.

Одно доменное имя может иметь несколько IP-адресов. Обычно это практикуется на популярных узлах Интернета, что позволяет с помощью специальных решений распределить нагрузку с одного компьютера на несколько. Аналогично несколько доменных имен могут соответствовать одному IP-адресу (например, при размещении на компьютере нескольких WWW-серверов, соответствующих различным организациям).

IP-адреса, соответствующие данному доменному имени, могут меняться. Например, организация переезжает или меняет интернет-провайдера. Сохранение "за собой" доменного имени позволяет не беспокоиться, что в подобных случаях придется нести затраты на "раскрутку" нового имени.

Серверы доменных имен (DNS)

NetBIOS-имя компьютера определяется при установке операционной системы. По умолчанию это же имя будет использовано в качестве имени хоста при получении IP-адреса, хотя в Windows можно назначить разные имена NetBIOS и DNS.

Для поиска компьютера в локальной сети по имени ранее использовались широковещательные запросы: система рассылает запрос на определение имени всем станциям и ждет ответа. Увеличение размеров сети заставляет отказаться от данного метода, поскольку он приводит к значительному росту подобного широковещательного трафика. В распределенных сетях на основе протокола TCP/IP для разрешения имен используются специальные серверы — DNS-серверы (Domain Name System).

Серверы DNS обеспечивают получение доменного имени по запросу на основе IP-адреса, и наоборот. Поэтому указание адреса сервера DNS является одной из основных настроек протокола TCP/IP, необходимых для работы в Интернете[1].

Адрес сервера DNS обычно сообщается автоматически при инициализации протокола IP. Имена серверов DNS сообщаются DHCP-серверами. Обычно указывается несколько DNS-серверов, чтобы система могла использовать второй сервер при временной недоступности первичного DNS.

WINS

Служба регистрации имен в сети Windows (Windows Inter-networking Name Server, WINS) использовалась для регистрации сетевых имен компьютеров в локальных сетях до Windows 2000. Служба WINS позволяла корректно разрешать имена в сетях с наличием маршрутизаторов[2].

Примечание

Хотя в настоящее время WINS-сервер в локальных сетях необходим станциям на базе Windows 3.1/9*x*/NT, однако и часть современных служб использует NetBIOS. Например, некоторые функции MS Exchange Server применяют NetBIOS-запросы. Поэтому целесообразно сохранить WINS в составе локальной сети.

При начале работы в сети компьютер "сообщает" серверу WINS свое имя и IP-адрес. Эти параметры заносятся в специальную базу и используются для поиска имени компьютера на основе его адреса, и наоборот. Поэтому, чтобы

---

[1] Если в настройках не указан IP-адрес сервера DNS, то пользователь не сможет полноценно работать в Интернете, поскольку ему будет не доступен переход по ссылкам, в которых использовано доменное имя, а это практически все ссылки на информационных серверах.

[2] Маршрутизаторы не пропускают широковещательные пакеты, поэтому сегменты локальной сети оказываются изолированными друг от друга при операциях просмотра без использования WINS.

узнать имя компьютера в локальной сети (или его адрес), достаточно сформировать запрос к WINS.

Адрес WINS обычно автоматически сообщается клиентам с помощью DHCP-сервера при получении параметров TCP/IP.

Статическое задание имен

В небольшой локальной сети для задания соответствия "IP-адрес — сетевое имя" можно использовать статические записи, формируемые вручную. Это позволяет обеспечить функционирование сети без использования серверов WINS, DHCP и т. п.

Если Windows не может динамически определить имена (IP-адреса) хостов, то система использует содержимое файлов hosts, networks и lmhosts. Первые два файла представляют обычный список соотношений "IP-адрес — имя" в прямом и обратном порядке:

- файл hosts:

```
...
195.12.156.31      ads.adximize.com
63.120.34.76       c3.xxxcouter.it
```

- файл networks:

```
...
ads.adximize.com  195.12.156.31
c3.xxxcouter.it    63.120.34.76
...
```

Файл lmhosts совместим с Microsoft LAN Manager 2.*x* и используется для загрузки специальных NetBIOS-имен (указания сервера домена, серверов приложений и т. п.). Файлы находятся в папке %systemroot%/system32/drivers/etc (для Windows 9*x* — в папке Windows). При установке системы обычно создаются примеры (имеют расширение sam), по образцу которых и следует редактировать необходимые файлы.

Изменять файлы можно в любом текстовом редакторе, однако для этого необходимы права администратора. Запись должна начинаться с первой позиции строки, а столбцы могут отделяться любым числом пробелов. Операция трудоемкая, особенно при добавлении в сеть новых компьютеров, поскольку это потребует внесения изменений в данные файлы для *всех* уже имеющихся в сети систем.

Последовательность разрешения имен

На практике вы можете столкнуться с тем, что часть систем "видит" одно число компьютеров в сети, а другая — иное. Одни компьютеры успешно ра-

ботают в сети, а на других отображается сообщение, что вход в сеть не может быть произведен, т. к. система не находит контроллер домена. Эти ситуации обусловлены различными используемыми методами *разрешения имен*.

Разрешение имен применяется для того, чтобы найти компьютер (определить IP-адрес) по его имени и получить информацию о сетевых службах, например, узнать адреса контроллеров домена.

Основное отличие методов разрешения имен различных версий Windows состоит в том, что системы до Windows 2000 использовали для разрешения имен NetBIOS, а Windows 2000 и старше (Windows 200x/XP) нуждаются в информации DNS.

При необходимости разрешения имени сначала производится попытка его поиска в локальных ресурсах. Прежде всего, это локальный кэш имен, который для увеличения производительности создают все системы (кэш имен NetBIOS или кэш имен DNS). Если нужное имя компьютера не найдено, то система пытается найти его в host-файлах. Если и эта попытка неудачна, то системы с Windows 2000 и старше обращаются к серверу DNS, определенному в параметрах настройки протокола TCP/IP их сетевого адаптера. Если сервер DNS недоступен или не смог вернуть имя, то на этом попытки прекращаются и сообщается, что имя не найдено.

Системы Windows 9*x* и Windows NT 4.0 в зависимости от параметров настройки NetBIOS либо рассылают широковещательные запросы на определение имени, либо обращаются к серверу WINS. Информация DNS используется только в том случае, если это явно указано в настройках сетевого адаптера.

Примечание

Если использование NetBIOS поверх TCP/IP запрещено настройками системы, то Windows 9*x* и Windows NT 4.0 не смогут правильно разрешать имена других компьютеров.

С помощью DNS системы на базе Windows 200*x*/XP находят и расположение служб. Например, адрес контроллера домена может быть узнан по имени _ldap._tcp.dc._msdcs.<имя_домена>, адрес службы Gatekeeper (используется при передаче IP-телефонии, видеоконференций и т. п. по каналам связи) определяется по результатам запроса на имя Q931._tcp.<имя_домена> и т. д.

При использовании NetBIOS станции, регистрируясь в сети, сообщают свое имя и имена служб, которые на них запущены. Эти имена можно просмотреть, например, при помощи команды `nbtstat -a <имя_компьютера>`. В результате будет отображена приблизительно такая информация:

```
>nbtstat -a test
Internal:
Адрес IP узла: [192.168.0.29] Код области: []
```

```
Таблица NetBIOS-имен удаленных компьютеров
Имя                    Тип          Состояние
---------------------------------------------------
TEST           <00>    Уникальный   Зарегистрирован
ACK            <1C>    Группа       Зарегистрирован
ACK            <00>    Группа       Зарегистрирован
TEST           <20>    Уникальный   Зарегистрирован
ACK            <1B>    Уникальный   Зарегистрирован
ACK            <1E>    Группа       Зарегистрирован
ACK            <1D>    Уникальный   Зарегистрирован
__MSBROWSE__.  <01>    Группа       Зарегистрирован
MP_ACK         <1A>    Уникальный   Зарегистрирован

Адрес платы (MAC) = 00-02-B3-4F-F9-E9
```

В нашем примере компьютер TEST зарегистрировал имя рабочей станции TEST (первая строка)[1]. Запись `ACK <1C>` свидетельствует о том, что этот компьютер является контроллером домена ACK, `ACK <00>` — это имя домена компьютера, `TEST <20>` свидетельствует о том, что на компьютере запущена служба *сервер*. Строка `ACK <1B>` говорит о том, что компьютер является мастер-просмотрщиком сети и т. п.

Эти имена сохраняются на компьютерах, выполняющих роли просмотра сети, а также на сервере WINS, с которых они могут быть получены по запросам клиентов.

Прокси

Еще один термин, с которым вам придется постоянно встречаться при работе в Интернете, — это *прокси-сервер* (proxy).

Практика показывает, что некоторая информация пользуется особой популярностью: ее запрашивают многие пользователи, иногда даже не по одному разу в день. Чтобы снизить нагрузку на сети, стали устанавливать так называемые прокси-серверы. На прокси-сервере автоматически сохраняется на некоторый срок вся проходящая через него информация. Если прокси-сервер обнаружит запрос данных, уже имеющихся на нем в копии, то именно эта копия и будет направлена пользователю.

Кроме того, включение прокси-сервера в настройки обозревателя Интернета позволяет повысить скорость просмотра сети. Это связано с тем, что многие файлы уже не приходится получать из Сети: скорость загрузки файлов с про-

[1] Типы служб, соответствующих сообщаемым командой кодам, можно посмотреть, например, по адресу **http://www.microsoft.com/technet/prodtechnol/winntas/support/ sur_apph.mspx**.

кси-сервера, располагающегося обычно "вблизи" пользовательского компьютера, выше скорости получения данных с удаленных хостов.

В параметрах правильно спроектированных страниц информационных сайтов должна быть указана возможность кэширования данных на прокси-серверах, а также "срок актуальности". Бывает, что разработчики не указывают такие значения и прокси-сервер использует свои настройки по умолчанию: в этом случае он может выдать пользователю устаревшие данные. Чтобы обновить страницу и загрузить последние данные, следует выполнить команду **Обновить** в меню программы просмотра. В этом случае прокси-сервер должен запросить данные из Интернета.

Работа через прокси-сервер не обязанность, а право. Прокси-сервер указывается в настройках программ, осуществляющих просмотр Интернета (например, Opera, IE и т. д.). Его использование позволяет повысить скорость работы в Сети и снизить затраты на оплату доступа в Интернет.

Для того чтобы повысить эффективность работы через прокси-сервер, следует предусмотреть достаточный объем жесткого диска для хранения данных, получаемых из Интернета. Обычно при оценке размеров кэша стоит ориентироваться на объем месячного трафика организации, обслуживаемой таким сервером.

На рис. 3.12 приведена диаграмма использования кэша прокси-сервера по итогам работы за месяц. Хотя конкретные показатели будут отличаться в различных организациях, видно, что работа через прокси существенно снижает трафик интернет-организации.

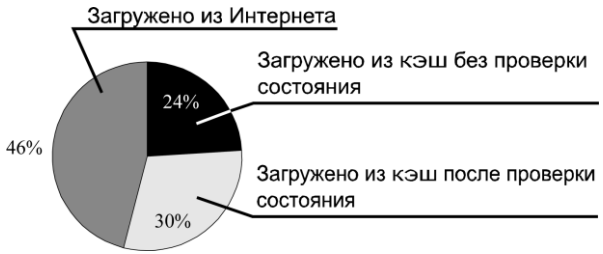


Рис. 3.12. Статистика использования кэша прокси-сервера

Автообнаружение прокси-серверов

Рабочие станции можно настраивать на автоматическое обнаружение и использование прокси-сервера. Существуют различные механизмы, при помощи которых клиенты локальной сети могут получать необходимые настройки для автоматического конфигурирования работы через прокси-сервер. Так, в домене Windows настройки прокси-сервера могут распространяться через групповую политику *(см. главу 6, разд. "Групповые и системные политики")*.

Для автоматической конфигурации параметров использования прокси-сервера предназначен специальный сценарий. По умолчанию такой сценарий должен иметь имя wpad.dat и публиковаться по протоколу HTTP на сервере с доменным именем WPAD.

Сценарий автообнаружения прокси написан на языке макропрограммирования. В случае необходимости его можно откорректировать. Например, при наличии двух точек доступа к Интернету сценарий может содержать функции случайного использования того или иного канала с заранее определенным весовым коэффициентом (при работе с массивом прокси-серверов). Если необходимо работать с некоторыми серверами Интернета только через один канал, то такую возможность можно реализовать именно через модификацию данного сценария.

Примечание

Обратите внимание, что если обозреватель получит из данного сценария параметры нефункционирующего прокси-сервера, то просмотр Интернета окажется невозможным.

Если вы имеете подобный сценарий (а он, например, создается автоматически при установке прокси-сервера Microsoft ISA Server), то необходимо создать на DNS-сервере запись, которая указывала бы на данный хост[1]. Параметры сценария могут сообщаться также и сервером DHCP: для этого нужно добавить новый стандартный параметр в меню **Predefined Options** оснастки управления сервером DHCP с номером 252[2] и установить его значение равным URL сценария автонастройки[3]. Например[4]:

```
http://wpad.<имя_домена>:8080/wpad.dat
```

Диагностика IP-протокола

Примечание

Диагностику IP-параметров diaul-up-подключения (подключения к провайдеру по телефонному каналу связи) необходимо проводить *после* установления модемного соединения.

---

[1] Например, можно создать запись-синоним — CNAME.

[2] Этому параметру можно дать любое название, например, Proxy Autodiscovery Option или просто wpad.

[3] Для Windows-клиентов необходимо записывать URL только строчными символами, поскольку, например, наличие прописной буквы может привести к ошибке автообнаружения прокси в случае использования ISA-сервера. См. KB307502.

[4] В параметрах DHCP можно указывать и номер порта, на котором публикуется сценарий. В случае DNS-записей допустима публикация только по стандартному порту HTTP — 80.

Для диагностики TCP/IP рекомендуется использовать следующую последовательность операций:

1. Проверка параметров настройки IP-протокола.
2. Проверка достижимости ближайших компьютеров сети.
3. Проверка функционирования серверов имен.
4. Проверка качества канала связи.

Примечание

В Windows XP существует специальный мастер диагностики сетевого подключения, который выполняет аналогичные операции и выдает результаты соответствующих тестов. Эта программа вызывается из меню утилиты **Сведения о системе** (**Пуск | Все программы | Стандартные | Служебные | Сведения о системе | Сервис | Диагностика сети**).

Проверка параметров настройки IP-протокола

Для отображения параметров IP-протокола используются утилиты `ipconfig` (Windows NT/200*x*/XP/Vista) и `winipcfg` (Windows 9*x*/ME). Утилита `ipconfig` выполняется в режиме командной строки. Утилита `winipcfg` имеет графический интерфейс.

Утилиты выводят на экран параметры настройки протокола TCP/IP: значения адреса, маски, шлюза. При запуске `ipconfig` с ключом `/all` на экран будут выведены все действующие параметры протокола. Отмечу также ключ `/renew`, который позволяет обновить автоматически полученные параметры IP-протокола, и ключ `/registerdns`, с помощью которого можно обновить запись на DNS-сервере данного компьютера (используется в Windows 200*x*/XP/Vista).

Примечание

Обратите внимание, что обычно при операции обновления сервер подтверждает ранее выданные адреса, поэтому о результате можно судить только по изменению информации в позициях `Доступ получен` и `Доступ истекает`.

Если утилита покажет, что сетевому адаптеру присвоен адрес 169.254.134.123 (или аналогичный), то можно сделать заключение, что в сети недоступен сервер, автоматически присваивающий параметры IP-протокола. Часто причиной подобной ошибки (если ранее компьютер нормально работал в сети) является нарушение контакта в подсоединении сетевого кабеля.

Проверка достижимости ближайших компьютеров сети

Для проверки достижимости компьютеров в сети TCP/IP используется команда `ping`. Эта команда посылает на заданный компьютер последователь-

ность символов определенной длины и выводит на экран информацию о времени ответа удаленной системы. Ключами команды можно регулировать количество отсылаемых символов и время ожидания ответа (через этот период выводится сообщение о превышении периода ожидания; если ответ придет позже, то он не будет показан программой).

При тестировании подключения рекомендуется применять следующую последовательность операций.

1. Сначала проверяется работоспособность протокола TCP/IP путем "пингования" адреса 127.0.0.1:

   ```
   ping 127.0.0.1
   ```

   Адрес 127.0.0.1 — это "личный" адрес любого компьютера. Таким образом, эта команда проверяет прохождение сигнала "на самого себя". Она может быть выполнена без наличия какого-либо сетевого подключения. Вы должны увидеть приблизительно следующие строки[1]:

   ```
   E:\ping 127.0.0.1
   Обмен пакетами с 127.0.0.1 по 32 байт:

   Ответ от 127.0.0.1: число байт=32 время<1мс TTL=128
   Ответ от 127.0.0.1: число байт=32 время<1мс TTL=128
   Ответ от 127.0.0.1: число байт=32 время<1мс TTL=128
   Ответ от 127.0.0.1: число байт=32 время<1мс TTL=128
   Статистика Ping для 127.0.0.1:
   Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь),
   Приблизительное время приема-передачи в мс:
   Минимальное = 0 мсек, Максимальное = 0 мсек, Среднее = 0 мсек
   ```

   Если будет показано сообщение о недостижимости адресата, то это означает ошибку установки протокола IP. В этом случае целесообразно удалить протокол из системы, перезагрузить компьютер и вновь установить поддержку протокола TCP/IP.

2. Следующим шагом необходимо проверить ответ локального компьютера по присвоенному ему IP-адресу. Для этого следует выполнить команду:

   ```
   ping <адрес>
   ```

---

[1] По умолчанию команда `ping` посылает пакет в 32 байта. Размер пакета может быть увеличен добавлением соответствующего ключа команды до 65 Кбайт. Таким образом можно обнаружить ошибки пересылки пакетов большого размера. После размера тестового пакета отображается время отклика удаленной системы (в нашем случае — меньше 1 мс). Далее выводится еще один параметр протокола — значение TTL (*время жизни пакета*; практически это число маршрутизаторов, через которые может пройти пакет: каждый маршрутизатор уменьшает значение TTL на единицу).

Результат, который должен быть выведен на экран в случае нормальной работы, практически аналогичен полученному в предыдущем примере.

3. Следующая проверка — это выполнение команды `ping` с указанием IP-адреса любого ближайшего компьютера. Можно использовать любой адрес, относительно которого вы уверены, что он достижим в локальной сети на момент проверки. Например, можно записать IP-адрес шлюза или адрес DNS-сервера.

   Наличие отклика свидетельствует, что канал связи установлен и работает. Отсутствие ответа обычно говорит либо о повреждении кабельной сети (например, нет контакта в разъеме), либо о неверно установленных параметрах статического адреса (если адрес получается автоматически, то следует обратиться в службу технической поддержки).

Проверка состояния порта TCP/IP удаленного компьютера

В случае применения брандмауэров для защиты подключения компьютера к Интернету наличие ответа от удаленной системы на команду `ping` совсем не означает, что пакеты, предназначенные другим портам, будут пропущены.

Существуют две возможности удостовериться в правильной настройке брандмауэра. Во-первых, в Support Tools от Windows 2003 присутствует утилита portqry.exe, которая позволяет увидеть ответ удаленной системы на запрос по конкретному порту. Так, для проверки достижимости FTP-сервера можно выполнить следующую команду:

```
portqry -n kenin -e 21
```

Результатом будет, например, такой вывод:

```
Querying target system called:
kenin
Attempting to resolve name to IP address...
Name resolved to 192.168.0.29
TCP port 21 (ftp service): LISTENING
Data returned from port:
220 kenin.ask.ru X2 WS_FTP Server 5.0.0 (1845270209)
331 Password required
```

Утилита сообщила, что порт 21 открыт, и отобразила информацию, которую выдает FTP-сервер, работающий на этом компьютере (имя компьютера `kenin`).

Примечание

Аналогичные утилиты, позволяющие осуществлять "пинги" на конкретные порты, легко найти в Интернете.

Второй способ состоит в применении утилиты `telnet`. Запуская эту утилиту с параметрами в виде имени удаленной системы и номером порта, вы осуществляете попытку подключения к соответствующему порту.

Если вы не можете подключиться к удаленной системе, то необходимо найти компьютер, на котором происходит фильтрация пакетов. Для этого следует проверить путь прохождения информации с помощью команды `tracert`, после чего протестировать возможность подключения к соответствующему порту каждого компьютера этой цепочки.

Листинг команды `tracert` таков:

```
E:\ tracert www.ack.ru

Tracing route to ack.ru [212.107.195.12]
over a maximum of 30 hops:

 1   120 ms   111 ms   112 ms  ask_pdc.ask.ru [192.168.0.67]
 2   117 ms   113 ms   111 ms  frw.ask.ru [192.168.0.2]
 3   121 ms   113 ms   116 ms  cisco.ask.ru [195.161.192.254]
 4  1011 ms   346 ms   136 ms  aa-s0-6-r2.ekaterinburg.rostelecom.ru
[195.161.94.137]
 5   387 ms   181 ms   397 ms  aa-fe0-2-sw1.ekaterinburg.rostelecom.ru
[195.161.94.5]
 6   504 ms   461 ms   134 ms  tschelkun-bbn0-po1-5.rt-comm.ru
[217.106.6.149]
 7   751 ms  1146 ms  1712 ms  kochenevo-bbn0-po2-0.rt-comm.ru
[217.106.6.130]
 8  1855 ms  1796 ms     *     trs20-dsr0-po8-0-0.rt-comm.ru
[217.106.6.138]
 9  1221 ms  1313 ms  1212 ms  vlad-dsr0-po6-0.rt-comm.ru [217.106.6.158]
10  1223 ms  1212 ms  1212 ms  vmts.vladivostok.rostelecom.ru
[195.161.4.94]
11     *        *        *     Request timed out.
12     *        *        *     Request timed out.
13  1727 ms  1871 ms  1703 ms  ack.ru [212.107.195.12]
Trace complete.
```

По результату выполнения данной команды можно оценить, что наибольшая задержка в прохождении сигнала возникает на каналах связи с узлами, стоящими в строках 7 и 8. Одиночные звездочки свидетельствуют, что ответ от этого узла не получен в заданный диапазон времени. Если в строке стоят все звездочки, то это может обозначать, что администраторы соответствующих хостов не разрешили прохождение ICMP-пакетов (пакеты, которые используются в том числе и командами `ping` и `tracert`).

Проверка функционирования серверов имен

Для проверки работоспособности сервера имен Интернета следует выполнить команду `ping`, указав в качестве параметра не IP-адрес, а доменное имя какого-либо компьютера[1]:

```
ping <имя>
```

Если команда сможет "разрешить" IP-адрес хоста и покажет отклик, то это означает работоспособность системы распознавания имен. Практически это говорит о правильной настройке протокола TCP/IP и работоспособности канала связи. Если не будет ответа на ввод команды с именем существующего хоста, то это может свидетельствовать либо об ошибке в задании DNS-серверов, либо об их неработоспособности.

Проверка качества канала связи

При работе в Интернете одни информационные серверы открываются быстрее, другие медленнее, бывают случаи недостижимости желаемого хоста. Часто причиной этого бывает недостаточное качество канала связи: большое время ожидания данных или существенный процент потерь пакетов, что обычно приводит к повторам передачи.

С помощью утилит `tracert` и `pathping` можно оценить качество канала связи по всей цепочке до желаемого источника. Утилита `tracert` выводит на экран время отклика каждой системы, находящейся на пути передачи данных к искомому серверу. Точка, после которой время отклика резко увеличено, свидетельствует о наличии в этом месте узкого "горлышка", не справляющегося с нагрузкой.

Более точную усредненную статистику достижимости удаленного хоста можно получить с помощью команды `pathping`. Эта утилита посылает на каждый промежуточный хост серию пакетов и выводит информацию о количестве откликов и среднем времени ответа:

```
C:\pathping www.microsoft.com
Tracing route to www.microsoft.akadns.net [207.46.230.219]
over a maximum of 30 hops:
0 ask-2002.ack.ru [192.168.0.52]
1 frw.ack.ru [192.168.0.12]
2 cisco.ack.ru [195.161.193.254]
3 aa-s0.ekaterinburg.rostelecom.ru [195.161.94.137]
4 aa-sw1.ekaterinburg.rostelecom.ru [195.161.94.5]
5 tschelkun.rt-comm.ru [217.106.6.149]
```

[1] Например, имя www-сервера вашего провайдера.

```
6 aksai.rt-comm.ru [217.106.6.97]
7 msk.rt-comm.ru [217.106.6.81]
8 ..spb.rt-comm.ru [217.106.6.70]
9 213.190.162.5
10 alv2-ge3-0.datanet.tele.fi [192.130.130.61]
11 208.51.142.197
12 ..pos8-0-2488M.cr1.CPH1.gblx.net [62.12.32.73]
13 pos1-0-2488M.cr2.SEA1.gblx.net [64.214.65.242]
14 so1-0-0-2488M.br2.SEA1.gblx.net [64.213.83.182]
Computing statistics for 375 seconds...
Source to Here This Node/Link
Hop RTT Lost/Sent = Pct Lost/Sent = Pct Address
0 ask-2002.ack.ru [192.168.0.52] 0/ 100 = 0% |
1 0ms 0/ 100 = 0% 0/ 100 = 0% frw.ack.ru [192.168.0.12] 0/ 100 = 0% |
2 1ms 0/ 100 = 0% 0/ 100 = 0% cisco.ack.ru [195.161.192.254] 2/ 100 = 2% |
3 637ms 2/ 100 = 2% 0/ 100 = 0% aa-s0.ekaterinburg.rostelecom.ru
[195.161.94.137] 0/ 100 = 0% |
4 613ms 4/ 100 = 4% 2/ 100 = 2% aa-sw1.ekaterinburg.rostelecom.ru
[195.161.94.5] 0/ 100 = 0% |
5 562ms 5/ 100 = 5% 3/ 100 = 3% tschelkun.rt-comm.ru [217.106.6.149] 0/
100 = 0% |
6 605ms 4/ 100 = 4% 2/ 100 = 2% aksai.rt-comm.ru [217.106.6.97] 0/ 100 =
0% |
7 623ms 4/ 100 = 4% 2/ 100 = 2% msk.rt-comm.ru [217.106.6.81] 0/ 100 = 0% |
8 725ms 5/ 100 = 5% 3/ 100 = 3% spb.rt-comm.ru [217.106.6.70] 0/ 100 = 0%
|
9 864ms 2/ 100 = 2% 0/ 100 = 0% 213.190.162.5 0/ 100 = 0% |
10 942ms 2/ 100 = 2% 0/ 100 = 0% alv2-ge3-0.datanet.tele.fi
[192.130.130.61] 1/ 100 = 1% |
11 868ms 3/ 100 = 3% 0/ 100 = 0% 208.51.142.197 0/ 100 = 0% |
12 927ms 3/ 100 = 3% 0/ 100 = 0% pos8-0-2488M.cr1.CPH1.gblx.net
[62.12.32.73] 1/ 100 = 1% |
13 1040ms 4/ 100 = 4% 0/ 100 = 0% pos1-0-2488M.cr2.SEA1.gblx.net
[64.214.65.242] 0/ 100 = 0% |
14 1059ms 4/ 100 = 4% 0/ 100 = 0% so1-0-0-2488M.br2.SEA1.gblx.net
[64.213.83.182] 96/ 100 = 96% |

Trace complete.
```

После опубликования цепочки хостов, через которые проходит сигнал по пути к заданному серверу, программа `pathping` выводит статистические данные о достижимости каждого промежуточного хоста, причем время усреднения выбирается исходя из конкретной ситуации (в примере подсчет проводился за период в 375 с). Первым параметром выводится время доступа к данному хосту, затем показано количество отправленных на него пакетов и число неполученных ответов (с процентом успеха). После этого отображаются анало-

гичные значения для достижимости конечного хоста при расчете прохождения пакетов от данной промежуточной точки. Так, цифры в 14-й строке говорят о том, что время доступа к хосту составляет 1059 мс и при отправке на него 100 пакетов на четыре отсутствовал ответ. А если бы сигнал на конечный хост передавался с позиции номер 14, то при посылке 100 пакетов ответ был бы получен на все. В завершение после имени данного промежуточного хоста утилита сообщила, что количество успешных пакетов составило 96%.

Переустановка протокола TCP/IP в Windows XP

Иногда "последним" средством восстановления работоспособности становится переустановка протокола TCP/IP. Поскольку в Windows XP данный протокол является практически основным компонентом, то пользователь не может его удалить обычными операциями удаления/добавления компонентов.

Чтобы вернуть параметры протокола в первоначальное состояние, следует воспользоваться командой `netsh`. Команда

```
netsh interface ip reset
```

установит настройки протокола TCP/IP в значения по умолчанию.

Настройка серверов WINS, DHCP, DNS

Службы серверов WINS, DHCP, DNS должны быть установлены на компьютер со статическим IP-адресом.

Установка и настройка WINS

Установка WINS крайне проста: достаточно указать эту службу в составе устанавливаемых компонентов Windows Server. Какой-либо последующей специальной настройки служба WINS не требует. Вам необходимо при "раздаче" клиентам настроек протокола TCP/IP указать только адрес сервера со службой WINS, после чего системы при старте автоматически будут регистрироваться в базе WINS. В случае необходимости (она возникает крайне редко) соответствующие записи можно занести вручную, если воспользоваться консолью управления WINS (статические записи).

Если в системе установлено *несколько* WINS-серверов, то необходимо настроить синхронизацию их баз данных. Для этого на каждом WINS-сервере следует указать адрес другого WINS-сервера, с которым нужно проводить синхронизацию данных.

Примечание

Если маршрутизаторы сети пропускают широковещательные сообщения, серверы WINS можно настроить на автоматическое обнаружение партнеров по

синхронизации. Для этого достаточно отметить соответствующую опцию на вкладке дополнительных свойств настройки WINS.

WINS-прокси

Компьютеры используют данные базы WINS только в том случае, если соответствующие настройки определены в их параметрах TCP/IP-протокола. Если вы хотите, чтобы все NetBIOS-компьютеры сети могли воспользоваться WINS для разрешения имен, то следует создать в каждом сегменте сети WINS-прокси.

Компьютеры, не использующие WINS, для разрешения имен рассылают широковещательные пакеты. WINS-прокси, обнаружив такой пакет, пытается разрешить имя в своем кэше и при неудаче передает запрос на тот WINS-сервер, который зарегистрирован для данной системы. Если сервер WINS возвращает имя, то WINS-прокси передает эти данные той системе, которая отправила широковещательный запрос.

Для включения режима прокси необходимо установить в 1 параметр `EnableProxy` в разделе `HKLM\System\CurrentControlSet\Services\NetBT\Parameters` реестра компьютера, который предполагается использовать в роли WINS-прокси.

Настройка DHCP

Использование DHCP-сервера требует от администратора обязательного определения ряда параметров. Для установки службы достаточно отметить ее в перечне параметров Windows Server, но после установки необходимо выполнить как минимум следующие действия:

- ❒ создать и настроить зону;
- ❒ авторизовать DHCP-сервер.

Примечание

При наличии в сети двух DHCP-серверов клиент "возьмет" настройки IP-протокола от того сервера, ответ от которого будет получен первым *(см. разд. "Порядок получения IP-адресов клиентами DHCP" далее в этой главе)*.

Создание и настройка зоны

Сервер начнет раздавать адреса только после того, как вы зададите диапазон этих адресов и определите необходимые параметры протокола. Делается это путем создания новой области (scope).

Примечание

Название области может быть задано произвольно; диапазон адресов менять в процессе работы допустимо, но значение маски подсети, определенное при

создании области, изменить *невозможно*. Можно только удалить область и создать новую с иным значением.

Для области необходимо определить, как минимум, диапазон распределяемых адресов, маску сети и указать срок аренды IP-адреса. Внутри диапазона адресов некоторые адреса можно исключать (например, если вы предполагаете задать их статически). Срок аренды выбирается исходя из особенностей вашей сети. При малом числе компьютеров он может быть существенно увеличен по сравнению со значением по умолчанию в 8 суток (вплоть до неограниченного значения).

Желательно в параметрах DHCP-сервера указать, чтобы он проверял IP-адрес перед его выдачей клиенту. Это позволит предупредить конфликты, возникающие при самостоятельном присваивании IP-адресов у клиентов, а также облегчит ситуацию восстановления сервера (например, после полной очистки его баз).

Примечание

Если в сети предприятия есть компьютеры с операционной системой до Windows 2000, то целесообразно установить в настройках DHCP обязательную регистрацию выдаваемого адреса на сервере DNS независимо от того, установлена данная опция у клиента или нет.

Авторизация DHCP-сервера

DHCP-серверы на операционных системах Windows 200*x*, работающих в составе домена Windows, должны быть *авторизованы*. Если DHCP-сервер не авторизован в службе каталогов, то он не будет выдавать IP-адреса. Чтобы авторизовать сервер, пользователю с правами администратора предприятия необходимо в меню консоли управления DHCP-сервером выбрать пункт **Авторизовать сервер**[1].

Примечание

Если в вашей сети имеется DHCP-сервер, работающий на платформе Windows NT 4.0 Server или на другой операционной системе, то он будет обслуживать клиентов *независимо от авторизации в службе каталогов*.

Настройка параметров области

Для полноценной работы в составе компьютерной сети обычно недостаточно получения только IP-адреса и маски сети. Так, клиентам минимально необхо-

[1] Индикатор, свидетельствующий об авторизации сервера, выдает статус с некоторой (обычно до 5 мин) задержкой. Поэтому после авторизации сервера следует выдержать незначительный промежуток времени и открыть консоль управления снова, чтобы убедиться в полной работоспособности сервера.

димы адреса DNS-серверов и адрес шлюза. Кроме того, могут понадобиться DNS-суффикс существующей сети, адрес WINS-сервера, адрес автоматической конфигурации прокси для доступа в Интернет и т. п. Все эти параметры могут сообщаться DHCP-сервером.

Для этого необходимо определить *опции* области.

Примечание

В последних версиях операционных систем мастер создания области автоматически предлагает заполнить основные параметры. При этом могут быть определены как параметры всего сервера, так и параметры области. Обратите внимание, что в случае конфликта параметров клиентам будут сообщаться параметры не сервера, а области.

Вы можете определить любые параметры области (как минимум, необходимо указать те величины, которые запрашиваются мастером создания новой зоны), а при необходимости — и создать собственные.

Резервирование адресов

DHCP-сервер можно настроить так, чтобы он выдавал клиентам не случайный, а заранее определенный адрес.

Примечание

Автор достаточно часто сталкивался с ситуацией, когда все адреса в локальной сети раздавались на основе резервирования. Администраторы осуществляли такую статическую настройку адресов для того, чтобы сочетать закрепление адресов, свойственное статическому распределению, с возможностью легкой смены таких параметров, как адрес DNS-сервера.

Чтобы настроить резервирование адреса, необходимо знать *MAC-адрес сетевого адаптера*[1] соответствующего клиента. Этот адрес достаточно просто определить, если сначала подключить клиента к сети любым способом (например, назначить адрес вручную или автоматически), после чего воспользоваться утилитой `arp` *(см. разд. "Протокол ARP" ранее в этой главе)*.

Сам процесс резервирования не представляет сложности: достаточно в оснастке управления DHCP-сервером ввести в окне операции резервирования имя клиента и его MAC-адрес.

Примечание

Обратите внимание, что для резервированного клиента DHCP-сервер позволяет установить свои, индивидуальные параметры протокола TCP/IP, отличные от параметров области.

---

[1] Для новых сетевых адаптеров MAC-адрес может быть определен по их упаковке (вторая часть адреса — это серийный номер адаптера).

"Подстройка" DHCP под группы клиентов

Очень часто администраторы сети хотели бы, чтобы часть клиентов получала IP-адреса из одного диапазона, а часть — из другого, возможно, с отличающимися параметрами настройки протокола TCP/IP. Если такие компьютеры расположены в одном сегменте Ethernet-сети (отсутствуют маршрутизаторы), то подобную конфигурацию DHCP-сервера выполнить невозможно (исключая случай разделения клиентов, использующих загрузку с сети, и клиентов, получающих адрес после старта операционной системы; такой результат достигается просто установкой двух DHCP-серверов, один из которых настроен на обслуживание *только* клиентов, загружаемых по сети, а другой — остальных).

При получении широковещательного запроса на выделение адреса сервер *всегда* будет отсылать предложение аренды IP-адреса того сегмента сети, в котором он находится сам.

Примечание

Если сервер имеет несколько сетевых адаптеров, подключенных к различным сегментам сети, то будут использованы параметры настройки адаптера, указанного *первым* в меню настройки дополнительных опций сетевого подключения.

Существует всего несколько возможностей "выделить" различных клиентов, но только для получения отличающихся параметров области (scope option).

Первая возможность — это резервирование клиентов. Для резервированных клиентов можно определить собственные параметры области. Но для создания такого клиента нужно точно знать его MAC-адрес.

Вторая возможность — это разделение клиентов по *классам*: классу вендоров (vendor class) и классу пользователей (user class). Для клиентов класса администратор может настраивать индивидуальные опции DHCP-сервера.

Классы DHCP имеют некоторые отличия определения. В DHCP вендором считается производитель соответствующего программного обеспечения операционной системы. Например, можно разделить клиентов с операционной системой Windows 2000 и операционной системой предыдущих версий. Правда, вы должны руководствоваться лишь теми параметрами, которые заложили сами вендоры. Например, в DHCP-сервере Windows 2000 для клиентов Microsoft можно настроить раздельно только параметры включения/выключения NetBIOS поверх TCP/IP, необходимости освобождения аренды адреса при выключении и метрику шлюза по умолчанию.

Примечание

Администраторы могут добавлять описания классов вендоров в параметры DHCP-сервера, но для этого придется узнать по технической документации необходимые настройки соответствующего производителя.

Использование *пользовательских классов* доступно в серверах DHCP Microsoft, начиная с версии 2000 и выше. Основное отличие от вендорского класса состоит в том, что устанавливать принадлежность к классу могут сами пользователи (с помощью команды `ipconfig /setclassid <имя_подключения> <класс>`). Например, можно применить пользовательские классы для осуществления различной настройки TCP/IP протокола мобильных и стационарных компьютеров.

Конечно, в больших организациях подобную настройку можно включить в образы операционной системы, которая потом будет тиражироваться раздельно по структурам предприятия (например, простым дисковым копированием или путем установки через Remote Installation Service — см. *главу 12, разд. "Клонирование рабочих станций"*). Но для малых организаций применение пользовательских классов, на мой взгляд, не имеет практического значения.

Обслуживание DHCP-сервером других сегментов сети

С помощью одного DHCP-сервера администраторы могут раздавать IP-адреса различным сегментам своей сети[1]. Для этого необходимо на DHCP-сервере создать области с диапазонами адресов, соответствующими этим сегментам, и обеспечить получение DHCP-сервером запросов из другого сегмента сети.

Создание областей с различными диапазонами IP-адресов выполняется типовым образом: вы создаете область и определяете для нее любой желаемый диапазон адресов. Однако раздавать из области адреса, не соответствующие диапазону собственной подсети, DHCP-сервер *не будет*, пока не получит адресованного ему запроса из другого сегмента.

Такие запросы может формировать специальный агент — агент ретрансляции DHCP (DHCP Relay Agent), входящий в состав сервера маршрутизации и удаленного доступа (Routing and Remote Access Server, RRAS).

Принцип работы агента ретрансляции DHCP достаточно прост. Агент прослушивает сеть на наличие пакетов запроса аренды адреса. Если такой пакет получен, то агент ожидает некоторое время (на случай, если в данном сегменте сети есть свой DHCP-сервер, который и обслужит клиента[2]). Если запрос клиента остается необслуженным, то агент ретранслирует запрос в соседние сегменты сети. Если в соседних сегментах есть DHCP-сервер, то он

---

[1] Для соединения сегментов могут использоваться RFC-1542-совместимые маршрутизаторы, которые имеют возможность пропускать пакеты с запросом аренды адреса. Однако обычно такая настройка достаточно трудоемка, требует внимательного анализа конфигурации сети и нечасто применяется на практике.

[2] Таким образом можно повысить отказоустойчивость данного сегмента сети, дублируя локальный DHCP-сервер соответствующей областью на удаленном DHCP-сервере.

получает данный запрос и, поскольку запрос отправлен с адреса другого сегмента сети, предоставляет в аренду адрес именно того диапазона, из которого пришел запрос.

Для установки программного агента ретрансляции достаточно в настройках IP-маршрутизации (**IP Routing**, пункт **General**) соответствующего сервера RRAS выбрать команду создания нового протокола маршрутизации и указать **DHCP Relay Agent**. В настройках агента ретрансляции следует указать IP-адрес DHCP-сервера, на который будут ретранслироваться запросы аренды адреса.

Далее нужно добавить в агент ретрансляции интерфейс (или несколько интерфейсов, если компьютер подключен к нескольким сегментам сети), через который будут пересылаться запросы аренды. Далее при необходимости следует отрегулировать порог ожидания (boot threshold) — время, в течение которого будет ожидаться ответ локального DHCP-сервера, и hop-count threshold — максимальное количество маршрутизаторов, через которые может пройти этот пакет.

Примечание

Агента DHCP Relay следует использовать также в тех случаях, когда сеть разделена маршрутизаторами, не пропускающими широковещательный трафик. Иначе сервер DHCP не сможет получить запрос выделения адреса от клиента, находящегося в другом сегменте локальной сети.

Порядок получения IP-адресов клиентами DHCP

Во многих случаях знание процедуры аренды IP-адреса может помочь в диагностике неисправностей сети.

- **Первичное получение адреса.**

  При включении компьютера клиент, настроенный на динамическое получение адреса, передает широковещательную рассылку с запросом IP-адреса[1]. Это сообщение называется DHCPDISCOVER. На этот запрос отвечают *все* DHCP-серверы сегмента сети, предлагая IP-адрес. Соответствующее сообщение называется DHCPOFFER. Выделяемые для аренды адреса на некоторый период резервируются и не предлагаются другим клиентам.

  Клиент ждет предложения по адресу от сервера DHCP одну секунду. Если оно не приходит ни от одного сервера, то запрос аренды повторяется еще пять раз (через увеличивающиеся промежутки времени приблизительно в течение 30 секунд). Если ответ от DHCP-сервера так и не получен, то кли-

[1] Запрос идет от адреса 0.0.0.0 с маской 255.255.255.255.

ент получает адрес по технологии APIPA *(см. разд. "Адресация APIPA" ранее в этой главе)*.

На *первое* полученное предложение от DHCP-сервера клиент отвечает широковещательным сообщением (DHCPREQUEST), в котором содержится IP-адрес сервера, выдавшего это предложение. После получения такого сообщения *другие* DHCP-серверы освобождают зарезервированные ими IP-адреса, а сервер, предложение которого принято, высылает подтверждение (DHCPACK). Только после получения этого подтверждения клиент полностью инициализирует TCP/IP-протокол своего сетевого адаптера.

- **Продление аренды.**

Запрос на продление аренды IP-адреса высылается после истечения половины периода аренды и при каждой перезагрузке системы. Для этого на сервер, выдавший адрес, отправляется DHCPREQUEST-запрос. Если подтверждение получено (DHCPACK), то клиент продолжает использовать текущие параметры конфигурации. Если ответ не получен, то запросы на данный сервер повторяются. Перед окончанием срока аренды и при отсутствии ответа от выдавшего IP-адрес DHCP-сервера клиент высылает уже широковещательные запросы DHCPDISCOVER, пытаясь получить адрес от *любого* DHCP-сервера.

Примечание

При отказе в аренде DHCP-сервером высылается специальный пакет DHCPNACK.

Если срок аренды закончился, а клиент не смог ни получить подтверждения от "своего" DHCP-сервера, ни запросить новый IP-адрес, то *текущие настройки IP-протокола освобождаются*, а клиент получает адрес по APIPA.

Если при перезагрузке операционной системы попытка обновления аренды адреса неудачна и клиент не может установить связь со шлюзом по умолчанию[1], то текущие настройки IP-адреса также освобождаются.

Диагностика и обслуживание DHCP-сервера

Обычно никаких проблем с использованием DHCP-сервера не возникает. В противном случае следует включить протоколирование его работы (опция на одной из вкладок консоли управления сервером). После выявления причин

[1] Такая ситуация может свидетельствовать о переносе компьютера в другой сегмент сети, поэтому он освобождает свой адрес.

неисправностей для повышения производительности системы ведение журнала работы DHCP-сервера следует отключить.

Сервер проводит фоновую дефрагментацию базы данных клиентов. Ручная *(офлайновая)* дефрагментация имеет смысл только в случае большой нагрузки на серверы (более 1000 записей клиентов). При меньшем числе клиентов ручную дефрагментацию (она проводится при помощи программы `jetpack`; которая требует предварительной остановки DHCP-сервера) рекомендуется проводить раз в несколько месяцев или еще реже.

При возникновении ошибок в базе достаточно просто исполнить операцию `reconcile` для соответствующей области или всего сервера. При серьезных проблемах допустимо остановить DHCP-сервер и удалить все файлы баз из его каталога. После старта они будут воссозданы с пустыми значениями, которые потом снова заполнятся по получении запросов.

Примечание

Для DHCP-серверов существует возможность переноса их с одного компьютера на другой с сохранением всех настроек (областей и их параметров, реальной базы клиентов). Поможет в этом утилита dhcpexim.exe (ее можно свободно загрузить с сайта разработчика операционной системы — **http://www.microsoft.com/windows2000/techinfo/reskit/tools/new/dhcpexim-o.asp**), позволяющая сохранить все параметры настройки DHCP-сервера в файл, а потом восстановить эти настройки на другом DHCP-сервере. В случае использования Windows Server 2003 перенос данных DHCP-сервера может быть выполнен при помощи операций экспорта и импорта утилиты `netsh`.

Отказоустойчивая конфигурация Microsoft DHCP-сервера

При построении отказоустойчивых информационных систем важно обеспечить стабильную работу сетевых служб, в том числе сохранить функционирование службы автоматического присвоения параметров IP-адреса в случае выхода сервера DHCP из строя. Реализация DHCP на основе сервера Microsoft имеет серьезный недостаток, связанный с невозможностью создания горячего резерва данной службы для одного диапазона IP-адресов.

Документы Microsoft предлагают для повышения отказоустойчивости два способа. Первый заключается в размещении службы DHCP на серверном кластере. В этом случае база адресов будет храниться на общем диске, а при выходе из строя одного сервера его работу "подхватит" второй сервер кластера. К сожалению, такое решение часто не доступно малым и средним организациям из-за высокой стоимости реализации отказоустойчивого кластера.

Второй вариант решения проблемы отказоустойчивости службы DHCP заключается в настройке для организации *двух* серверов DHCP с *различными* (неперекрывающимися) частями используемого диапазона адресов организа-

ции. В этом случае клиент будет получать параметры адреса от любого сервера (вернее, от того, который ответит раньше), а при выходе из строя одного из серверов второй продолжит обслуживание организации.

DNS

В доменах Windows информация о необходимых для работы систем службах хранит DNS. И основное количество проблем функционирования домена (службы каталогов) связано именно с неверной настройкой администраторами службы DNS. Поэтому стоит рассмотреть сервер DNS более подробно.

Термины DNS

DNS (Domain Name System, система доменных имен) — это служба разрешения имен в сетях на основе протокола TCP/IP.

- **Зоны DNS.**

  Зона DNS — это часть пространства имен, для которого DNS-сервер может выполнять операции разрешения имен. Существуют зоны прямого и обратного просмотра, которые на практике для удобства называют *прямой* и *обратной* зонами.

  Прямая зона позволяет по имени системы получать ее IP-адрес, *обратная* — по IP-адресу "выдает" информацию об имени хоста. Поэтому если нужно по имени компьютера узнать его адрес, то говорят о *прямом разрешении имени*. Если по IP-адресу хотят получить имя компьютера, то в этом случае происходит *обратное разрешение имени*. Строго говоря, если в DNS зарегистрировано прямое разрешение имени, то должно быть зарегистрировано и обратное.

Примечание

Отсутствие обратного разрешения имени является достаточно частой ошибкой в Интернете. Обычно владельцами прямой зоны данного домена и обратной зоны, которая соответствует этому имени, являются разные люди (организации), поэтому в процессе регистрации новых DNS-записей часто забывают создать соответствующую запись обратной зоны.

Фактически прямые зоны соответствуют доменам некоторого уровня. Например, зона ask.ru позволяет разрешить все запросы имен, относящихся к домену ask.ru.

Для разрешения обратных имен в домене самого верхнего уровня создана зона in-addr.arpa. Названия зон обратного просмотра формируются добавлением к этому имени слева имени трех октетов адреса сети в обратном порядке. Например, для сети 195.161.192.0/24 имя обратной зоны будет 192.161.195.in-addr.arpa.

В большинстве случаев отсутствие регистрации в обратной зоне не мешает нормальной работе в Сети. Однако оно может и привести к ошибкам в тех случаях, когда необходимо установить по IP-адресу имя сервера. Например, при обмене почтовыми сообщениями в настоящее время принято проверять принадлежность сервера к тому домену, от имени которого он передает почту. Если обратное разрешение имени не будет проведено, то система может получить отказ в приеме почты.

- **Первичная и вторичная зоны.**

  У создаваемых записей DNS должен быть один "хозяин". Чтобы все записи были корректны, их необходимо вносить на одном DNS-сервере. В этом случае говорят, что на таком DNS-сервере расположена первичная зона. Для отказоустойчивости на других серверах можно создать копии этой зоны: такие зоны будут называться вторичными зонами. Вторичная зона содержит те же записи, что и первичная, но в нее нельзя вносить изменения или добавлять новые записи. Эти операции можно делать только[1] для первичной зоны.

- **Серверы имен зоны.**

  Для каждой первичной зоны можно создать сколько угодно копий на других серверах. Обычно в настройках DNS-серверов предусматриваются специальные механизмы оповещений, которые обеспечивают синхронность записей первичной зоны и ее копий на вторичных серверах. Но, если это не запрещено настройками DNS-сервера, вы можете создать на своем сервере вторичную зону, обновления которой будут производиться по некоему графику. В результате записи такой копии могут оказаться неактуальны. Поэтому принято для домена определять серверы имен, информация которых "официальна". Такие серверы называют NS-записями соответствующего домена. Обычно для каждого домена создается два или три NS-сервера. Если ответ на запрос разрешения имени получен от NS-сервера, то он считается авторизованным, другие серверы возвращают неавторизованные ответы.

Примечание

Это не значит, что в этом случае возвращаются неверные данные. DNS-сервер разрешит запрос клиента на основании данных своей копии только в том случае, если эти данные не устарели. Но если срок жизни записей на сервере имен был установлен, например, равным неделе, то в случае внесения изменений в первичную зону необходимо быть готовым к тому, что еще до недели после смены информации на NS-сервере другие серверы DNS могут возвращать ста-

[1] В случае домена Windows 200*x* и использования зоны DNS, интегрированной со службой каталогов, изменения можно вносить на любом DNS-сервере такой зоны.

рые значения. То есть вы столкнетесь с ситуацией, когда часть систем уже получила правильные данные об имени, а часть — нет. Поэтому перед предполагаемой сменой записей DNS необходимо уменьшить время их жизни и выждать период, равный старому времени жизни. Это позволит сократить период такой неопределенности в разрешении имен. После выполнения операции настройки следует вернуться к старым величинам, чтобы снизить нагрузку на сеть и DNS-серверы.

Если вы предполагаете, что копия DNS-записей на сервере DNS неактуальна, то следует выполнить операцию *очистки кэша* для соответствующей зоны. Для этого необходимо в консоли управления сервером включить опцию отображения дополнительных параметров, найти нужную зону среди структуры кэша и выполнить для нее очистку. При следующем запросе данных из этой зоны сервер загрузит копию с того сервера DNS, на который настроена пересылка запросов. Поэтому и эта операция также не гарантирует получение актуальной копии записей. При рассмотрении проблемных ситуаций следует выяснить на официальных ресурсах адреса NS-серверов данного домена и проверить записи с помощью утилиты `nslookup`, подключаясь к соответствующему NS-серверу *(см. разд. "Обслуживание и диагностика неисправностей DNS-сервера" далее в этой главе)*.

Примечание

Для обновления записей DNS на клиентских компьютерах следует очистить кэш DNS-записей (`ipconfig /flushdns`).

- **Передача зон.**

  Так называется специальная операция копирования всех записей данной зоны с одного DNS-сервера на другой. По соображениям безопасности передача зон обычно разрешается только на заранее определенный администратором системы список IP-адресов DNS-серверов. Если операция передачи зоны запрещена, то вы не сможете создать на своем DNS-сервере вторичную зону для данного домена.

- **Делегирование зон.**

  Если на DSN-сервере создана, например, прямая зона для домена test.local, то запись о домене третьего уровня level3.test.local должна содержаться на этом же сервере. Если географически домен level3.test.local удален от основного домена, то поддержание записей в его зоне на DNS-сервере становится не очень удобным. Проще поручить администратору этого домена вносить изменения в DNS-записи самостоятельно, для чего используется процесс делегирования зоны. При делегировании зоны DNS-сервер создает у себя запись, указывающую, что запросы разрешения имени для этой зоны должны перенаправляться на другой DNS-сервер, на который произведено делегирование зоны.

- **Stub-зона (зона-заглушка).**

  При делегировании зоны на исходном сервере сохраняется информация о NS-сервере делегированной зоны. Поскольку администратор делегированной зоны может изменять ее DNS-записи, то он может сменить и записи NS-сервера. Если соответствующее изменение не будет внесено на сервер, который осуществляет делегирование, то процесс разрешения имен будет нарушен (основной сервер по-прежнему будет отправлять запросы на уже не существующий адрес, и в результате будет формироваться неверный ответ).

  Для исправления подобной ситуации в DNS-сервере Windows Server 2003 введены *stub-зоны*. При создании stub-зоны в ней определяются NS-записи делегированной зоны. Причем если администратор делегированной зоны меняет эти записи, то соответствующие изменения вносятся и в записи stub-зоны. В результате гарантируется целостность процесса разрешения имен.

- **Зона "точка".**

  Домен самого верхнего уровня, как уже писалось, принято называть именем "точка". Если в DNS создать зону "точка"[1], то это будет фактически означать, что данный сервер является корневым в структуре DNS *(см. следующий раздел)*, т. е. он должен разрешать самостоятельно любые запросы имен. Если этот DNS-сервер не может разрешить имя, то его ответ будет гласить, что такого хоста не существует.

Примечание

При необходимости пересылки запросов DNS на другие серверы зону "точка" следует удалить, после чего появится возможность настройки пересылки запросов DNS.

Порядок разрешения имен в DNS

- **Типы запросов.**

  Для разрешения имен в DNS предусмотрено два типа запросов: итеративный и рекурсивный.

  Итеративный запрос служит для получения от DNS-сервера, которому он направлен, наилучшего ответа, который может быть получен *без обращения* к другим DNS-серверам. *Рекурсивный запрос* предполагает, что сервер DNS должен выполнить все операции для разрешения имени. Обычно для

[1] Зона с таким именем создается при установке службы каталогов с одновременной установкой и настройкой сервера DNS.

этой цели необходимо выполнить несколько запросов к различным серверам DNS.

- **Последовательность разрешения DNS-имен.**

  Процесс определения имени с использованием итеративных запросов весьма трудоемок. Нужно найти NS-сервер для данного домена и затем запросить от него данные по требуемому имени. Обычно клиенты все эти операции "возлагают" на DNS-серверы, отправляя им рекурсивный запрос.

  DNS-сервер после получения рекурсивного запроса просматривает собственный кэш имен. Если он находит нужную запись и она еще не устарела, то это значение возвращается клиенту. Если записи нет, то сервер предпринимает попытку поиска сервера имен для домена, содержащегося в запросе. Чтобы найти такой сервер, запрос *всегда* отправляется на корневой сервер, от него получают информацию по домену первого уровня, запросом на домен первого уровня получают информацию о NS-серверах домена второго уровня и т. д. После этого отправляется итеративный запрос на NS-сервер соответствующего домена. Естественно, что большинство информации от корневых доменов уже кэшировано[1] на данном сервере. В результате запросы "не доходят" до корневых серверов, но сама цепочка разрешения имени *всегда выполняется от корня* до текущего домена.

  Обычно администраторы локальных DNS-серверов настраивают свой сервер на пересылку (forwarding) запросов разрешения имен на тот или иной сервер DNS (обычно это DNS-сервер провайдера). Тем самым вся процедура разрешения имен будет выполняться уже другим сервером. Поскольку мощные серверы Интернета обычно имеют существенно больший кэш и лучший канал подключения к глобальной сети, то таким способом достигается уменьшение времени ответа и снижение трафика.

Основные типы записей DNS

При создании первичной зоны для своего домена следует обратить внимание на создание некоторых специальных записей ресурсов (resource records), которые полезны для получения информации общего типа:

- **SOA (Start of Authority).**

  Серийный номер зоны. В DNS автоматически увеличивается при *любом* изменении записей зоны. Используется в операциях переноса зон (если номер изменился, то происходит обновление записей вторичной зоны). На практике принято этот номер формировать на основе даты последнего изменения: год-месяц-день-(время). Например, так: 20050810.

---

[1] Этим резко снижается нагрузка на сеть и уменьшается время ответа на запрос.

- **NS (Name Server).**

  Адреса "официальных" серверов имен данной зоны. Эти серверы возвращают *авторизованные* ответы.

- **RP (Responsible Person).**

  Адрес электронной почты лица, ответственного за внесение изменений в записи зоны. Наличие записи и поддержание ее актуальности желательно, чтобы в случае возникновения каких-либо вопросов по домену организации у специалистов были реальные контактные данные. Обратите внимание, что символ @ адреса электронной почты заменяется на точку.

- **A (Host Address).**

  Эта запись содержит информацию об имени системы и ее IP-адресе. Именно этот тип записи добавляется в DNS-сервер при регистрации хостов.

- **PTR (Pointer, указатель).**

  Так называется запись в обратной зоне. Настройками DNS локальных доменов обычно предусматривается автоматическое создание (изменение) PTR-записи при добавлении A-записи в прямую зону.

- **CNAME (Canonical NAME).**

  Записи псевдонима. Используются, если хосту необходимо дать второе DNS-имя.

- **MX (Mail eXchanger).**

  Запись хранит IP-адрес сервера электронной почты (SMTP-сервера), который обслуживает данный домен. Чтобы на данный домен можно было отправлять электронную почту, в базе DNS для домена должна быть обязательно создана MX-запись. В целях резервирования может быть создано несколько MX-записей, причем каждой записи соответствует определенный *вес*. По умолчанию почта отправляется на адрес, содержащийся в MX-записи с наименьшим весом. Если этот сервер не отвечает, то делаются попытки отправить почту на адреса, соответствующие MX-записям с другими весами в порядке их возрастания.

- **SRV (Запись службы).**

  Специальный тип записи, используемый для обнаружения в домене служб (например, службы IP-телефонии и т. п.). Записи о системных службах Windows автоматически создаются службой каталогов. Ручное добавление записей осуществляется при настройке дополнительных продуктов в соответствии с прилагаемой технической документацией.

Примечание

Кроме описанных существуют и другие типы записей, предназначенные, например, для DNSSEC, IPv6 и т. п., но мы не будем их касаться в этой книге.

Установка сервера DNS

Сервер DNS можно установить только на компьютер со статическим IP-адресом. При этом удостоверьтесь, что сервер DNS, который предназначается для обслуживания организации, может правильно разрешать *неполные* имена. То есть он должен сообщить правильный адрес как на запрос для test.mydomain.local, так и для запроса на имя test. Для этого необходимо, чтобы основной DNS-суффикс компьютера, на котором устанавливается сервер DNS, совпадал с суффиксом имени домена организации. Соответствующие настройки выполняются в параметрах TCP/IP-протокола, статически устанавливаемых для сетевого адаптера сервера DNS.

Для установки службы DNS-сервера достаточно выбрать соответствующую опцию среди добавляемых компонентов. В целях отказоустойчивости информационная система должна быть настроена на использование нескольких серверов DNS.

Примечание

Сетевые адаптеры контроллеров домена, на которых установлены DNS-серверы, следует настроить "перекрестно": в качестве первого сервера DNS для адаптера первого контроллера указывается адрес DNS-сервера второго контроллера и наоборот.

После запуска службы DNS следует уточнить некоторые параметры настройки. Во-первых, если сервер должен разрешать имена сети Интернет, то следует удалить зону "точка" (если такая создана при установке) и указать IP-адреса тех серверов DNS, на которые будут пересылаться запросы разрешения имен. Обычно в качестве таковых указываются DNS-серверы провайдера.

Примечание

DNS-сервер Windows Server 2003 позволяет определить для перенаправления запросов различные внешние DNS-серверы в зависимости от зон. Эту опцию целесообразно использовать при наличии нескольких подключений к Интернету и/или к удаленным офисам.

Далее следует создать на сервере DNS необходимые зоны. Эта операция выполняется при помощи соответствующего мастера. Следует учесть, что если сервер предназначен для разрешения имен домена Windows и является контроллером домена, то оптимальным решением будет создание зоны, *интегрированной со службой каталогов*. Такой вариант позволит использовать службы Windows для репликации данных между серверами DNS. При этом

зона DNS на *каждом* сервере фактически будет являться первичной (допускать внесение изменений), а сами данные — безопасными (при работе с зоной будет использована действующая в Windows система безопасности).

Интегрированная в службу каталогов система имен реплицируется в Windows 200*x* по всем контроллерам домена. Начиная с Windows Server 2003, добавлена возможность размещения зоны DNS в *собственных разделах каталога*. Это позволяет реплицировать интегрированные в службу каталогов зоны *только* на серверы DNS либо домена, либо леса, в зависимости от того, какой раздел[1] вы создаете, исходя из структуры организации.

Для зон, обслуживающих домен Windows, обязательно должна быть включена опция динамического обновления. В целях безопасности следует выбрать вариант безопасных динамических обновлений записей. При этом рекомендуется, чтобы служба DHCP была настроена на запуск не от системной учетной записи, а от имени специально созданного для такой цели пользователя.

Если вы не хотите регистрировать всех клиентов в DNS, то можно настроить сервер DNS так, чтобы он перенаправлял неразрешенные запросы имени на WINS-сервер. Для этого в настройках DNS-сервера в свойствах зоны на вкладке **WINS** следует включить опцию пересылки запросов на WINS-сервер и указать соответствующие IP-адреса.

После установки и настройки основных параметров DNS-сервера необходимо выполнить его первичную проверку. Для этого следует в свойствах сервера на вкладке мониторинга включить опции проверки как работы самого сервера, так и правильности перенаправления запросов и провести тест, после чего проверить корректность разрешения имен как внутренней сети, так и внешней (если сервер DNS используется и для разрешения имен Интернета) с помощью команды `nslookup` *(см. разд. "Обслуживание и диагностика неисправностей DNS-сервера" далее в этой главе)*.

Примечание

При создании домена одновременно с установкой DNS прямая зона создается автоматически. Зону обратного разрешения следует создать вручную.

Записи домена Windows

Если на сервере DNS зарегистрирована зона, соответствующая домену Windows, то в этой зоне должны присутствовать специализированные записи, которые определяют нахождение служб каталогов домена. Данные записи создаются автоматически через некоторое время после установки службы каталогов.

---

[1] Создание такого раздела выполняется из оснастки управления сервером DNS (соответствующая команда меню сервера).

Эти записи используются для нахождения служб, отвечающих за функционирование как домена, так и всего леса, поэтому все компьютеры леса должны иметь возможность разрешать имена в зоне _msdcs.<имя_домена>. Поскольку в Windows 2000 интегрированная зона DNS реплицируется *только внутри домена*, то администратору следует принять меры, обеспечивающие доступность зоны _msdcs.<имя_домена> во всех доменах организации. Возможный вариант — это замена зоны _msdcs внутри зоны <имя_домена> на делегированную зону, и размещение новой зоны _msdcs.<имя_домена> на этом же сервере DNS с последующей настройкой ее вторичных зон на всех серверах DNS организации.

Разделение DNS

Все большее число сотрудников начинают использовать мобильные компьютеры для доступа к ресурсам организации как изнутри локальной сети, так и из Интернета. В целях сокращения затрат на изменение конфигураций персональных компьютеров следует выполнять настройки программного обеспечения так, чтобы доступ к сетевым ресурсам локальной сети осуществлялся *единообразно*, независимо от того, выполняется подключение из локальной или глобальной сети. Реализуется такое требование *разделением DNS* (DNS split).

Технология разделения DNS подразумевает, что разрешение имен локальной сети и Интернета для *одного доменного имени* настраивается на *различные DNS-серверы*. Суть решения будет понятна из рассмотрения двух возможных ситуаций.

Примечание

Мы не рассматриваем вариант использования ресурсов локальной сети через VPN-подключение, поскольку в этом случае удаленный компьютер фактически становится членом локальной сети.

- **Одинаковые имена локального домена и домена Интернета.**

  Если имя домена Windows совпадает с именем домена Интернета, то единственная необходимая операция — это правильная настройка публикации внутренних ресурсов в глобальной сети. Когда клиент локальной сети пытается получить доступ к каким-либо ресурсам, он запрашивает их месторасположение у *локального, внутреннего* сервера DNS. Этот сервер возвращает клиенту внутренний адрес ресурса, к которому и осуществляется подключение (рис. 3.13).

  На сервере DNS, обслуживающем домен Интернета этой же организации, необходимо настроить A-запись соответствующего ресурса на *внешний адрес* брандмауэра данной организации, а на брандмауэре настроить пуб-

ликацию внутреннего ресурса таким образом, чтобы запрос, приходящий на брандмауэр и адресованный на данное имя, перенаправлялся на локальный адрес ресурса.

В результате, независимо от точки подключения, запрос клиента всегда будет доставлен на один и тот же локальный ресурс системы.

При использовании технологии разделения DNS клиент локальной сети и компьютер Интернета при разрешении одного и того же имени будут обращаться к различным DNS-серверам. В результате локальный клиент будет обращаться по локальному адресу, а клиент Интернета перешлет запрос на брандмауэр организации, который и перенаправит его на локальный адрес запрашиваемого ресурса.

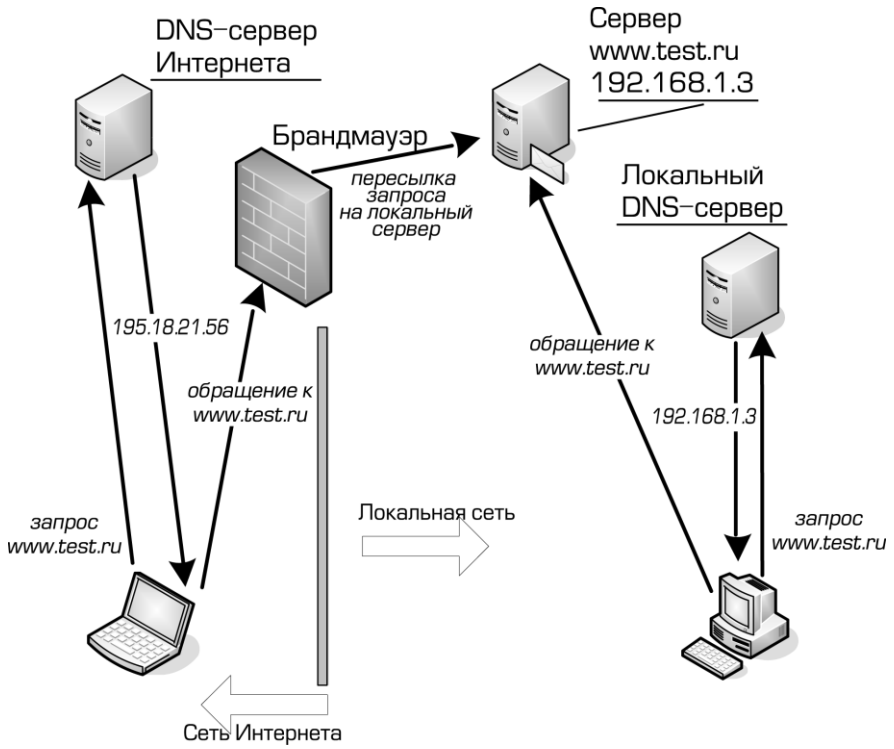


Рис. 3.13. Разделение DNS

- **Различные имена локального домена и домена Интернета.**

  Если "внутреннее" и "внешнее" имена домена организации не совпадают, то на внутреннем сервере DNS необходимо создать первичную зону для домена с "внешним" именем. Далее в этой зоне следует создать записи, соответствующие именам систем, предоставляющих необходимые служ-

бы[1], причем в качестве IP-адресов этих записей должны быть указаны *локальные* IP-адреса систем. Таким образом, на внутренних DNS-серверах будет по две зоны: зона, соответствующая "внутреннему" домену Windows (реальные внутренние названия компьютеров локальной сети), и зона с "внешним" именем (фактически содержащая синонимы, вторые имена только для компьютеров, публикующих ресурсы в глобальной сети). Так же, как и в предыдущем примере, следует настроить публикацию внутренних ресурсов на брандмауэре организации.

Клиентов необходимо настроить (в том числе и в локальной сети) на подключение к ресурсам по *внешним именам*. Если клиент обратится к почтовому серверу *изнутри* организации, то он запросит *внутренний* сервер DNS об адресе, соответствующем внешнему имени почтовой системы. Поскольку на внутреннем сервере DNS существует одноименная первичная зона, то сервер будет считаться авторизованным для ответов и сообщит клиенту *внутренний адрес* почтовой системы. Произойдет подключение по локальному адресу системы.

А если, например, клиенту необходимо обратиться к этому же почтовому серверу из Интернета, то он запросит внешний сервер DNS, получит от него адрес брандмауэра и отправит запрос на него. Брандмауэр, получив запрос, проанализирует его и перешлет на локальный адрес почтовой системы.

- **Настройка удаленных офисов.**

Возможны различные варианты конфигурации разрешения имен для удаленных офисов. В наиболее часто используемом случае подключения удаленного офиса к основному через Интернет по VPN-каналу можно реализовать следующую настройку DNS. DNS-сервер удаленного офиса настроить на пересылку запросов разрешения имени на DNS-сервер интернет-провайдера, а пересылку запросов на разрешение внутренних имен настроить на DNS-сервер центрального офиса. Такая конфигурация легко реализуется на DNS-серверах Windows Server 2003. В случае использования DNS на базе Windows 2000 можно осуществить передачу внутренней зоны на DNS-сервер удаленного офиса.

Примечание

Ресурсом, для которого наиболее часто приходится реализовывать подключение пользователей как изнутри организации, так и снаружи, является почтовая система. Если в организации установлен MS Exchange Server и клиенты применяют MS Outlook (полной версии), то для локального подключения к почтовой системе по умолчанию применяется протокол RPC. Подключение по этому про-

[1] Естественно, что изменение записей этой зоны должно выполняться только вручную.

токолу использует динамическое открытие портов на сервере, что вызывает серьезные сложности в настройке брандмауэра при подключении клиента Outlook из глобальной сети. В результате на практике такое подключение из Интернета фактически не использовалось. Начиная с Windows Server 2003, для реализации всей функциональности полной версии Outlook предназначена специальная технология создания RPC Proxy, которая подробно описана в документах базы данных Microsoft (см. документ "Exchange Server 2003 RPC over HTTP Deployment Scenarios" или KB 833401). Обратите внимание, что одновременно следует настроить и клиента Outlook так, чтобы по умолчанию для подключения к почтовому серверу Exchange использовался вариант RPC over HTTP (статья "Configuring Outlook 2003 for RPC over HTTP").

Обслуживание и диагностика неисправностей DNS-сервера

Самый простой способ проверить работоспособность сервера — включить опции мониторинга на соответствующей вкладке консоли управления. Вы должны получить положительную диагностику при тестировании самого сервера и ответа от сервера, на который настроена пересылка запросов.

Сервер DNS ведет протокол своих основных событий в специальном журнале — DNS-сервер (доступен с помощью программы Просмотр событий). В этом журнале по умолчанию фиксируются только основные события (старт или остановка службы, серьезные ошибки: невозможность передачи зоны и т. п.). Если необходимо подробно проанализировать работу сервера, то можно включить крайне детализированный протокол — установить опции *ведения журнала отладки* на соответствующей вкладке консоли управления сервером DNS. Но использовать эту возможность следует *только* на период отладки. В журнал по умолчанию заносится вся информация (подробно — все данные пакетов), что негативно сказывается на производительности сервера.

Универсальная утилита, которую можно использовать для получения данных с любого DNS-сервера (и, соответственно, проверки его работоспособности), — это `nslookup`. Она по умолчанию присутствует среди утилит в системах с установленным протоколом TCP/IP.

Утилита `nslookup` позволяет вручную получить от сервера DNS такую же информацию, какую системы получают в автоматическом режиме при разрешении имен. Поэтому она часто используется при диагностике систем.

После запуска утилиты осуществляется подключение к серверу DNS, указанному в настройках сетевого адаптера по умолчанию. Далее в режиме командной строки можно получить ответ на запрос к любому DNS-серверу.

Рассмотрим пример использования программы `nslookup` (строки, вводимые пользователем, отмечены знаком в начале строки >).

```
>nslookup
Default Server: ack
Address: 192.168.0.10
```

Примечание

После запуска программа выдала сообщение, что подключена к DNS-серверу ack с IP-адресом 192.168.0.10.

```
>server ns.unets.ru
Default Server: ns.unets.ru
Address: 195.161.15.19
```

Примечание

В окне программы `nslookup` была введена команда подключения к DNS-серверу **ns.unets.ru**. В ответ программа сообщила, что подключилась к этому серверу и сообщила его IP-адрес.

```
>uzvt.ru
Server: ns.unets.ru
Address: 195.161.15.19

Non-authoritative answer:
uzvt.ru nameserver = ns.isp.ru
uzvt.ru nameserver = ns.e-burg.ru
ns.e-burg.ru internet address = 195.12.66.65
```

Примечание

Пользователь ввел запрос на разрешение имени **uzvt.ru**. Утилита сообщила, что сервер **ns.unets.ru** предоставил неавторизованную информацию (Non-authoritative answer) об этом имени. Из того, что сервер "вернул" данные NS-записей, следует, что **uzvt.ru** — это домен Интернета, что его серверы имен — **ns.e-burg.ru** и **ns.isp.ru**.

```
>set type=mx
>uzvt.ru
Server: ns.unets.ru
Address: 195.161.15.19

Non-authoritative answer:
uzvt.ru MX preference = 50, mail exchanger =
relay.utnet.ru
uzvt.ru MX preference = 10, mail exchanger = mail.uzvt.ru

uzvt.ru nameserver = ns.isp.ru
uzvt.ru nameserver = ns.e-burg.ru
mail.uzvt.ru internet address = 195.12.67.218
relay.utnet.ru internet address = 195.209.191.2
ns.e-burg.ru internet address = 195.12.66.65
```

Примечание

Следующими командами пользователь определил, что ему нужна информация о почтовых серверах (`set type=mx`), и вновь указал в запросе тот же домен (**uzvt.ru**). Утилита вернула от сервера DNS ответ, что для домена зарегистрированы два почтовых сервера с разными приоритетами (**mail.uzvt.ru,** приоритет 10 и **relay.utnet.ru**, приоритет 50), и сообщила их адреса. Поскольку **mail.uzvt.ru** имеет меньший приоритет, то именно по этому адресу и будет направляться электронная почта для домена **uzvt.ru**.

Для проверки разрешения имен DNS почтового сервера MS Exchange используется специальная утилита, которую необходимо загрузить с сайта Microsoft — `dnsdiag`. Эта программа должна быть запущена на компьютере почтового сервера из папки информационного сервера (IIS).

Выходная информация программы полностью соответствует тем данным, которые получает почтовый сервер в процессе разрешения имен. Эта информация может помочь в диагностике проблемных ситуаций.

Рассмотрим пример использования утилиты `dnsdiag`.

Примечание

В примере вызова утилиты после параметра `v` стоит цифра 1. Это номер виртуального сервера, соответствующего почтовому серверу (может быть иным в зависимости от конфигурации системы).

```
c:\WINNT\system32\inetsrv>dnsdiag mail.ru -v 1
mail.ru is an external server (not in the Exchange Org).
No external DNS servers on VSI. Using global DNS servers.
Created Async Query:
------------
QNAME = mail.ru
Type = MX (0xf)
Flags =  UDP default, TCP on truncation (0x0)
Protocol = UDP
DNS Servers: (DNS cache will not be used)
192.168.0.32
192.168.0.10

Connected to DNS 192.168.0.32 over UDP/IP.
Received DNS Response:
------------
Error: 0
Description: Success
These records were received:
mail.ru    MX    10    mxs.mail.ru
mxs.mail.ru    A    194.67.23.20
```

```
Processing MX/A records in reply.
Sorting MX records by priority.

Target hostnames and IP addresses
------------
HostName: "mxs.mail.ru"
194.67.23.20
```

Утилита сообщила параметры MX-записи для домена **mail.ru** и необходимую дополнительную информацию.

Перенос записей зон

Информация зон DNS домена может быть экспортирована в обычный текстовый файл. Таким способом можно легко вручную перенести зону DNS с одного сервера на другой (например, при модернизации платформы или после какого-либо восстановления).

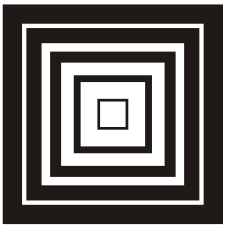
Отказоустойчивость системы DNS доменов Microsoft

В домене Windows легко можно создать несколько серверов DNS, каждый из которых будет первичным сервером для зоны организации: достаточно выбрать вариант интеграции зоны в службу каталогов. Хотя это и создает резервирование службы DNS, однако основная проблема заключается в клиентах Windows. На практике в случае выхода из строя сервера DNS, который указан в качестве *первой* записи в настройке параметров IP-протокола рабочей станции Windows, последняя *не может* переключиться на использование второго сервера. Ситуацию спасает перезагрузка рабочей станции, но такое решение недопустимо для систем, требующих непрерывной работы.

Учитывая вышесказанное, как и для службы DHCP, отказоустойчивым вариантом исполнения службы DNS является реализация ее на кластере серверов.

Примечание

Существуют, естественно, и другие варианты отказоустойчивого решения. Например, использование оборудования аппаратной балансировки запросов. В нормальных условиях такое устройство равномерно распределяет запросы DNS к нескольким серверам, а в случае выхода из строя одного из них просто блокирует работу с ним. Подобные решения обычно используются в публичных информационных системах, обслуживающих большое число пользователей (десятки и сотни тысяч одновременных запросов).



ГЛАВА 4

Компьютерные сети малых предприятий

В малых предприятиях с небольшим числом компьютеров к функционированию сети не предъявляется особых требований. Обычно нужно получить доступ к файлам на диске другого компьютера, распечатать документ на общем принтере и выйти в Интернет. Сотрудники хорошо знают друг друга, и не возникает необходимости разделения прав доступа к каким-либо ресурсам и т. п. Такие сети принято называть *домашними*.

Домашние сети

Самая простая организация такой сети может быть выполнена на рабочих станциях Windows 9*x*; особой причины использовать системы на базе Windows NT (Windows 2000/XP/Vista) нет (если, конечно, это не требуется прикладным программным обеспечением). В этом случае необходимо только осуществить прокладку локальной сети, установить рабочие станции и предоставить ресурсы для совместного использования. Обычно все эти шаги не вызывают сложностей даже у не очень подготовленного пользователя.

Для работы в Интернет можно использовать любые программы маршрутизации, которые легко найти в глобальной Сети, причем доступны и бесплатные версии. Можно использовать и совместный доступ, предусмотренный в Windows *(см. разд. "Совместное использование интернет-подключения" главы 8)*.

С целью упрощения настроек можно использовать протокол NetBEUI. Сразу после включения[1] компьютеры будут нормально функционировать в сети без какого-либо дополнительного вмешательства администратора. Чтобы работать в Интернете, нужно просто добавить протокол TCP/IP с настройками по

[1] Рекомендуется начинать сетевые операции (например, просмотр сети или подключение к сетевому ресурсу), выдержав некоторую паузу (3—5 мин) после включения компьютера.

умолчанию. Обычно программа маршрутизации "раздает" соответствующие параметры этого протокола автоматически.

Если же рабочие станции приобретены вместе с операционными системами Windows 2000/XP/Vista, то в этом случае у администратора могут возникнуть некоторые проблемы.

Первая заключается в следующем. Если ресурсы предоставляются для совместного использования с рабочей станции с Windows 2000/XP/Vista, то на ней должны быть созданы пользователи, соответствующие текущим пользователям *каждой* рабочей станции сети. Если в Windows нет учетной записи с именем и паролем пользователя, пытающегося подключиться с другой станции (а обычно операция производится от имени того, кто работает на компьютере), то в подключении будет отказано. То есть, если на одном компьютере работает пользователь `Иванов` с паролем `пароль`, на втором — `Петров` с паролем `пароль2`, то необходимо создать пользователей `Иванов` и `Петров` с соответствующими значениями паролей[1] на той станции Windows, ресурсы которой предоставляются для совместного использования. Причем при необходимости смены паролей они должны изменяться синхронно.

Более удобный в этом случае вариант для малой сети — это включить учетную запись **Гость**, которая в новых системах по умолчанию заблокирована *(см. разд. "Автоматически создаваемые учетные записи" главы 5)*. Это самый простой способ, но он не позволяет выборочно контролировать или както ограничивать доступ к ресурсам, поскольку все подключения к компьютеру будут осуществляться от имени одной учетной записи. Если ресурс будет предоставлен в общее пользование, то он станет доступен любому пользователю.

Вторая проблема — это ограничения, искусственно введенные в рабочие станции Windows. Прежде всего, это максимальное количество подключений пользователей по сети — 10. Это ограничение не мешает подключиться одиннадцатому пользователю, но при этом автоматически разорвется одно из имеющихся неактивных соединений. Хотя, честно говоря, в малых организациях данное ограничение обычно не заставляет приобретать серверную версию операционной системы.

Кроме того, существуют ограничения по количеству одновременно открытых по сети файлов. К сожалению, это условие становится критичным при использовании популярной программы "1С:Предприятие" (в комплексной версии или при работе уже 3—4 сотрудников в обычной конфигурации[2]).

---

[1] На практике на малых предприятиях в этом случае на всех компьютерах прописывается один и тот же пользователь с одинаковым ненулевым паролем.

[2] Возможный выход — это переход на SQL-версию "1С". Или установка 1С на основе Linux.

Одноранговые сети

Описанная выше сеть является частным случаем *одноранговой сети*, в которой каждый компьютер управляется автономно и отсутствуют какие-либо централизованно реализуемые правила. Все управление ресурсами компьютера остается за локальным администратором. Кстати, по такому принципу реализован и Интернет.

Для объединения компьютеров в одноранговую сеть достаточно только создать структуру сети (провести кабели или купить беспроводные точки доступа, поставить коммутаторы и т. п.). Компьютер подключается к сети и настраивается на использование ресурсов других систем. В свою очередь администратор каждого компьютера должен определить, какие ресурсы локальной системы предоставляются в общее пользование и с какими правами, и осуществить необходимые настройки.

Одноранговая сеть удобна, если число компьютеров не превышает одного-двух десятков. С увеличением числа компьютерных систем осуществлять автономное управление каждой по единым требованиям предприятия администратору становится слишком затруднительно. Поэтому при росте локальной сети вводится то или иное централизованное управление. Конкретный критерий смены варианта управления сети определяется спецификой функционирования каждой организации.

Выбор операционной системы

Для сетей небольших организаций в качестве операционной системы рабочих станций может быть использована любая программа. Учитывая, что большинство пользователей имеют на домашних компьютерах ту или иную версию Windows и что обычно на таких предприятиях не существует серьезных производственных задач, можно рекомендовать построение небольшой локальной сети на основе Windows.

Если предприятие приобретает новые системы, то не имеет смысла покупать их вместе с Windows Vista Bussines. Для работы на малых предприятиях прекрасно подойдет версия Windows Vista Home Edition или Windows XP Home Edition, стоимость которых существенно ниже профессионального варианта. Различие между этими системами касается в основном вопросов безопасности и не существенно в данном случае.

На малых предприятиях до сих активно используются версии Windows 9*x*. В большинстве случаев также не имеет смысла обновлять эти версии операционных систем: прежде чем тратить средства на такое обновление, следует тщательно оценить, какие преимущества принесет эта операция и будут ли оправданы затраты.

Примечание

Определенным стимулом для западных пользователей является наличие поддержки операционных систем изготовителем. В настоящее время Microsoft уже не поддерживает Windows 98 и Windows NT 4.0. Однако, учитывая, что российские пользователи практически не прибегают к такому сервису, данный факт не может быть серьезным основанием для замены операционных систем новыми версиями.

Поскольку подключение к Интернету используется уже в большом количестве организаций, то для обеспечения доступа в Интернет, его защиты (установка межсетевых экранов), почтового обслуживания наиболее рационально применить системы на основе Linux. Во-первых, это бесплатные решения, что немаловажно для организаций. Во-вторых, единожды настроенные, такие компьютеры практически более не требуют к себе никакого внимания. В-третьих, эти системы не так требовательны к аппаратной составляющей, как новые версии Windows, что позволяет существенно продлить срок жизни компьютерных систем и сэкономить затраты.

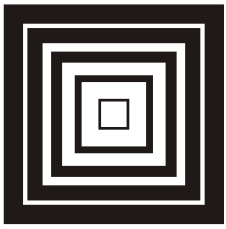
Microsoft Windows Fundamentals for Legacy PCs

Специально для использования на старых компьютерных платформах Microsoft выпустила в июле 2006 г. операционную систему Microsoft Windows Fundamentals for Legacy PCs (WinFLP). Эта операционная система построена на том же коде, что и Windows XP SP2. Пользователям WinFLP доступны такие службы, как межсетевой экран, автоматическое обновление, групповые политики и т. д. А администраторы могут с ее внедрением снизить расходы на поддержание системы (обслуживание аналогично Windows XP) и повысить общий уровень безопасности.

WinFLP не поступает в продажу как отдельный продукт. Она доступна только по специальной программе обновления программного обеспечения для корпоративных пользователей (Software Assurance).

WinFLP предъявляет следующие минимальные требования к аппаратной составляющей:

- процессор от Pentium 233 и выше;
- память от 64 Мбайт (после установки операционной системы компьютер может работать с 32 Мбайт памяти);
- жесткий диск от 500 Мбайт;
- видеоадаптер и монитор с разрешением 800×600;
- сетевая карта от 10 Мбит/с.



ГЛАВА 5

Сеть с централизованным управлением

В средних и больших организациях для упрощения управления сетью создают систему централизованного управления. В случае Windows — это создание *доменов Windows*.

В доменах Windows каждый компьютер "теряет" свою автономность, он становится "подчиненным" центру — специально выделенным серверам (контроллерам домена) и единому администратору. Локальный администратор может осуществлять свои функции в некоторых пределах, пока они не противоречат настройкам, заданным администратором домена.

Управление локальными ресурсами

Для того чтобы централизованно управлять компьютером, на нем необходимо осуществить ряд настроек. Эти операции выполняются при *включении компьютера в домен*. Обычно систему добавляют в домен с локальной консоли. Данная операция включена в меню свойств компьютера на вкладке сетевой идентификации. Она должна выполняться с правами локального администратора. Кроме того, необходимо знать идентификационные данные (имя пользователя и пароль) учетной записи, которая имеет право добавлять компьютеры в домен.

Примечание

Операцию можно выполнить из командной строки с помощью утилиты `netdom` (`netdom join` *`ComputerName /Domain DomainName /UserD DomainUserUPN /PasswordD * /User0 ComputerAdminUser /Password0 * /Reboot`*). Эта программа позволяет осуществить операцию подключения и *удаленно*. Однако первоначальная установка Windows имеет политику безопасности, разрешающую *только* локальное выполнение данной операции.

Возможность добавлять рабочие станции в домен

Начиная с Windows 2000, право добавлять рабочие станции в домен предоставлено обычным пользователям домена. Но с ограничением — не более десяти станций. В некоторых случаях желательно разрешить пользователю превысить этот лимит.

Обычные рекомендации для изменения такого лимита сводятся к тому, чтобы отредактировать права доступа к объекту **Подразделение** (Organization Unit, OU): предоставить конкретному пользователю право создания объектов типа "компьютер" и модификации его атрибутов. Операция легко выполняется настройкой соответствующих свойств безопасности для OU в оснастке управления AD (Active Directory, служба каталогов). Но это не единственная возможность и далеко не лучшая.

Если необходимо изменить лимит, установленный для *всех* пользователей, то следует модифицировать атрибуты объекта службы каталогов. Количество рабочих станций, которое пользователь может добавить в домен, определяется атрибутом **ms-DS-MachineAccountQuota** объекта "домен". Для его изменения достаточно воспользоваться программой ADSI Edit и установить желаемое значение (рис. 5.1). Установка значения этого параметра в 0 предоставляет пользователям право добавлять в домен *неограниченное* количество компьютеров.

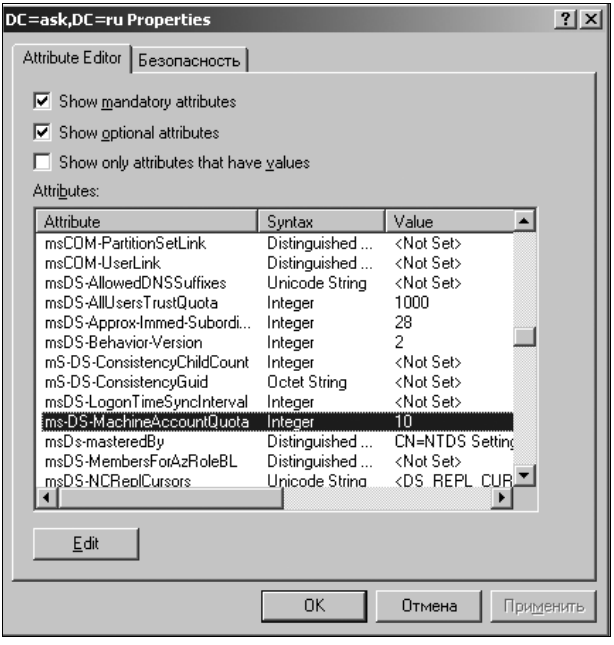


Рис. 5.1. Изменение квоты на добавление компьютеров в домен

Более целесообразно не пускать создание новых систем в домене "на самотек". Администратору следует создать объекты типа "компьютер" в службе каталогов и предоставить право подключения данных компьютеров в домен соответствующим пользователям, для чего следует в момент их создания выбрать опцию **Изменить** и определить пользователя, которому будет предоставлено такое право (рис. 5.2).

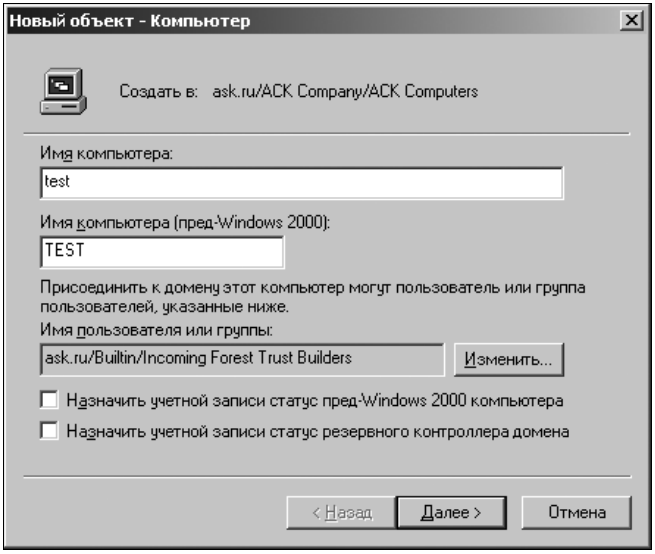


Рис. 5.2. Создание объекта "компьютер" с делегированием его подключения к домену

Изменения настроек системы при подключении ее к домену

При добавлении станции в состав домена производится ряд изменений настроек системы.

Во-первых, назначаются новые ресурсы для совместного использования. Предоставляются для совместного использования корневые каталоги локальных дисков (под именами C$, D$ и т. д.), каталог установки системы (ADMIN$), создается совместный ресурс IPC$ (используется для установки соединений по именованному каналу — *named pipes*), PRINT$ (для управления принтерами) и FAX$ (при наличии факса с совместным доступом). Эти ресурсы носят название *административных*, поскольку они предназначены для управления системами.

Данные ресурсы *невидимы* при просмотре сети (как и все другие ресурсы совместного использования, имя которых заканчивается знаком $). Если вы по-

пытаетесь удалить их, то после перезагрузки системы они вновь восстановятся[1].

Во-вторых, в локальную группу безопасности **Администраторы** добавляется группа администраторов домена, а в группу локальных пользователей — группа пользователей домена. Именно потому, что администратор предприятия состоит в группе локальных администраторов, он и получает право управления этим компьютером. А пользователи домена могут работать в системе, поскольку они состоят в группе пользователей домена, входящей в группу пользователей этого компьютера.

Примечание

При входе пользователей домена на рабочую станцию система использует данные учетных записей (имя, пароль, установленные ограничения и т. п.), хранимые на контроллерах домена. Обычно политикой безопасности разрешено кэширование нескольких паролей пользователя, что позволяет последнему войти в систему даже при отсутствии связи с контроллером домена, используя параметры последнего входа. Если работу начинает локальный пользователь, то данные берутся из локальной базы учетных записей.

Методы управления локальной системой

После добавления рабочей станции в домен администратор домена получает над ней фактически неограниченную власть.

Примечание

Системы на базе Windows 9*x* после включения в домен практически не допускали централизованного управления. Для управления системами можно было использовать только сценарии входа в домен, а также достаточно ограниченные по набору параметров групповые политики. Существовала еще возможность централизованного управления реестром Windows 9*x*, но для этого предварительно требовалось вручную установить соответствующий пакет с дистрибутива системы. На практике для централизованного управления такими системами применялись программы третьих фирм.

Какие возможности управления есть у администратора?

Во-первых, имеющиеся в системе оснастки (например, **Управление компьютером**) позволяют — при наличии соответствующих прав — управлять не только локальной системой, но и любой удаленной. Так, администратор может останавливать и запускать службы, просматривать протоколы работы системы, создавать удаленных локальных пользователей и менять их членство в группах и т. п. Операции достаточно понятные и не требуют особого

[1] Настройкой реестра системы можно отключить эти ресурсы.

объяснения. Нужно только выполнить подключение соответствующей оснастки к удаленному компьютеру (рис. 5.3).

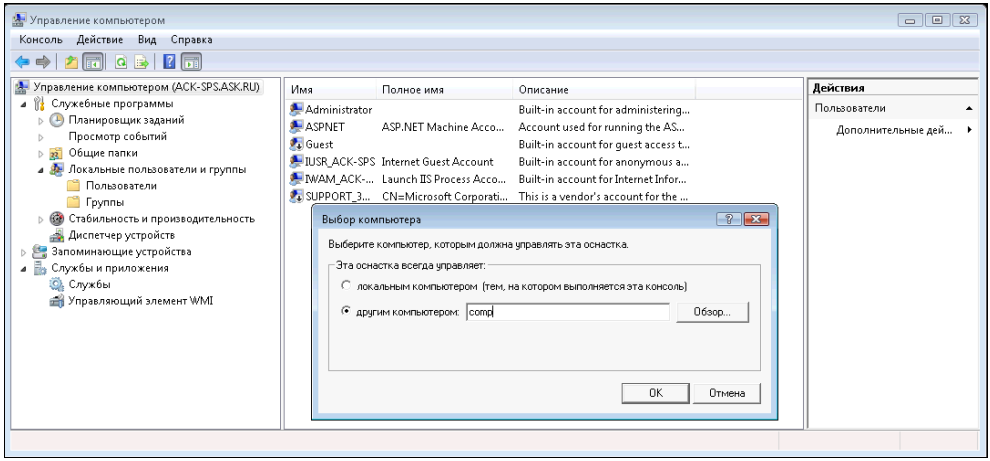


Рис. 5.3. Подключение оснастки управления к удаленному компьютеру

На практике подобные инструменты администратора обычно используются разово, для индивидуальных настроек. Применение их нерационально для операций, например, с десятком компьютеров.

Во-вторых, каждый пользователь при регистрации в домене на компьютере — члене домена[1] вызывает исполнение *сценария входа в систему*. Необходимость выполнения сценариев определяется в свойствах учетной записи пользователя на вкладке **Профиль**. Достаточно создать желаемый сценарий, который должен выполняться при начале работы пользователя, сохранить его в папке Scripts на контроллере домена и назначить пользователям.

В Windows 9*x*, Windows NT 4.0 пользователь мог прервать выполнение сценария входа в систему (например, во время исполнения пакетного файла нажать комбинацию клавиш <Ctrl>+<C>). Начиная с Windows 2000, выполнение сценария по умолчанию производится скрыто. Хотя администратор может с помощью групповой политики включить отображение выполнения команд (**Конфигурация Windows | Административные шаблоны | Система | Сценарии**) и выбрать синхронный (пока сценарий не будет выполнен до конца, пользователь не начнет работу в системе) или асинхронный вариант выполнения сценария.

---

[1] Групповые политики позволяют задать выполнение сценария входа для *компьютера*. Но на практике автор не встречался с использованием таких сценариев, поскольку обычно администраторы больше используют сценарии входа пользователей и групповые политики.

Поскольку в последних версиях Windows возможности управления из командной строки существенно расширены, то с помощью подобных сценариев можно выполнять практически любые действия: подключать сетевые диски в зависимости от членства пользователя в группе безопасности или в OU, переопределять принтеры, осуществлять копирование файлов и т. п.

В-третьих, есть наиболее распространенный вариант управления системами — это использование групповых политик для Windows 200*x*/XP/Vista. Его преимущество состоит в том, что одна настройка, заданная администратором, автоматически распространяется на определенный круг компьютеров. Например, администратор включил в групповую политику домена параметры прокси-сервера для подключения к Интернету, после чего любой компьютер, подключаемый к домену, будет получать эти настройки без каких-либо дополнительных ручных операций.

Примечание

Использование групповых политик будет рассмотрено в *главе 6*.

В-четвертых, администратор может выполнять на удаленных компьютерах любые сценарии или WMI-скрипты. Правда, для этого на локальных системах должны быть установлены соответствующие службы (например, Windows Scripting Host). Поэтому без дополнительных настроек этот способ также не реализуем на системах с Windows 9*x*/NT.

Примечание

Некоторые основы составления сценариев *см. разд."Windows Scripting Host" главы 13*.

"Кто кого": локальный или доменный администратор

Централизованное управление порой вызывает у некоторых пользователей негативную реакцию. При этом опытные пользователи вполне могут наложить ограничения на реализацию тех или иных функций управления. Рассмотрим некоторые такие возможности.

Примечание

Опытный пользователь, работающий на локальном компьютере, всегда может получить пароль локального администратора, необходимый для выполнения описываемых операций, использовав, например, способы, описанные в *главе 9*, *разд. "Восстановление пароля администратора"*.

- **Исключение компьютера из домена.**

  Один из самых эффективных способов блокирования централизованного управления — это исключение локальной системы из домена. Достаточно

отключить компьютер от сети, в свойствах системы изменить ее сетевую идентификацию — вместо домена указать *одноименную* рабочую группу. Мастер идентификации выдаст сообщение о невозможности удаления учетной записи компьютера в домене, но успешно завершит все локальные операции.

После чего необходимо создать локального пользователя, имя которого и пароль *совпадают* с данными пользователя домена. В результате пользователь сохранит практически всю функциональность работы в сети, но исключит любое централизованное управление.

"Технически" противостоять такому решению весьма сложно. Ограничения, которые может накладывать администратор домена для исключения такого варианта, должны основываться на анализе членства *учетной записи компьютера* в домене. Практически единственный способ — это включение политики ipsec и настройка ее на разрешение сессий *только* с членами домена. Однако такой вариант неприменим в случае наличия в сети рабочих станций с операционными системами предыдущих версий, которые также не являются членами домена.

- **Отключение совместного использования административных ресурсов.**

  Локальный пользователь может отключить создание административных ресурсов, если добавит параметр

  ```
  AutoShareWks : DWORD = 0
  ```

  в ветвь реестра

  ```
  HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
  ```

  (Для восстановления необходимо удалить этот параметр.)

  Следует учитывать, что отключение этих ресурсов может нарушить работу имеющейся в домене системы управления.

- **Исключение администратора домена из группы локальных администраторов.**

  Поскольку локальный администратор имеет полные права над своей системой, то он может ограничить администратора предприятия, исключив его из группы локальных администраторов. В системах с Windows NT 4.0 против такого решения практически не было "противоядия". С Windows 2000 появилась возможность регулировать членство в группах с помощью групповых политик. То есть администратор предприятия может самостоятельно определить список членов группы локальных администраторов.

  Блокировать такой вариант можно, только приняв меры по недопущению применения групповой политики для данной системы.

- **Блокировка администратора домена на уровне файловой системы.**

  С помощью ограничений доступа к файлам локального компьютера можно запретить, например, конкретным администраторам домена локальный вход в систему. Для этого следует установить для учетной записи такого администратора запрет доступа к файлам nddagnt.exe, userinit.exe, win.com, wowexec.exe. Выполнять операцию следует внимательно, чтобы случайно не запретить доступ, например, самому себе.

  Примечание

  Данная рекомендация может быть использована также при приеме на работу нового администратора. Поскольку в системе нет штатных средств ограничения локального входа администратора, то это, по сути, единственный способ защиты наиболее ответственных участков от непрофессиональных действий нового, непроверенного работника.

  Конечно, данное ограничение нельзя рассматривать всерьез, поскольку, например, групповой политикой (если не заблокировать ее) администратор домена может восстановить права доступа к значениям по умолчанию.

- **Блокирование групповой политики.**

  Поскольку основное управление осуществляется через применение групповых политик, то целью локального администратора может являться изменение ограничений, налагаемых групповой политикой, или полная ее блокировка.

  Во-первых, локальный администратор может изменить параметры, определяемые групповой политикой. Групповая политика для компьютера применяется при старте системы, а для пользователя — в момент его входа в сеть. Впоследствии система периодически проверяет изменения настроек групповой политики и применяет *только* обнаруженные *изменения* в групповой политике. Конечно, можно задать периодическое применение *всех* параметров групповой политики. В этом случае параметры, занесенные локальным администратором, будут вновь переписаны на централизованные. Но администраторы домена редко используют такие настройки, поскольку это существенно увеличивает нагрузку на контроллеры домена.

  Поэтому если параметр настройки доступен для изменения локальным администратором, то он будет сохраняться в этом измененном состоянии фактически *до следующей перезагрузки системы*. А компьютер можно не перезагружать весьма долго...

  Во-вторых, можно заблокировать применение *всех* политик, сохранив членство компьютера в домене. Например, поскольку групповые политики копируются в виде файлов с контроллеров домена (из папок SYSVOL), то можно создать такую настройку ipsec, которая будет блокировать SMB-трафик с контроллеров домена ("закрыть" порты 137, 139, 445).

Способы, к которым может прибегнуть локальный администратор для ограничения возможностей своего доменного коллеги, можно перечислять еще долго. Данная проблема имеет только одно принципиальное решение — это организационные меры, когда подобные действия локального администратора повлекут за собой "воспитательные меры" руководителей подразделений.

Проблема аудитора

Серьезные проблемы безопасности в Windows создает наличие у администратора (как локального, так и всей сети в целом) полных и единоличных прав над своей системой. Поэтому он может выполнить какие-либо операции в системе, а потом попытаться их скрыть, замаскировав тем или иным способом. Например, переписав журнал протокола. Это создает потенциальные бреши в системе безопасности. Для исключения подобных действий в сетевых системах (например, в сетях Novell) обычно имеется специальный *аудитор* — пользователь, который не имеет административных прав, но может протоколировать *любые* действия. Причем даже администратор не имеет технической возможности изменить состояние файлов протоколов. Иными словами, скрыть свои операции.

Возможный вариант решения данной проблемы в рамках систем, построенных исключительно на Windows, — это сбор данных протоколов работы компьютеров в реальном времени на отдельную, изолированную рабочую станцию. В этом случае принципиально останется возможность сравнения данных с работающих систем и архивов аудита. Администратору доступно много программ, реализующих данную функцию (например, MOM, *см. разд. "Контроль функционирования систем. Microsoft Operation Management Server" главы 13*).

Каталог

Информационные системы обычно создаются для организаций, обладающих четкой структурой. При реализации тех или иных бизнес-действий в обязательном порядке должны учитываться права пользователей, их подчиненность и т. п. Поэтому структура компьютерной информационной системы, как правило, должна создаваться по образу и подобию организационной структуры предприятия.

Средством описания такой структуры являются *каталоги*. Фактически каталоги — это базы данных. Объектами такой базы данных являются пользователи, компьютеры, подразделения, территории, предприятия и т. п. Каждый объект описывается многими характеристиками — *свойствами*. Например, у пользователя это имя, фамилия, группа, в которую он входит, время действия

учетной записи, допустимые часы работы в компьютерной сети, адрес электронной почты и т. п. Работа с такими объектами производится с учетом прав доступа (кто может создать нового пользователя, кому разрешено перевести его в другую штатную структуру и т. п.), сами операции специфичны для каждого объекта. Набор объектов, их атрибутов (свойств) и методов (допустимых операций) принято называть *схемой каталога*.

Стандарты позволяют создавать структуру каталога так, чтобы наиболее полно удовлетворить потребности каждого конкретного случая. Существуют каталоги разработки различных фирм. Но все каталоги поддерживают единые правила взаимодействия с ними. Это протокол *LDAP* (Lightweight Directory Access Protocol, протокол облегченного доступа к каталогам).

Применяя любую утилиту, которая реализует протокол LDAP, пользователь (программа) может соединиться с каталогом и, используя предоставленные права, запросить или записать информацию, выполнить другие допустимые операции. При этом изменения, вносимые в каталог, могут привести к существенной перестройке всей структуры компьютерной сети. Так, перемещение одного объекта `Подразделение` может привести к изменению десятков и сотен характеристик подчиненных объектов (вложенных подразделений, компьютеров, пользователей).

Примечание

Наиболее "быстрым" каталогом по данным тестов является каталог eDirectory разработки фирмы Novell. Разработки других фирм, в целом существенно уступая eDirectory, показывают приблизительно одинаковую производительность.

Домены Windows

Исторически иерархические сети на основе Windows создавались на базе *доменов*.

В локальных сетях на базе Windows понятие "домен" используется для обозначения совокупности пользователей и компьютеров, объединенных общими правилами безопасности (централизованная регистрация нового пользователя, единые правила доступа к совместно используемым ресурсам, единые требования по ограничениям времени работы в сети и т. п.). Единая политика безопасности в доменах Windows обеспечивается специально выделенными компьютерами сети — *контроллерами домена*.

Примечание

Не следует путать термины "домен Windows" и "домен Интернета". Хотя внешне доменная структура Windows и строится аналогично системе имен Интернета, но, говоря о домене Windows, в первую очередь имеют в виду не единую систему имен, а единую политику управления и безопасности.

Служба каталогов Windows (Active Directory)

Описанный выше каталог реализован в Windows (начиная с Windows 2000) как *служба каталогов* (Active Directory, AD). Служба каталогов Windows имеет в своей структуре такие единицы, как:

- лес;
- дерево;
- домен;
- организационное подразделение (Organization Unit, OU);
- сайты.

Хотя многие методы управления сетью в Windows базируются на службе каталогов (например, групповые политики), все же существенная часть операций унаследована исторически. Например, группы безопасности существуют отдельно от подразделений. И если вы меняете членство пользователя в подразделении, то для последующей коррекции его прав доступа необходимо дополнительно вручную изменить группу безопасности, в которую входит пользователь.

Примечание

Хотя современные программы используют данные службы каталогов, предыдущие разработки могут, например, использовать только старое — windows — имя группы (его называют также *pre-Windows 2000*).

Оснастка AD также включает поисковые возможности. Использование возможностей запросов к службе каталогов существенно повышает возможности поиска тех или иных специальных объектов. Например, можно найти рабочие станции, установленные с помощью RIS, пользователей по фамилии, учетные записи, для которых установлен неограниченный срок действия пароля,

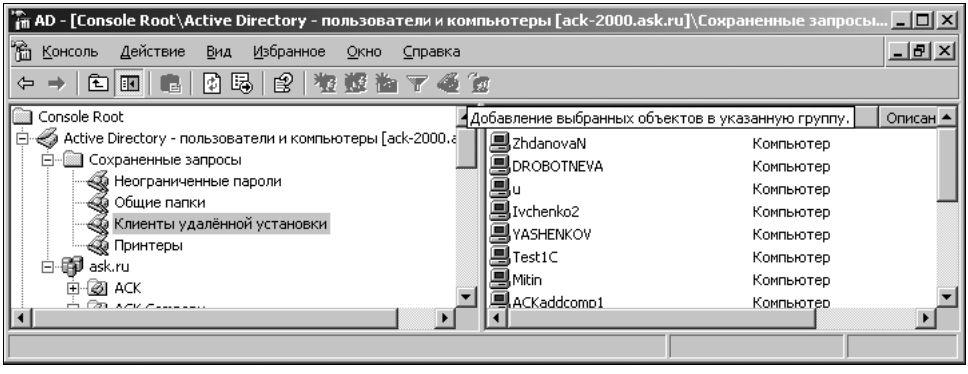


Рис. 5.4. Сохраненные поисковые запросы оснастки службы каталогов

и т. п. Каждый раз составлять заново строку поиска[1] неудобно, проще сохранить часто используемые запросы в самой оснастке и вызывать их по названию (рис. 5.4).

Домен

Традиционно основной логической единицей в Windows считается *домен*. Внутри домена реализуются все политики управления пользователями, компьютерами и сетью в целом.

В одной организации может существовать *несколько* доменов. Это могут быть как *вложенные* домены, так и домены с различными пространствами имен.

Примечание

Пространство имен — это совокупность уникальных имен. В данном пространстве имен по конкретному имени однозначно может быть определен соответствующий ему объект. Типичный пример — структура DNS. Например, в пространстве имен различных доменов могут существовать компьютеры с одинаковым именем хоста: test.primer.org и test.primer2.org. Однако в пространстве имен NetBIOS одинаковых наименований компьютеров быть не может. Поэтому при объединении таких компьютеров в единую локальную сеть вам необходимо будет дать им различающиеся NetBIOS-имена.

Наличие в одной организации доменов с отличающимися именами характерно для транснациональных организаций. Например, головное предприятие может иметь домен testorg.ru, а его подразделение в другой стране — testorg.cs.

В то же время создание *вложенных* доменов не имеет особого смысла при проектировании информационной структуры предприятия. Подобная структура оправдана только в том случае, если для некоторого подразделения необходима иная политика паролей учетных записей (например, более строгие требования к составу пароля, наличие блокировок и т. п.). Все другие настройки могут быть выполнены политиками подразделений.

Подразделение

Домены Windows (начиная с версии Windows 2000) могут содержать *подразделения* (Organization Unit, OU). OU — это своеобразный контейнер, в который можно помещать как компьютеры, так и пользователей[2].

---

[1] Например, даже простой поиск сотрудников, которым разрешен удаленный доступ в сеть, требует ввода запроса (&(&(objectclass=person)(msNPAllowDialin=TRUE))).

[2] Очевидно, что речь идет о соответствующих логических объектах.

Основная причина создания OU для администраторов системы — это возможность применения к объектам OU *групповых политик (см. главу 6)*. Повторюсь, что групповые политики — это основное средство управления компьютерной сетью. С их помощью можно автоматически устанавливать на заданные компьютеры программное обеспечение, выполнять настройку прикладных программ, менять параметры безопасности сегмента сети, разрешать или запрещать запуск конкретных программ и т. п.

Каждое OU может, в свою очередь, содержать внутри себя любое количество вложенных OU, учетные записи компьютеров и пользователей, группы (пользователей). Если попробовать изобразить графически такую структуру — домен с несколькими вложенными доменами со структурой OU, пользователями и компьютерами, то такой рисунок будет напоминать *дерево* с вершиной, ветвями, листьями. Этот термин и сохранен для описания такой структуры.

Примечание

Обратите внимание, что при удалении OU будут удалены и содержащиеся в нем объекты (например, учетные записи компьютеров).

Лес

Если на одном предприятии существуют несколько доменов с различными пространствами имен (например, testorg.ru и testorg.cs), то представленная графически такая структура будет напоминать *лес*. Лес — это коллекция (одного или более) доменов Windows 2000/2003, объединенных общей схемой, конфигурацией и двусторонними транзитивными доверительными отношениями.

Обратите внимание, что деревья в таком лесу не самостоятельны. Все эти деревья создаются *внутри одной организации* и управляются централизованно администраторами предприятия. Говоря терминами логической организации сети, между любыми доменами внутри предприятия существуют *доверительные двусторонние отношения*.

Практически это означает, что администратор предприятия является "начальником" администратора любого домена, а пользователь, прошедший аутентификацию в одном домене, уже "известен" в другом домене предприятия.

Примечание

Многие администраторы доменов в структуре леса заблуждаются, считая что только они могут управлять безопасностью объектов. Даже если они явно запретили доступ каким-либо пользователям, то владелец корневого домена (леса) Windows *всегда* имеет возможность получить доступ к объектам и назначить собственные права. Иными словами, в сети с централизованным управле-

нием необходимо полностью доверять тем администраторам, которым принадлежат корневые права.

Сайты

Если домены и OU описывают логическую организацию, то *сайты* (Sites) предназначены для описания *территориальных делений*. Считается, что *внутри одного сайта* присутствуют скоростные каналы связи (обычно компьютеры сайта находятся в одном сегменте локальной сети). А различные сайты связаны друг с другом относительно медленными каналами связи. Поэтому между ними создаются специальные механизмы репликации данных. Например, можно задать график репликации (использовать периоды наименьшей загрузки каналов связи), выбрать используемый протокол (IP или путем приема/передачи сообщений по протоколу SMTP) и т. п.

Соотношение территориальной и логической структуры выбирается из конкретной конфигурации предприятия. Например, можно создать несколько сайтов в одном домене или сформировать в каждом сайте свой домен и т. п.

Примечание

Поскольку алгоритм выбора контроллера домена рабочей станцией использует структуру сайтов, то создание дополнительных сайтов может быть способом балансировки нагрузки между контроллерами домена.

Режимы совместимости доменов и леса

Домены Windows могут обслуживаться контроллерами на базе операционных систем Windows NT 4.0 Server или Windows 200*x*. Более новая операционная система обеспечивает большие возможности в управлении доменами и большую безопасность. Однако в целях обратной совместимости домены Windows могут работать в различных *режимах* (mode). Если в вашей сети нет контроллеров на базе предыдущих версий ОС, то следует перевести домен в режим наибольшей безопасности.

Данная операция доступна в свойствах домена в оснастке управления, а для леса — в соответствующей оснастке управления сайтами и службами (в свойствах соответствующего объекта).

Хозяева операций

Если в домене Windows NT 4.0 один контроллер всегда является *основным* (primary), а все остальные выполняют роль резервных систем, то в Windows 200*x* все контроллеры *равнозначны*.

Однако для обеспечения правильной синхронизации данных между различными контроллерами некоторые функции зафиксированы только за одной

системой. Такие функции носят название Flexible Single Master Operation role (FSMO). В доменах Windows 200*x* их пять:

- Schema master (один на лес);
- Domain naming master (один на лес);
- RID master (один на домен);
- PDC emulator (один на домен);
- Infrastructure master (один на домен).

При первоначальной установке домена все пять ролей зафиксированы за первым контроллером. Впоследствии их можно переносить на другие контроллеры, учитывая специфику структуры организации. Важно только, чтобы при исключении контроллера домена администратор контролировал, что все эти пять операций не потеряли хозяина.

Смена хозяев операций

Три роли (PDC, RID, Infrastructure) легко переносятся с помощью оснастки AD **Пользователи и компьютеры**. Необходимо просто открыть оснастку, подключиться к тому контроллеру домена, на который планируется перенести соответствующую роль, и выполнить соответствующую команду в меню.

Все операции по переносу ролей можно выполнить в командной строке. Для этого используется утилита `ntdsutil`. Главное, что эту утилиту можно использовать не только для переноса ролей при *работающих* контроллерах, но и для *назначения* нового владельца роли в случае аварийного выхода из строя прежнего хозяина.

Примечание

Назначение ролей следует использовать с осторожностью, при наличии полной уверенности в том, что прежний хозяин не будет вновь доступен в сети. Появление двух хозяев одной роли может привести к неработоспособности всего домена.

Опишем кратко последовательность операций, которые необходимо выполнить для назначения контроллеру домена новой роли.

1. Открыть утилиту и набрать команду `ROLES`.
2. Указать, к каким контроллерам необходимо подключиться, для чего набрать команду `CONNECTIONS` и ввести команду подключения к необходимому контроллеру, после чего закрыть опцию `CONNECTIONS`, набрав `QUIT`.
3. Выбрать нужную команду `SEIZE ...`, чтобы переписать соответствующую роль.

Утилита сначала попытается корректно перенести выбранную роль, и лишь при недоступности соответствующего контроллера будет выполнена операция перезаписи.

Примечание

Если в структуре предприятия присутствует *несколько* доменов, то совмещение ролей Infrastructure Master с сервером глобального каталога *недопустимо*.

Сервер глобального каталога (GC)

Контроллеры домена хранят информацию об объектах *текущего* (собственного) домена. Поскольку в логической структуре предприятия может существовать несколько доменов, то для выполнения операций, затрагивающих объекты разных доменов, необходим доступ к соответствующим контроллерам. Для ускорения операций в системе существуют специальные контроллеры, которые хранят[1] *все объекты леса*, но только не с полным, а с частичным набором атрибутов. Такие контроллеры называются *серверами глобального каталога* (Global catalog, GC).

В качестве GC может быть назначен любой контроллер домена. Назначение контроллера домена сервером глобального каталога производится через оснастку AD **Сайты и Службы**. Раскрыв узел, соответствующий нужному контроллеру, в свойствах **NTDS Settings** необходимо включить параметр использования контроллера в качестве GC.

Примечание

В локальных сетях рекомендуется назначать серверами глобального каталога не менее двух контроллеров домена.

Серверы GC хранят наиболее часто используемые атрибуты объектов. Условно можно считать, что объем хранимых на GC данных снижается примерно в 2 раза по сравнению с "полным" вариантом описания объекта. Но если конкретным приложениям необходим частый доступ к нереплицируемым атрибутам, то администратор может внести изменения в параметры GC, откорректировав *схему организации*. Для этого достаточно в консоли управления оснасткой AD **Schema** включить репликацию в свойствах соответствующих атрибутов; по умолчанию этой оснастки нет в списке меню, ее следует добавить в консоль управления.

Примечание

Некоторые приложения активно используют обращения к GC. Например, MS Exchange Server. В этих случаях сервер GC обязательно должен быть включен в соответствующий сайт ("рядом" с таким приложением).

---

[1] В режиме *только для чтения*.

В реальной сети необходимо обеспечить некую разумную избыточность GC, имея в виду, что каждый дополнительный GC — это и дополнительный объем копирования данных, передача которых может привести к повышенной нагрузке на системы и каналы связи.

DN, RDN

Для успешной работы с каталогами необходимо ориентироваться в терминах DN (Distinguished Names) и RDN (Relative Distinguished Names).

Объекты каталога хранятся в иерархической структуре. Условно можно сравнить такую структуру со структурой файловой системы. Есть корневой каталог, есть вложенные в него каталоги, в них, в свою очередь, могут храниться как сами файлы, так и другие папки. В этой аналогии DN подобен *полному пути имени файла*. В DN приводится полный путь к объекту, начиная с самой "верхней" точки иерархии каталога.

RDN подобен *относительному* пути к файлу. Это может быть только само имя файла (обычный RDN) или относительный путь (многоатрибутный RDN). Например, в организации может быть заведен пользователь `Иванов`. Если в организации в разных отделах работают два Иванова, то только по фамилии невозможно будет определить конкретного работника. Но если использовать многоатрибутный RDN, состоящий, например, из фамилии и названия отдела, то работник будет обозначен точно:

```
cn = Иванов + ou = Бухгалтерия
```

Управление структурой домена предприятия

При проектировании логической структуры компьютерной сети организации следует учитывать многие факторы: решаемые задачи, требования безопасности, количество офисов, квалификацию обслуживающего персонала и т. п.

В небольших организациях не имеет особого смысла создание разветвленной логической структуры сети, поскольку обычно внутри организации применяются только одна или две групповые политики. С увеличением численности компьютерных систем структура становится все более сложной.

В большинстве случаев логическая структура домена будет "следовать" за организационной структурой предприятия. На малых и средних предприятиях обычно не возникает задача оптимизации количества и размещения контроллеров домена[1]. Если исходить из критериев мощности компьютера, то производительности одного сервера обычно вполне достаточно для обслуживания нескольких сотен рабочих станций. Однако в целях резервирования

[1] Ситуация с удаленным офисом будет обсуждена в *главе 8*.

целесообразно иметь в сети не менее двух контроллеров, чтобы временные неисправности на одном из них не отразились на функционировании предприятия.

Создание нового домена

Для создания нового домена необходимо запустить утилиту `dcpromo` (ее можно стартовать также из задачи управления сервером, выбрав в меню пункт создания контроллера домена). В зависимости от ответов на вопросы мастера операции, вы сможете добавить новый контроллер в существующем домене либо создать новый домен. Можно создать новый домен внутри уже существующего, либо создать новое дерево доменов, дав домену уникальное имя. Все операции достаточно просты и обычно выполняются в течение нескольких минут. После чего, перезагрузив компьютер, вы получаете новый контроллер домена.

Примечание

Естественно, что для выполнения операций пользователь должен обладать соответствующими правами. Так, для создания нового дерева доменов предприятия операцию необходимо выполнять с правами администратора предприятия.

Перед началом операции следует тщательно обдумать то доменное имя, которое вы дадите вновь создаваемому домену. Если ваша организация имеет уже зарегистрированное в Интернете доменное имя, то имя домена Windows может быть основано на нем[1]. Ничто не запрещает вам избрать для внутреннего домена имя, которое не соответствует реальным доменам Интернета, например дать название myorg.local.

Примечание

Проследите, чтобы полное доменное имя *не являлось именем первого уровня*, а обязательно состояло из двух частей. В противном случае необходимо выполнить ряд дополнительных настроек, которые следует уточнить по документации с сайта разработчика.

Создание домена обязательно требует наличия сервера DNS. Если сервер DNS не настроен, по умолчанию программа установки предлагает создать и настроить сервер DNS локально. В общем случае служба каталогов не требует обязательного использования DNS-сервера разработки Microsoft. AD может быть установлена, например, на сервер BIND. При этом следует учесть, что BIND версии 4.9.7 и старше поддерживает возможность создания SRV-

[1] Можно присвоить внутреннему домену реальное имя Интернета, а можно дать только локальное название. В любом случае по соображениям безопасности данные структуры домена Windows (DNS-сервера) *не публикуются* в глобальной сети.

записей, которые необходимы для работы службы каталогов, а, начиная с версии 8.2.2, поддерживаются и динамические обновления записей данного типа.

Особенности создания дополнительного удаленного контроллера в домене Windows Server 2003

После создания нового контроллера домена программа пытается выполнить его синхронизацию с другими контроллерами. Объем данных, передаваемый в этой операции по сети, обычно составляет десятки мегабайт, а в средних организациях может превышать и несколько сотен мегабайт. Поэтому установку контроллеров для филиалов, подключенных через медленные каналы связи, лучше производить непосредственно в центральном офисе. После первоначальной синхронизации компьютер можно выключить и перевезти на удаленную площадку. Объем синхронизуемых данных, которые будут переданы после включения компьютера в удаленном офисе, в этом случае будет существенно ниже объема первоначальной синхронизации и не создаст критической нагрузки на каналы связи.

В Windows 2003 введена новая возможность при создании контроллера домена — это выполнение первоначальной синхронизации из файлов резервного копирования.

Для создания нового контроллера в удаленном офисе необходимо сначала выполнить резервное копирование состояния (system state) любого контроллера домена, после чего полученные файлы резервной копии любым способом передать в удаленный офис (например, нарезать на CD-матрицы). В удаленном офисе следует восстановить эти данные утилитой `ntbackup` *в другое место* (выбрать данную опцию и указать папку для восстановления). Затем запустить утилиту `dcpromo` с ключом `/adv`. При таком варианте ее запуска на одном из шагов появится дополнительная опция, запрашивающая место, откуда следует провести загрузку первичных данных (рис. 5.5). Вам достаточно указать папку, в которую было проведено восстановление данных с контроллера домена. В завершение операции система проведет синхронизацию последних изменений службы каталогов.

Новая возможность Windows 2003 Server позволяет при создании второго контроллера загрузить большую часть данных из файлов резервного копирования основного контроллера, сократив объем реплицируемых по каналам связи данных.

Примечание

Для проведения операции создания нового контроллера домена при *любом варианте* необходимо иметь связь с действующими контроллерами домена (для проверки прав и внесения необходимых изменений в схему организации).

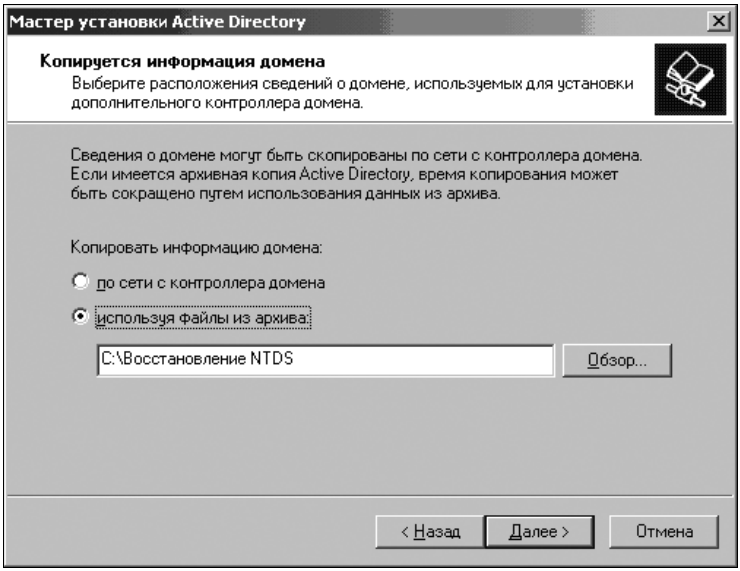


Рис. 5.5. Копирование данных контроллера домена из архивной копии

Удаление контроллера домена

Штатное удаление контроллера домена производится с помощью той же утилиты `dcpromo`. Ее следует запустить на компьютере, роль которого предполагается понизить до обычного сервера. Указав необходимые параметры операции (например, пароль будущего локального администратора), администратору нужно только дождаться сообщения о требуемой перезагрузке системы. Для успешного завершения операции компьютер должен иметь связь с другими контроллерами (если это не последний контроллер домена).

Бывают ситуации, когда контроллер выходит из строя, например из-за неполадок в оборудовании, и его не планируется восстанавливать из резервной копии. В таком случае необходимо удалить из службы каталогов все записи, которые связаны с этим контроллером. Для этого штатно используется утилита `ntdsutil`.

Примечание

В Windows Server 2003 графические утилиты пополнены новыми опциями удаления контроллера, однако в Windows 2000 описываемый в тексте способ является единственным.

Опишем последовательность шагов, которые необходимо выполнить в данной утилите для удаления отсутствующего контроллера домена.

1. После запуска утилиты на экране появится окно ее интерфейса. Вам необходимо перейти к опции **metadata cleanup**.
2. Теперь нужно подключиться к работающему контроллеру домена (**connections | connect to server <*имя*>**), на котором мы будем выполнять операцию удаления метаданных.
3. После подключения к контроллеру снова возвращаемся в режим **metadata cleanup**. На этом шаге необходимо выбрать тот контроллер, данные о котором предполагается удалить.
4. Набираем команду **Select operation target**, после перехода в этот режим последовательно подключаемся к ресурсам организации. Например, чтобы указать на конкретный сервер, сначала нужно будет просмотреть список сайтов (**List sites**), после чего подключиться к нужному сайту (**Select site <*номер, полученный на предыдущем шаге*>**). Затем просмотреть список доменов и подключиться к нужному и т. д. В завершение после выполнения команды `List servers for domain in site` вы увидите нумерованный список серверов. Вам нужно выбрать тот сервер, который предполагается удалить (**Select server <*номер*>**), и вернуться в меню **metadata cleanup**.
5. В меню **metadata cleanup** дать команду на удаление параметров выбранного сервера (**Remove selected server**).

Переименование домена

Имя домена Windows невозможно сменить для доменов на основе операционных систем Windows NT 4.0 Server/Windows 2000 Server. Для доменов, работающих в режиме Windows 2003, такая возможность появилась, и автору приходилось ее выполнять. Но эта операция весьма ответственна и не всегда в ходе ее осуществления могут быть изменены все наименования. Например, сертификаты, выданные на старые имена, окажутся недействительны, придется менять настройки почтового сервера и т. п.

Примечание

Операция переименования домена возможна только при условии перевода домена в режим Windows 2003 Server.

Для выполнения операции необходимо загрузить с сервера Microsoft последнюю версию утилиты переименования домена[1]. В составе загрузочного комплекта присутствует весьма подробное описание условий и операций, которые необходимо выполнить в процессе подготовки и переименования домена.

[1] Domain rename tool.

Утилиты управления объектами службы каталогов

Управление доменом может проводиться не только с серверов Windows. При наличии соответствующих прав большинство операций может быть выполнено удаленно с рабочих станций (см., например, рис. 5.3, на котором показан вызов аналогичной утилиты с рабочей станции Vista). Для этого необходимо установить пакет администрирования (Adminpak.msi), который поставляется с дистрибутивом сервера.

Стандартные средства для управления структурой службы каталогов — это оснастки управления пользователями и компьютерами, доменами и доверием, сайтами и службами. Как в случае любой графической утилиты, этими программами удобно и быстро можно выполнять типовые операции, для которых они были разработаны. В нашем случае — это операции создания пользователей и подразделений, назначение им свойств, перемещение пользователей, компьютеров и подразделений между различными контейнерами и т. п.

Выполнение данных операций с помощью указанных оснасток достаточно прозрачно, все проблемы администратор легко решит с помощью справочной системы.

Утилиты запросов командной строки службы каталогов

В системе присутствует несколько утилит, которые позволяют в режиме командной строки выполнить простейшие операции со службой каталогов Windows: поиск объектов по заданным критериям, добавление и удаление объектов, их перемещение и т. п. Это команды `dsquery` (выполняет поисковые запросы к службе каталогов), `dsadd` (добавляет новые объекты), `dsget` (отображает параметры объектов), `dsmod` (изменяет параметры объектов), `dsmove` (перемещает объекты), `dsrm` (удаляет объекты).

Например, с помощью команды `dsquery` можно легко получить список компьютеров, не работавших в сети в течение какого-либо периода времени:

```
dsquery computer -inactive 5
```

где 5 — число недель, в течение которых компьютер не входил в сеть.

Утилита `csvde` позволяет импортировать/экспортировать объекты в формате CSV. Этот формат удобен для последующего анализа, например, в Excel. Синтаксис команды аналогичен описываемому ниже для `Ldifde`. Особенность использования `csvde` состоит в том, что с ее помощью можно добавлять объекты, но нельзя изменять их атрибуты или удалять существующие объекты.

LDAP-управление

Служба каталогов Windows представляет собой иерархическую структуру, управление которой может осуществляться различными стандартными мето-

дами. Например, администратор может получить доступ к объектам службы каталогов с использованием сценариев на Visual Basic, применяя запросы ADO и т. п.

Поскольку служба каталогов поддерживает протокол LDAP, ставший стандартом для доступа к подобным службам, то для управления структурой домена можно применять соответствующие утилиты.

Во-первых, можно использовать оснастку ADSI Edit (рис. 5.6). С помощью этой оснастки можно подключиться к любому узлу структуры службы каталогов, увидеть его атрибуты, при необходимости отредактировать их и установить желаемые права доступа. Оснастка позволяет создавать новые объекты в структуре каталогов, удалять существующие, перемещать их и т. п.

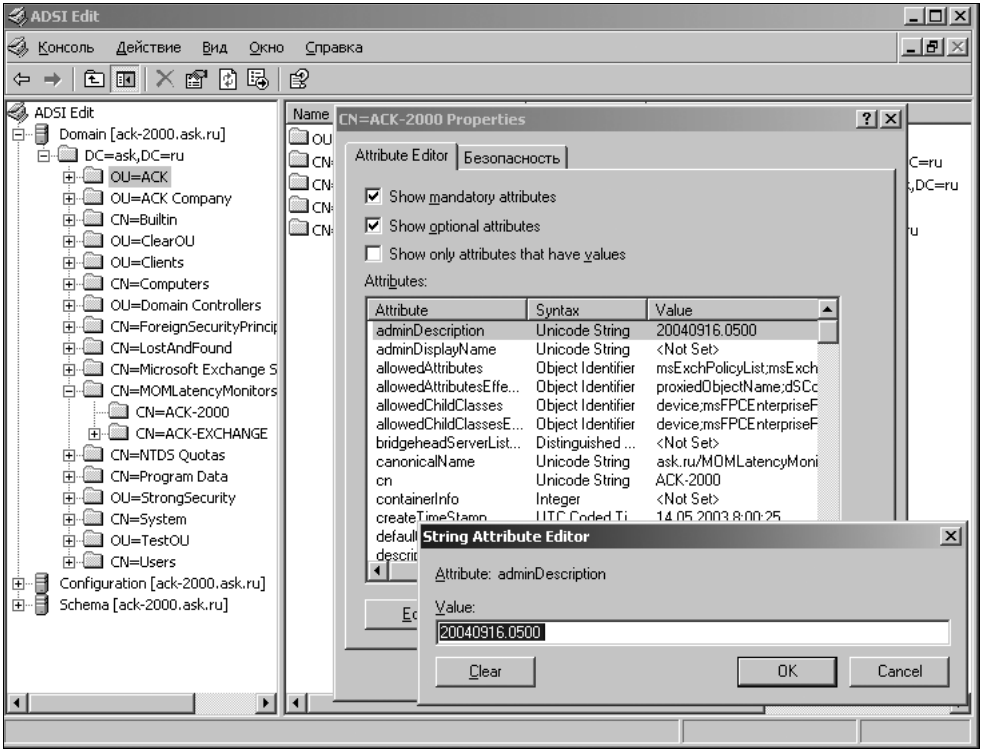


Рис. 5.6. Утилита ADSI Edit

Примечание

Обратите внимание, что с помощью этой оснастки можно подключиться к любой точке структуры каталогов, а не только к элементам **Domain**, **Configuration**, **Schema**. Достаточно указать соответствующие параметры в меню программы.

Во-вторых, при установке Support Tools в систему добавляется утилита ldp.exe, которая позволяет подключаться к службам по протоколу LDAP, добавлять и удалять объекты, редактировать их, выполнять поиск. Утилита несколько необычна в использовании, поскольку предполагает первоначальные знания администратором структуры каталогов. При ее запуске следует выполнить подключение к службе в нужной точке *(connect)* и зарегистрироваться *(bind)*.

Конечно, применять ldp.exe в случаях, когда можно, например, использовать графические оснастки, не имеет смысла. Но эта утилита позволяет выполнять операции *с объектами* службы каталогов с использованием синтаксиса LDAP-протокола. Например, первоначально ldp.exe являлась единственным бесплатным вариантом восстановления удаленных объектов каталога *(см. разд. "Просмотр и восстановление удаленных объектов каталога" далее в этой главе)*.

Синтаксис поисковых запросов LDAP

Для обозначения *свойств* объектов (по терминологии Microsoft) в стандартах LDAP применяется термин *атрибуты*.

В LDAP используются специальные конструкции для фильтров, в которых оператор ставится *до* самих величин. Например, если вам необходимо найти всех пользователей с фамилией Иванов, то фильтр следовало бы записать по следующей форме: `(И(тип=пользователь)(фамилия=Иванов))`. То есть два условия объединены требованием `И`, которое записано *до* условий.

В фильтрах допустимы операторы, перечисленные в табл. 5.1.

Таблица 5.1. *Допустимые операторы фильтров*

Оператор	Описание
=	Равно
~=	Приблизительно равно
<=	Меньше или равно
>=	Больше или равно
&	И
|	ИЛИ
!	НЕТ

Примечание

Некоторые объекты допускают использование поиска по маске (`*`); в общем случае наличие такой возможности следует уточнить по документации.

Если в запросе необходимо использовать символы: `(`, `)`, `*` и `NUL`, то они должны быть записаны через escape-последовательность так, как указано в табл. 5.2.

Таблица 5.2. *Escape-последовательности*

Символ	Записывается как
*	\2a
(	\28
)	\29
\	\5c
NUL	\00

Примечание

Аналогично через escape-последовательность записываются двоичные данные с разбиением по два байта.

Определенную сложность при первых обращениях к операциям поиска вызывает знание необходимого атрибута, который должен быть использован в операции. Можно порекомендовать просмотреть все атрибуты объекта этого же типа, выбрать нужное свойство и использовать его в запросе. Это можно сделать и в самой программе ldp.exe, если включить отображение вывода в результате поиска *всех* атрибутов. Для этого следует открыть окно поиска, нажать кнопку **Option** и в строку перечня атрибутов ввести звездочку (`*`).

Примечание

Чтобы вернуться к выводу сокращенного списка атрибутов, следует в данной строке перечислить (через точку с запятой) названия тех атрибутов, которые должны отображаться на экране по результатам поиска.

Покажем на небольшом примере, как можно быстро найти пользователя по второму почтовому адресу.

Дополнительные адреса электронной почты, которые присвоены пользователю, перечисляются в атрибуте `proxyaddresses`. Дополним перечень отображаемых атрибутов этим значением (допишем его в строку `Attributes` после точки с запятой) и снимем флажок в параметре `Attributes`, чтобы программа поиска вывела на экран значения атрибутов. Установим в окне настройки фильтра поиска в качестве начальной точки имя нашего домена, а критерием поиска выберем следующую строку:

```
(&((objectclass=user)(proxyaddresses=*адрес*)))
```

Она означает, что мы хотим искать только пользователей, у которых один из адресов электронной почты содержит символы `адрес` (в любом месте адреса). Выберем зону поиска по всей базе (SubTree). Выполнив поиск, мы получим на экране необходимые сведения.

Команда *ldifde*

Большая часть системных администраторов предпочитает использовать для конфигурирования серверов текстовые файлы, поскольку с ними удобнее работать, чем с двоичной информацией. Для каталогов существует стандарт LDIF[1], который определяет правила представления данных каталога в текстовом файле.

LDIF-файл представляет собой текстовые строки, в которых приведены атрибуты объектов, их значения и директивы, описывающие способы обработки этой информации. В Windows имеется утилита `ldifde`, которая выполняет такое преобразование данных из службы каталогов, используемой в Windows, в текст и обратно. Ключи утилиты позволяют уточнить точку подключения, глубину выборки, указать фильтры операции и т. п.

На эту утилиту обычно обращается мало внимания, хотя она может существенно упростить многие административные задачи.

Предположим, что вам необходимо откорректировать параметры пользовательских учетных записей, например, указать для всех работников некоторого подразделения в свойствах учетных записей название их отдела. Выполнение операции "в лоб" — последовательное открытие учетных записей и вставка нужного описания в соответствующее поле — весьма трудоемко и нерационально при значительном числе сотрудников.

С помощью же данной утилиты можно выполнить экспорт в текстовый файл параметров учетных записей пользователей *только* для заданного подразделения (установив фильтр по данному OU), после чего с помощью обычного текстового редактора одной операцией поиска и замены откорректировать значения нужных атрибутов. В завершение достаточно выполнить импорт полученного файла. В результате атрибуты для *всех* записей будут откорректированы практически за несколько шагов.

Примечание

Такая операция также весьма просто выполняется с помощью сценария Visual Basic. Достаточно подключиться к нужному контейнеру, установить фильтр для выборки только объектов типа "пользователь" и запустить цикл для каждого элемента данного типа в этом контейнере. Однако приведенная схема не тре-

[1] LDAP Interchange Format, определен в RFC 2849.

бует от администратора знания сценариев и может быть выполнена буквально в течение нескольких минут.

Выше мы приводили пример, как с помощью команды `dsquery` получить список компьютеров, длительное время не работавших в составе сети. Приведем второй способ, как можно получить в файл такой список с помощью команды `ldifde`:

```
ldifde -f <имя_файла>.txt -n -d "dc=<имя_домена>,dc=ru" -r
"(&(objectcategory=computer)(|(lastlogon<=127296891259257277)(!lastlogon=*
)))" -p SubTree -l lastlogon
```

В фильтре использовано представление даты в машинном формате. Такие значения легко можно получить при помощи простых операций, например:

```
Dim Time1 As System.DateTime = System.DateTime.Now().AddMonths(-2)
Dim FileTime1 = Time1.ToFileTime
```

Переменная `FileTime1` будет иметь значение, соответствующее дате двухмесячной давности[1]. Фильтр также выводит имена компьютеров, для которых отсутствует значение параметра времени входа в систему.

Представленный пример несколько искусственен, поскольку результат может быть получен более простым способом. Но привели его именно для того, чтобы проиллюстрировать существование различных возможных вариантов действий администраторов.

Делегирование прав

Традиционно системный администратор объединял в себе все текущие функции управления доменом. Он создавал и удалял пользователей, добавлял компьютеры в домен, следил за членством в группах и т. п. Большинство таких рутинных операций без ущерба для функционирования сети может быть переложено на других сотрудников. Например, новые учетные записи пользователей в соответствующем подразделении могут создаваться сотрудником кадровой службы при оформлении приема на работу; компьютеры в домен добавляться сотрудниками технической службы сервиса; разработка групповых политик, предусматривающих установку специализированных программ, вестись техническими специалистами соответствующего отдела; добавление пользователей в группы безопасности — сотрудниками подразделений безопасности и т. п. При этом за администратором предприятия сохранились бы все руководящие функции для возможных экстренных вмешательств, но "освободились руки" для подготовки и реализации стратегических решений.

---

[1] Необходимо учитывать, что компьютеры, которые не перезагружались в течение этого периода, также будут иметь "старые" значения времени входа в систему.

Для того чтобы осуществить на практике такую передачу прав, которую принято называть *делегированием*, администратору достаточно изменить разрешения безопасности на соответствующий контейнер. Так, если необходимо делегировать кому-либо право создания пользователей, то этому сотруднику следует дать право на создание объекта типа "пользователь" в заданном подразделении. При этом перечень возможных прав доступа для контейнера является настолько подробным, что администратор без труда может настроить объем делегирования (например, дать право добавления в домен компьютеров, но лишить возможности изменения или удаления таких объектов).

Делегирование прав создания учетных записей позволит более тесно "связать" кадровые записи и записи служб каталогов. Учетная запись в этом случае может иметь только минимальные начальные права для входа в систему. Предоставление дальнейших прав по доступу к ресурсам (изменение членства в группах) могут осуществлять менеджеры соответствующих групп.

Большинство утилит графического управления объектами службы каталогов содержат в меню команду *делегирования прав*. Эта команда вызывает мастер, который меняет список прав доступа (рис. 5.7). Запуск данного мастера является самым простым способом делегирования прав на объекты. Но при этом администратору следует учитывать два момента.

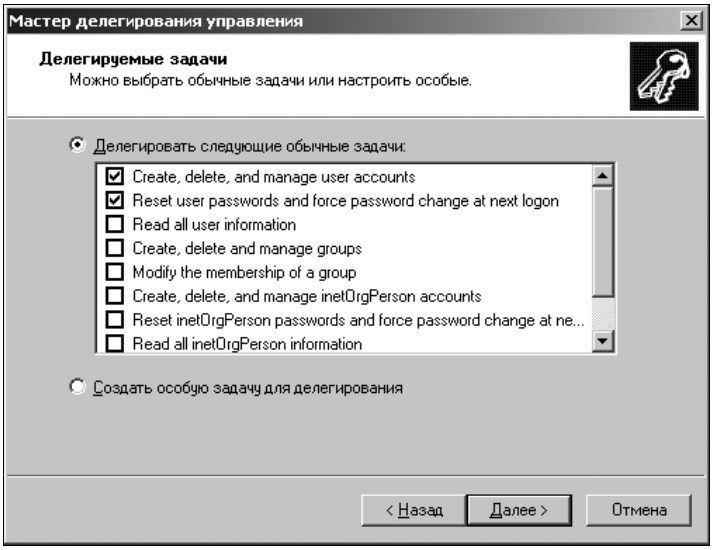


Рис. 5.7. Мастер операций предлагает определить объем делегирования прав

Во-первых, всегда можно более точно откорректировать права доступа, если обратиться к редактированию параметров безопасности контейнера *напрямик*.

Во-вторых, хотя мастер делегирования прав присутствует в системе, но мастера *отзыва прав* не предусмотрено. Иными словами, если, например, необходимо передать право управления от одного сотрудника другому, то администратору придется вначале *вручную* исключить первого из списка доступа.

Просмотр и восстановление удаленных объектов каталога

Удаленные объекты каталога (например, учетная запись пользователя или компьютера) в домене Windows сначала помещаются в специальный контейнер (аналог Корзины), в котором они сохраняются по умолчанию 60 суток. В течение этого времени данные объекты можно *восстановить*.

Примечание

Этот интервал можно изменить, если ввести, например с помощью ADSI Edit, новое значение атрибута `tombstoneLifetime` для объекта `cn=Directory Service,cn=Windows NT,cn=Services, cn=Configuration,<DN_корня_леса>`.

Администратор может использовать и утилиту для автоматического восстановления удаленных объектов каталога (см. **http://www.sysinternals.com /Utilities/AdRestore.html**), но приведенный ниже пример является хорошей практикой непосредственной работы с объектами каталога.

Для просмотра и восстановления удаленных объектов необходимо использовать утилиту `ldp` из состава Support Tools. После ее запуска нужно подключиться к контроллеру домена (операция **Connect**) и "предъявить" свои учетные данные (операция **Bind**). Если теперь отобразить дерево каталога домена, то в окне программы вы увидите папку Deleted Objects с удаленными объектами.

Удобнее отобразить удаленные объекты с помощью операций поиска утилиты `ldp`. Для этого нужно выполнить команду меню **Browse | Search**. После появления окна опций поиска необходимо правильно настроить параметры операций:

- в строке **Base Dn** ввести `cn=Deleted Objects,<DN_имя_домена>`, например: `cn=Deleted Objects,dc=ask,dc=ru`;
- в строке **Filter** ограничить область поиска только удаленными объектами, введя `(isDeleted=TRUE)`;
- параметр **Scope** установить в значение **One Level**;
- далее нажать кнопку **Options** и ввести следующие параметры:
  - **Tile limit**, **Time out** и т. п. — установить в соответствии с предполагаемым объемом поиска и временными затратами;

- в строке **Attributes** через точку с запятой перечислить названия атрибутов объектов, которые должны быть отражены в результате поиска, например: `name;lastKnownParent`;
- **Search Call Type** установить в **Extended**;

❒ нажать кнопку **Controls** и в списке **Load Predefined** выбрать значение **Return Deleted Objects**; если поиск производится на Windows 2000, то в этом случае ввести в строку **Object Identifier** следующие символы `1.2.840.113556.1.4.417` и нажать кнопку **Check In**. В обоих случаях указанная последовательность цифр должна появиться в окне **Active Controls**;

❒ закрыть два окна настройки параметров, вернуться к окну поиска и выполнить операцию **Run**.

В результате программа покажет список удаленных объектов, соответствующих заданным вами условиям поиска.

На рис. 5.8 приведен результат поиска удаленных пользователей домена, имена которых начинаются с символов `test` (при удалении к имени добавляется код, поэтому поиск следует выполнять по первым символам с добавлением маски). Был применен фильтр поиска `(&(isDeleted=TRUE)(cn=test*))`. В результате программа нашла три таких объекта.

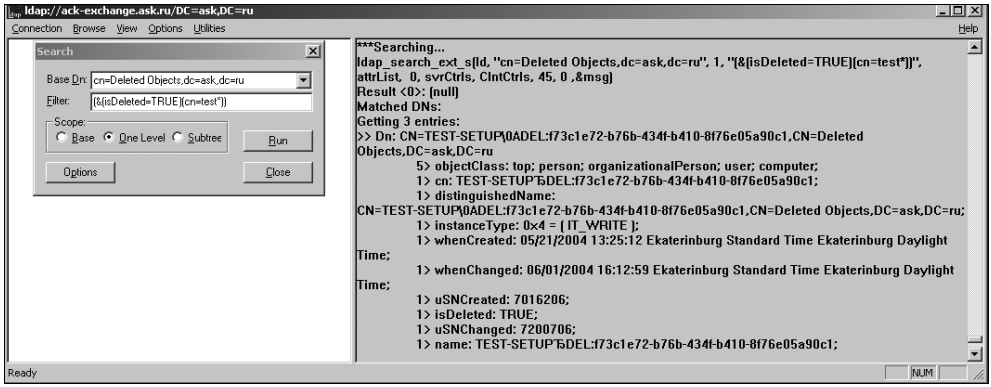


Рис. 5.8. Поиск удаленных объектов службы каталога

Восстановление удаленных объектов имеет некоторые особенности. Чтобы восстановить объект, нужно выполнить следующие действия:

❒ *удалить* атрибут **isDeleted** для данного объекта;

❒ *заменить* значение атрибута **distinguishedName** на то, куда будет восстановлен объект (обычно выбирается прежнее расположение, которое можно уточнить по значению параметра **lastKnownParent**);

- *установить* обязательные атрибуты (если таковые требуются для данного типа объекта).

Все эти действия должны быть выполнены *за одну операцию*. Если описать кратко операцию восстановления по шагам, то следует:

1. *Подключиться к* контроллеру домена, ввести свои учетные данные.
2. Добавить контроль **Return Deleted Objects** (или `1.2.840.113556.1.4.417` для Windows 2000) в меню **Options | Control**.
3. Найти тот объект, который предполагается восстановить (так, как описано выше), и запомнить его DN.
4. Выполнить команду **Browse | Modify** и указать в качестве DN соответствующее значение восстанавливаемого объекта.
5. В строке **Attribute** указать **distinguishedName**, в строке **Value** ввести новое значение (то, которое должно быть у восстановленного объекта), выбрать операцию **Replace** и нажать кнопку **Enter**.
6. Указать в качестве **Attribute** значение **isDeleted**, очистить строку **Value**, в качестве операции указать **Delete** и нажать кнопку **Enter**.
7. После этого следует добавить обязательные атрибуты, если они необходимы для восстанавливаемого объекта.
8. Отметить флажки **Synchronous** и **Extended**.
9. Нажать на кнопку **Run** (рис. 5.9).

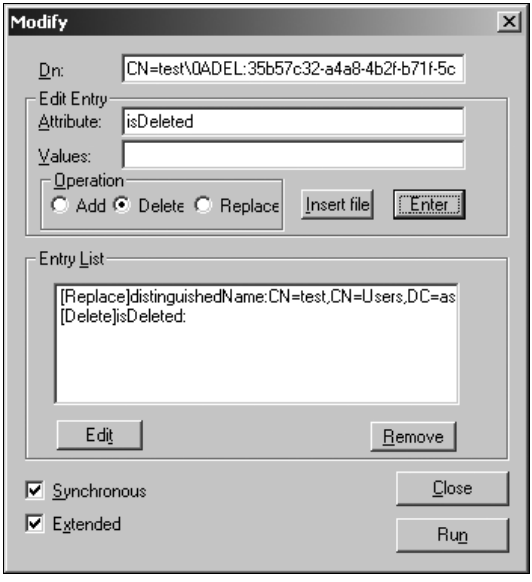


Рис. 5.9. Восстановление объекта путем прямого редактирования каталога

Результаты операции можно будет увидеть в правой части окна утилиты `ldp`, предназначенной для вывода сообщений.

После восстановления объектов, имеющих идентификаторы безопасности (SID), необходимо снова включить их в те группы безопасности, в которых они были до удаления. Эта операция необходима, т. к. процесс удаления очищает соответствующие значения.

При восстановлении пользователя необходимо разблокировать его и восстановить в тех группах безопасности, членом которых он был. Если пользователь имел ящик на почтовом сервере Exchange, то рекомендуется очистить эти атрибуты его учетной записи и осуществить переподключение с помощью оснастки управления MS Exchange.

По умолчанию правом восстановления объектов каталога обладают администраторы. Это право также можно делегировать другим пользователям, но данная операция нецелесообразна по соображениям безопасности (имея возможность восстановить пользователей, злоумышленник может получить доступ от имени такого восстановленного пользователя к ресурсам организации).

Распределенная файловая структура

Распределенная файловая структура (Distributed File System, DFS) предоставляет администратору возможность создавать структуру данных, которые *не привязаны к какому-либо компьютеру сети*. Например, в домене можно создать одну точку подключения к файлам, физически находящимся на различных компьютерах. Иными словами, пользователь подключается к совместно используемому ресурсу DFS, указывая не сетевой адрес конкретного компьютера, а доменный путь. В результате администратор получает возможность в процессе работы прозрачно для пользователей перемещать совместно используемые файловые ресурсы с одного компьютера на другой, а пользователь по-прежнему будет обращаться к файлам по старому пути, который он однажды запомнил и который сохранен в параметрах установки программ.

Вторая возможность DFS — это автоматическое поддержание хранения копий данных на нескольких компьютерах. Например, можно создать копию папки с файловыми ресурсами центрального офиса в удаленном филиале, и система самостоятельно будет синхронизировать изменения, независимо вносимые пользователями в каждом офисе. Причем подключения пользователей будут автоматически осуществляться к тому компьютеру, данные которого расположены "ближе" к пользователю.

Создание DFS

DFS представляет собой коллекцию ссылок на совместно используемые ресурсы, находящиеся на различных компьютерах сети, доступ к которым производится через единую точку входа, *не привязанную* к конкретному компьютеру[1]. Структура DFS напоминает дерево каталогов: на самом "верху" расположена одна точка входа, называемая *корнем DFS*, к которой подключены вложенные папки.

Корень DFS может быть создан на любом сервере Windows 200*x*, причем на рядовых серверах возможно создание только одного корня DFS, тогда как в домене может поддерживаться *несколько корней DFS* (разными контроллерами).

В качестве корня DFS указывается любая совместно используемая папка (мастер создания DFS позволяет создать такую папку в процессе настройки). Рекомендуется не хранить в этой папке никаких файлов, а использовать ее только для создания ссылок на сетевые ресурсы.

После создания корня DFS необходимо начать "собирать" структуру папок распределенной файловой системы. Для этого с помощью оснастки управления DFS следует добавить ссылки на уже существующие *совместно используемые ресурсы сети*. Причем возможно указать несколько ссылок на аналогичные ресурсы на разных компьютерах. Операция обычно не представляет никакой сложности.

Если администратору по каким-либо причинам необходимо переместить ресурс в структуре DFS на другой сервер, достаточно просто скопировать файлы по новому пути и заменить ссылку со старой сетевой папки на новую. При этом для клиентов все используемые ими сетевые пути (если, конечно, они указывали на структуру DFS) останутся неизменными.

Примечание

Конечно, можно воспользоваться и средствами автоматической репликации для такого переноса данных (создать пустую папку и добавить ее в репликацию), как описывается ниже. Но при большом объеме файлов ресурсов системы может не хватить для нормального завершения операции. Например, на практике автора система потребовала изменения настроек в реестре при попытке создания автоматической копии структуры папок документов объемом порядка 5 Гбайт.

Репликация DFS

Как уже говорилось, структуру DFS можно сделать *отказоустойчивой*. Каждую ссылку можно продублировать, создав вторую ссылку на аналогичный

[1] Структура DFS-домена хранится в службе каталогов (AD).

сетевой ресурс на другом компьютере. В результате при недостижимости одного ресурса клиенты будут автоматически перенаправлены к функционирующему компьютеру. Причем система может *автоматически синхронизировать* эти ресурсы. Если данные будут изменены в папке по одной ссылке, то в папке по другой ссылке они будут продублированы.

Реплицируемые ресурсы должны быть расположены в папках с NTFS 5.0, поскольку система использует систему протоколирования этой файловой структуры для отслеживания изменений.

Примечание

Если необходимо использовать ограничения прав доступа к документам в папках DFS, то эти настройки следует применить *только* к папкам сервера (\\<*имя_сервера*>\<*имя_папки*>). Иначе при создании ссылки DFS по новому месту репликации папка унаследует права родительской структуры.

По умолчанию репликация не включена. Чтобы организовать синхронизацию данных нескольких серверов, необходимо выделить соответствующие ссылки на ресурсы и выбрать команду **Синхронизовать**. При создании репликации требуется указать, какой ресурс будет являться основным *(мастером)*. Когда первоначальная репликация завершится, все ссылки станут равнозначными: изменение в одном месте повлечет изменение по другой ссылке.

Автоматически синхронизируются не все файлы. Из репликации исключаются временные файлы (список расширений можно просмотреть в настройках). Сами файлы реплицируются только после того, как с ними завершена работа пользователя. Иными словами, если пользователь открыл файл и работает с ним в течение всего дня, то копия файла по реплицируемой ссылке изменится только *после завершения работы — вечером*.

Если два пользователя одновременно работают с одним и тем же файлом в различных репликах, то система разрешит такой конфликт путем сохранения тех изменений, которые были внесены в файл, сохраненный позже.

Репликацию можно использовать для поддержания копий документов на нескольких территориально разделенных площадках. В этом случае часто имеет смысл ограничить время репликации периодами минимальной загрузки канала. Для этого в меню расписания следует определить разрешенные периоды, в течение которых будет проводиться синхронизация данных.

Настраивается график репликации в задаче AD **Пользователи и компьютеры**. Открыв оснастку, следует включить отображение дополнительных функций (**Вид** ⇒ **Дополнительные функции**) и найти необходимый корень DFS. Открыв его свойства на вкладке **Набор репликации**, нужно нажать кнопку **Изменить расписание** и отредактировать график (рис. 5.10).

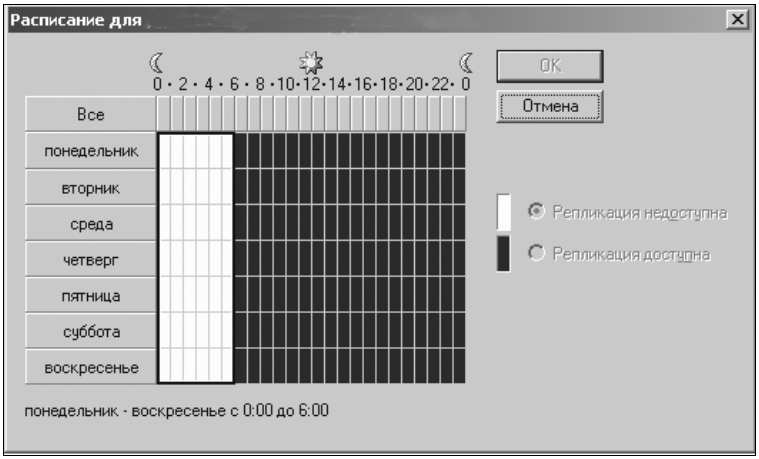


Рис. 5.10. Настройка графика репликаций DFS

График репликации можно задавать для каждого корня. При этом следует учитывать специфику использования данных и стоимость канала передачи данных в определенные периоды времени.

Учетные записи и права

Понятие учетной записи

Если вы имели опыт работы администрирования и работы с операционными системами Windows 9*x*, то одной из главных отличительных особенностей профессиональных версий Windows воспринимается повышенное внимание к тому, *кто* и *что* делает на компьютере.

Программа, которая исполняется на компьютере с установленной операционной системой Windows NT/200*x*/XP/Vista, всегда запущена от имени какого-либо пользователя и обладает данными ему правами. Если вы начали работу на компьютере, введя свое имя и пароль, то любая задача: графический редактор или почтовый клиент, дефрагментация диска или установка новой игры — будет выполняться от этого имени. Если запущенная программа вызывает в свою очередь новую задачу, то она также будет выполняться в контексте вашего имени. Даже программы, являющиеся частью операционной системы, например служба, обеспечивающая печать на принтер, или сама программа, которая запрашивает имя и пароль у пользователя, желающего начать работу на компьютере, выполняются от имени определенной учетной записи (**Система**). И так же, как программы, запускаемые обычным пользователем, эти службы имеют права и ограничения, которые накладываются используемой учетной записью.

Операционная система "различает" пользователей не по их имени (полному или сокращенному), а по специальному уникальному номеру (идентификатору безопасности — SID)[1], который формируется в момент создания новой учетной записи. Поэтому учетные записи можно легко переименовывать, менять любые иные их параметры. Для операционной системы после этих манипуляций ничего не изменится, поскольку такие операции не затрагивают идентификатор пользователя.

Примечание

При создании новой учетной записи обычно определяются только имя пользователя и его пароль. Но учетным записям пользователей — особенно при работе в компьютерных сетях — можно сопоставить большое количество различных дополнительных параметров: сокращенное и полное имя, номера служебного и домашнего телефонов, адрес электронной почты и право удаленного подключения к системе и т. п. Такие параметры являются дополнительными, их определение и использование на практике зависит от особенностей построения конкретной компьютерной сети. Эти параметры могут быть использованы программным обеспечением, например, для поиска определенных групп пользователей (см., например, *группы по запросу*).

Стандартные учетные записи имеют идентичные SID[2]. Например, `S-1-5-18` — это SID учетной записи Local System; `S-1-5-19` — учетной записи NT Authority\Local Service; SID `S-1-5-20` "принадлежит" учетной записи NT Authority\Network Service и т. д. Учетные записи пользователя домена "построены" по такой же структуре, но обычно еще более "нечитаемы". Вот пример реального доменного SID:

```
S-1-5-21-61356107-1110077972-1376457959-10462
```

Если при изменении имени входа пользователя в систему ничего "существенного" для системы не происходит — пользователь для нее не изменился, то операцию удаления учетной записи и последующего создания пользователя точно с таким же именем входа операционная система будет оценивать как появление *нового* пользователя. Алгоритм формирования идентификатора безопасности пользователя таков, что практически исключается создание двух учетных записей с одинаковым номером. В результате новый пользова-

---

[1] Существуют многочисленные утилиты, которые позволяют по имени входа пользователя определить его SID и наоборот. Например, такая утилита входит в состав Resource Kit для Windows NT 4.0 (getsid). В статье KB276208 базы знаний Microsoft приведен код на Visual Basic, который позволяет выполнить запросы SID/имя в обычном сценарии. Код хорошо комментирован и легко может быть применен без поиска специализированных утилит. Можно также установить на компьютер утилиты Account Lockout and Management Tools (см. рис. 5.11), которые добавляют к оснастке управления пользователями в домене еще одну закладку свойств, на которой в том числе отображается и SID пользователя.

[2] Перечень Well Known Security Identifiers приведен, например, в KB243330.

тель не сможет, например, получить доступ к почтовому ящику, которым пользовался удаленный сотрудник с таким же именем, не прочтет зашифрованные им файлы и т. п.

Локальные и доменные учетные записи

При работе в компьютерной сети существуют два типа учетных записей. *Локальные учетные записи* создаются на данном компьютере. Информация о них хранится локально (в локальной базе безопасности компьютера) и локально же выполняется аутентификация такой учетной записи (пользователя).

Доменные учетные записи создаются на контроллерах домена. И именно контроллеры домена проверяют параметры входа такого пользователя в систему.

Чтобы пользователи домена могли иметь доступ к ресурсам локальной системы, при включении компьютера в состав домена Windows производится добавление группы пользователей домена в группу локальных пользователей, а группы администраторов домена — в группу локальных администраторов компьютера. Таким образом, пользователь, аутентифицированный контроллером домена, приобретает права пользователя локального компьютера. А администратор домена получает права локального администратора.

Необходимо четко понимать, что одноименные учетные записи различных компьютеров — это *совершенно различные пользователи*. Например, учетная запись, созданная на локальном компьютере с именем входа `Иванов`, и доменная учетная запись `Иванов` — это два пользователя. И если установить, что файл доступен для чтения "локальному Иванову", то "доменный Иванов" не сможет получить к нему доступ. Точнее, доменный Иванов сможет прочесть файл, если его пароль *совпадает* с паролем локального Иванова. Поэтому если на компьютерах одноранговой сети завести одноименных пользователей с одинаковыми паролями, то они смогут получить доступ к совместно используемым ресурсам автономных систем. Но после изменения одного из паролей такой доступ прекратится.

Примечание

Обратите внимание, что в локальные группы можно включать не только локальные ресурсы (учетные записи пользователей и локальных групп), но и *доменные* учетные записи.

После установки пакета Account Lockout and Management Tools в свойствах учетной записи отображается вкладка, на которой администратор может увидеть в том числе и количество неудачных попыток входа в систему (рис. 5.11). Данную информацию можно получить и выполнив непосредст-

венный запрос к службе каталогов. В качестве фильтра можно указать следующую строку:

```
(&(objectclass=user)(!(objectclass =computer))(!(badPwdCount=0))
(badPwdCount=*))
```

При необходимости вы можете создать такой запрос, сохранить его в оснастке управления AD и получать сведения о результатах подключения к домену без установки упомянутого пакета.

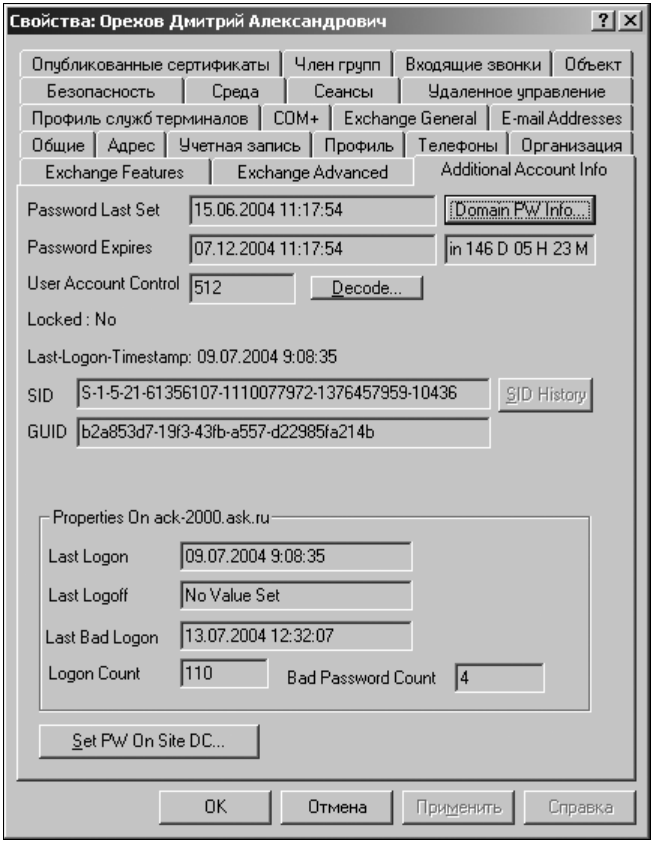


Рис. 5.11. Дополнительные параметры учетной записи

Группы пользователей

Разные пользователи должны иметь разные права по отношению к компьютерной системе. Если в организации всего несколько сотрудников, то администратору не представляет особого труда индивидуально распределить

нужные разрешения и запреты. Хотя и в этом случае возникают проблемы, например, при переходе сотрудника на другую должность администратор должен вспомнить, какие права были даны ранее, "снять" их и назначить новые, но принципиальной необходимости использования каких-либо объединений, групп пользователей не возникает.

Иная ситуация в средней организации. Назначить права доступа к папке для нескольких десятков сотрудников — достаточно трудоемкая работа. В этом случае удобно распределять права не индивидуально, а по *группам пользователей*, в результате чего управление системой существенно облегчается[1]. Поскольку книга посвящена, в первую очередь, работе в составе компьютерной сети, уделим особое внимание именно группам, создаваемым в доменах Windows.

Исторически сложилось так, что существует несколько типов групп. Связано это в основном с необходимостью совместимости различных версий операционных систем.

Во-первых, есть группы, которым, как и пользователям, присваивается идентификатор безопасности. Это означает, что вы можете назначать права доступа, основываясь не на индивидуальном членстве, а сразу всей группе пользователей. И есть группы, которые не имеют такого SID. Например, Distribution Group. Объясняется это наличием групповых операций, для которых не нужно контролировать параметры безопасности. Например, создание группы пользователей для распространения программного обеспечения или группы для централизованной рассылки почты. Отсутствие SID не мешает в этом случае правильному функционированию программ, но существенно снижает нагрузку операционной системы.

Во-вторых, группы могут различаться по области действия. Например, существуют локальные группы, глобальные и универсальные.

В-третьих, группы могут иметь постоянных членов (каждый пользователь назначается в соответствующую группу администратором) или основываться на выборке пользователей по каким-либо правилам. Например, можно создать группу, в которую будут включаться пользователи с записью в их свойствах, что они работают в "отделе 22". Изменилось соответствующее поле в свойствах пользователя — и при очередных операциях с данной группой система произведет выборку пользователей, "увидит" новых членов группы и выполнит необходимые действия. Обратите внимание, что такие группы с

[1] При смене должности пользователя достаточно переместить его в другую группу. При создании новых проектов права доступа к ним будут назначаться на основе существующих групп и т. п.

динамическим членством *не имеют SID*, т. е. не могут быть использованы для контроля прав доступа.

Примечание

В Windows пользователь "получает" список групп, в которых он состоит, *при входе в систему*. Поэтому если администратор сменил у пользователя членство в группах, то это изменение начнет действовать *только* после нового входа в систему. Если пользователь должен быстро получить доступ к ресурсам, ему следует завершить работу в системе (`log off`) и сразу же вновь войти в нее (`log on`).

Возможные члены групп. Области применения групп

Универсальные группы появились с приходом Windows 2000. В *смешанном* режиме допустимы были только группы Distribution Group, при переходе в основной режим стало возможным создавать и универсальные группы безопасности.

Универсальные группы могут включать учетные записи (и другие группы) из *любого* домена предприятия и могут быть использованы для назначения прав также в *любом* домене предприятия.

Глобальные группы могут включать другие группы и учетные записи *только* из того домена, в котором они были созданы. Но группа может быть использована при назначении прав доступа в *любом* домене.

Локальные группы могут включать объекты как из текущего домена, так и из других доменов. Но они могут быть использованы для назначения прав *только в текущем домене*.

В группы можно включать как учетные записи пользователей и компьютеров, так и другие группы. Однако возможность вложения зависит от типа группы и области ее действия (табл. 5.3).

Таблица 5.3. *Группы пользователей*

Группа	Включает объекты	Допустимые вложения групп
Локальная	Пользователи	Универсальные и глобальные группы *любого* домена
Локальная безопасности	Пользователи	Глобальные группы
Глобальная	Пользователи	Глобальные группы этого же домена
Глобальная безопасности	Глобальная группа	Нет
Универсальная	Пользователи и компьютеры	Универсальные и глобальные группы *любого* домена

Примечание

Если пользователь является членом универсальной группы, то при входе его в сеть необходимые права должны быть проверены с *сервера глобального каталога*, а не с любого контроллера домена. Для ускорения операций проверки, начиная с Windows Server 2003, введена возможность кэширования членства универсальных групп. Включение кэширования осуществляется через оснастку управления сайтом: необходимо выделить соответствующий сайт и в правом окне оснастки открыть свойства **NTDS Settings**. После чего установить соответствующий параметр в значение "включено" и отредактировать расписание кэширования (в случае необходимости).

Преобразования групп

Начиная с Windows 2000 с режима native mode, администраторы могут изменять типы групп, а именно преобразовывать группу безопасности в Distribution Group, и наоборот. Возможна также смена области действия группы с универсальной на доменную. Наиболее полные возможности преобразования существуют в режимах сервера для Windows 2000 или Windows Server 2003.

Обратите только внимание, что наличие вложенных групп в некоторых случаях может препятствовать преобразованию типа родительской группы.

Результирующее право: разрешить или запретить?

При назначении прав можно определить как *разрешение*, так и *запрещение* на выполнение какой-либо операции. Если пользователь входит в несколько групп, то каждая из них может иметь свой набор разрешений и запретов для данной операции. Как формируется итоговое разрешение, особенно если разрешения различных групп противоречат друг другу?

Первоначально проверяется, существуют ли *запреты* на выполнение операций для какой-либо из групп, в которые входит пользователь, и для самой учетной записи. Если хотя бы для одной группы определен запрет доступа, то система сформирует отказ в операции. Затем проверяется наличие разрешений на *доступ*. Если хотя бы для одной группы будет найдено разрешение, то пользователь получит право выполнения желаемого действия.

В соответствии с описанным правилом обработки, если пользователь как член одной группы имеет разрешение на выполнение действия, а как член другой группы — запрет, то результатом явится отказ в выполнении операции.

Следует быть крайне осторожным при назначении явных запретов. Очень легко (если на компьютере используется сложная структура групп) запретить даже самому себе выполнение тех или иных операций.

Примечание

Существует единственное отступление от данного принципа преимущества запрета перед разрешением, известное автору. Это определение итогового разрешения на основе *наследуемых* и *явно указанных* прав, которое описано в *разд. "Наследуемые разрешения: будьте внимательны" далее в этой главе*.

В последних версиях Windows система позволяет отобразить результирующие разрешения доступа к данном объекту для любого пользователя или группы. Эта операция вызывается из меню дополнительных параметров безопасности соответствующего объекта системы (рис. 5.12).

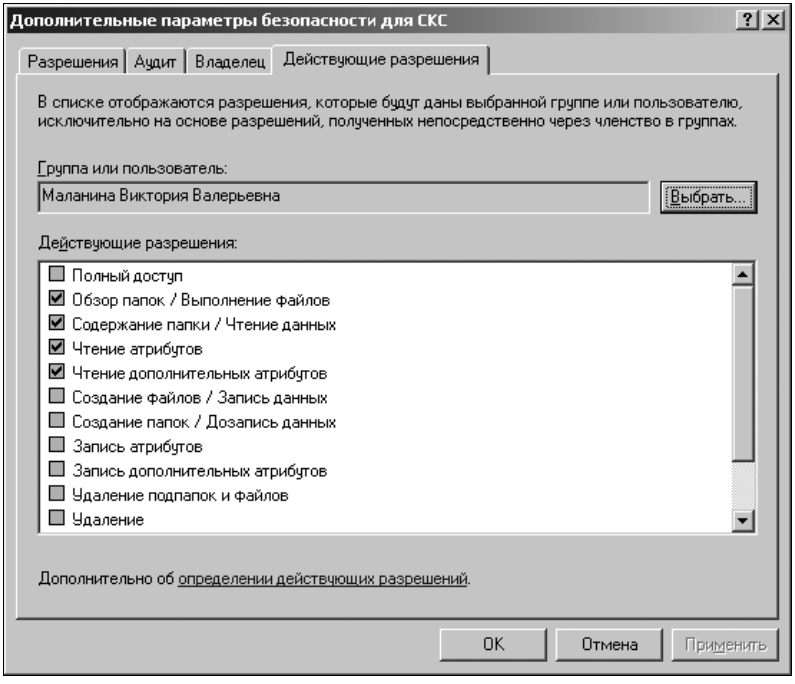


Рис. 5.12. Результирующее разрешение

Разрешения общего доступа и разрешения безопасности

Для объектов, предоставляемых в совместное использование, существуют два типа разрешений. Это разрешения общего доступа и разрешения безопасности. Разрешения *общего доступа* определяют право на использование данного ресурса при сетевом подключении. Если у пользователя нет такого права (или это действие запрещено явно), то он просто не сможет *подключиться* к запрашиваемому ресурсу.

Разрешение *безопасности* — это разрешение на уровне прав доступа файловой системы. Оно существует при использовании файловой системы типа NTFS и проверяется *независимо* от разрешений общего доступа. Иными словами, если пользователю разрешено подключаться к этому ресурсу по сети, но доступ к файлам запрещен разрешениями безопасности, то в итоге работа с такими файлами будет невозможна. Если на диске с ресурсами использована файловая система FAT (FAT32), то доступ по сети будет контролироваться *только* разрешениями общего доступа.

Примечание

Типичной ошибкой пользователей, связанной с наличием двух типов разрешений, является предоставление в совместное использование папок, находящихся на рабочем столе. После предоставления общего доступа к таким папкам другие пользователи не могут открыть файлы и т. п. Связана эта ошибка с тем, что рабочий стол — это папка в профиле пользователя. А разрешение безопасности на профиль пользователя по умолчанию разрешает доступ к нему *только* этому пользователю и администратору компьютера. Поэтому для возможности работы других пользователей с такой общей папкой необходимо добавить для них *разрешения безопасности* на уровне файловой системы.

Поскольку эти разрешения в определенной степени дублируют друг друга (с точки зрения результата), то на практике их обычно комбинируют в зависимости от желаемых условий доступа.

- Права доступа ко всем объектам сетевого ресурса одинаковы для всех пользователей.

  В этом случае разрешения общего доступа и разрешения безопасности выставляются идентичными для всех заданных групп пользователей.

- Права доступа различны для различных объектов сетевого ресурса

  Часто бывает так, что к одним файлам нужно предоставить полный доступ, а другие разрешить только просматривать и т. д. В этом случае можно настроить права доступа следующим образом.

  Разрешения общего доступа устанавливаются по максимально возможным правам. Так, если часть файлов должна быть доступна только для чтения, а часть и для редактирования, то разрешения общего доступа следует установить как *"полный доступ"* для всех групп пользователей, которым ресурс должен быть доступен по сети. А разрешениями безопасности нужно выполнить точную настройку: установить разрешение только для чтения для одних папок, полный доступ — для других, запретить доступ к определенным папкам для некоторых групп пользователей и т. д.

  Такой подход упростит структуру ресурсов сети при сохранении всех необходимых разрешений.

Наследуемые разрешения: будьте внимательны

По умолчанию вновь создаваемые ресурсы наследуют свои разрешения безопасности от родителей. Так, при сохранении нового файла его разрешения будут установлены по разрешениям той папки, в которой создается файл.

При необходимости изменения прав внутри такой структуры наследования легко можно добавить новые права для любых учетных записей. С исключением дело обстоит несколько сложнее. Сначала необходимо *разорвать* цепочку наследования (в диалоговом окне, открывающемся при нажатии кнопки **Дополнительно** в свойствах безопасности, снять флажок **Разрешить наследование разрешений от родительского объекта...**) и отредактировать список установленных прав.

Назначение разрешений файловой системы обычно не представляет особой сложности. При этом наиболее частый вопрос, который возникает у пользователей, — это изменение прав доступа, когда в свойствах объекта они отображаются квадратиками с серым фоном.

Такое отображение свидетельствует о том, что разрешения на данный объект *наследуются* от родительского. Для того чтобы изменить их, необходимо данную связь разорвать. Эта операция выполняется через кнопку **Дополнительно** — достаточно снять уже упоминавшийся флажок **Разрешить наследование....**

Разрешения, которые добавлены к списку унаследованных, называют *явно установленными*. Явно установленные разрешения имеют *преимущество* перед унаследованными. При этом не работает принцип верховенства запрета. Если унаследовано право запрета на доступ, а явно задано разрешение, то в результате пользователь *сможет* выполнять операции с файлами (рис. 5.13).

В свойствах файла отмечены как запреты (унаследованы от родительской папки, выделены серым фоном флажка выбора), так и явно назначенные полные права владения. В этом случае будет действовать *явное назначение прав*. Пользователь сможет выполнять с файлом любые операции, несмотря на наличие запрета.

В такой ситуации результирующие права неверно отображались самой системой: было показано полное отсутствие прав, несмотря на наличие разрешения полного доступа.

Примечание

Администратору следует внимательно отнестись к такому правилу, поскольку это может привести к неучитываемым возможностям доступа к данным. Причем на компьютере автора окно отображения результирующих прав доступа неверно показывало существующие разрешения: права доступа к файлу не были показаны, хотя они фактически имелись.

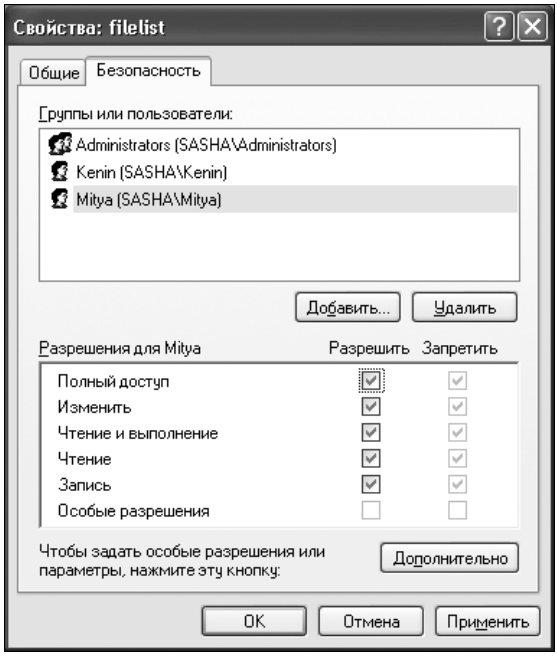


Рис. 5.13. Наследованные и явно заданные разрешения противоречат друг другу

Восстановление доступа к ресурсам

В условиях предприятия нередки ситуации, когда необходимо получить доступ к ресурсам, разрешения на использование которых не существует. Это могут быть файлы уволившегося пользователя или ресурсы, ставшие недоступными для всех пользователей вследствие ошибки, произошедшей при наложении разрешений.

Для разрешения подобных ситуаций используется специальное право — право *владельца объекта*.

Владелец объекта — эта та учетная запись, от имени которой создан данный объект. У владельца объекта есть *неотъемлемое право* — назначать разрешения безопасности. Иными словами, если пользователь создал файл, а потом администратор запретил ему с помощью разрешений безопасности доступ к этому файлу, то пользователь как владелец этого файла сможет в любой момент восстановить работу с данным ресурсом (или предоставить право работы другому пользователю).

Владельца объекта можно заменить. По умолчанию возможностью присвоить себе право владельца объекта обладают только администраторы.

Для получения доступа к объектам в общем случае администратор должен выполнить следующие действия:

1. Сначала стать владельцем этих объектов (выполняется через кнопку **Дополнительно** в настройках безопасности).
2. Воспользовавшись правом владельца объекта, установить для него желаемые разрешения безопасности.

Примечание

Обратите внимание, что квоты использования дискового пространства рассчитываются по владельцам объектов, поэтому после того как для получения разрешения безопасности администратор стал владельцем некоей папки, объем этой папки перешел из квоты пользователя в квоту администратора.

Обход перекрестной проверки

Если пользователю запрещен доступ к текущей папке, но разрешен к вложенной, то он сможет, например, открыть файл из последней, указав явным образом полный путь к нему. Эту особенность принято называть *обходом перекрестной проверки*.

Настройкой параметров безопасности можно запретить данную возможность. Однако такое решение должно применяться только в особых, специально аргументированных случаях, поскольку оно повлечет сбои в работе многих программ (например, невозможность работы в Outlook Web Access).

Администратору следует учитывать данный вариант предоставления прав доступа и правильно настраивать соответствующие параметры.

Изменение атрибутов объектов при операциях копирования и перемещения

Установка разрешений на доступ к объектам в Windows не представляет особой сложности. Достаточно выделить объект, открыть его свойства и назначить необходимых пользователей с желаемыми правами.

В то же время принципы изменения свойств объектов при их копировании или перемещении часто остаются без внимания, хотя неточное понимание вариантов изменения разрешений может привести к незапланированному результату. Так, если при копировании файла он перестанет быть зашифрованным, а вы по-прежнему считаете информацию, содержащуюся в нем, защищенной, то такой факт может привести к неприятным последствиям. О таких последствиях пользователю стала сообщать Windows Vista, но в случае работы в предыдущих версиях этот факт нужно учитывать самостоятельно.

Примечание

Описываемые далее правила изменения атрибутов имеют смысл только при файловых операциях на дисках с системой NTFS. Если файл копируется/перемещается на диск с файловой системой FAT32 (FAT), то он теряет атрибуты шифрования, сжатия и т. п. Иными словами, после копирования шифрованного файла на дискету он не будет оставаться зашифрованным. Следует учитывать это и при копировании файлов на сетевые ресурсы, поскольку они могут размещаться на дисках с файловыми системами FAT.

Что необходимо учитывать при выполнении файловых операций? По умолчанию вновь создаваемые объекты *наследуют* те разрешения, которые присвоены их родителям. Так, файл будет иметь те же параметры безопасности, что и папка, в которой он создается. Иными словами, если вы создаете новый файл в папке, которой присвоен атрибут "зашифрованный", то этот файл также будет зашифрованным. Или если вы создаете файл в папке, к которой нет доступа пользователю `Иванов`, то и к файлу этот пользователь доступа не получит.

При операциях копирования файл *создается* заново. Поэтому по новому месту он всегда будет иметь атрибуты той папки, в которую скопирован. В результате если вы скопируете зашифрованный файл в незашифрованную папку, то файл в этой папке после завершения операции окажется незашифрованным. Если вы копируете обычный файл в папку с атрибутом "сжатый", то новый файл будет подвергнут динамическому сжатию.

Операции перемещения имеют некоторые особенности. Если файл перемещается *с одного диска на другой*, то операция фактически будет состоять из двух этапов: копирования файла, а потом удаления его по прежнему месту. Поэтому атрибуты файлу будут присвоены по правилам операции копирования. Файл будет иметь атрибут той папки, в которую он помещен.

Если файл перемещается *в пределах одного диска*, то операционная система не выполняет операцию копирования. Файл остается на прежнем месте, только в таблице размещения файлов для него меняется соответствующий указатель. Иными словами, все атрибуты файла остаются неизменными. То есть при перемещении незашифрованного файла в зашифрованную папку на том же диске информация в файле останется незашифрованной.

Результирующие права и утилиты

Как правило, в организации существует достаточно сложная структура групп пользователей с отличающимися правами доступа к информации. При этом часть прав наследуется от родительских групп, некоторые права прописываются за пользователями или группами явно. А для доступа по сети к совместно используемым ресурсам необходимо интегрировать как права доступа,

заданные для файловой системы, так и права доступа совместного использования.

Поскольку обычно пользователь одновременно входит в несколько групп, то определить, получит ли он в итоге право доступа к данному объекту, часто бывает очень сложно. Поэтому в системе введена возможность отображения *результирующего права* пользователя.

Для того чтобы узнать, какие права пользователь (группа) будет иметь по отношению к некоторому объекту, достаточно открыть свойства объекта, на вкладке **Безопасность** нажать кнопку **Дополнительно** и выбрать вкладку **Действующие разрешения**. После чего необходимо выбрать пользователя, для которого будут определяться действующие права, и посмотреть итоговый результат (рис. 5.14).

Примечание

Средствами групповой политики администратор имеет возможность отключения просмотра результирующих прав.

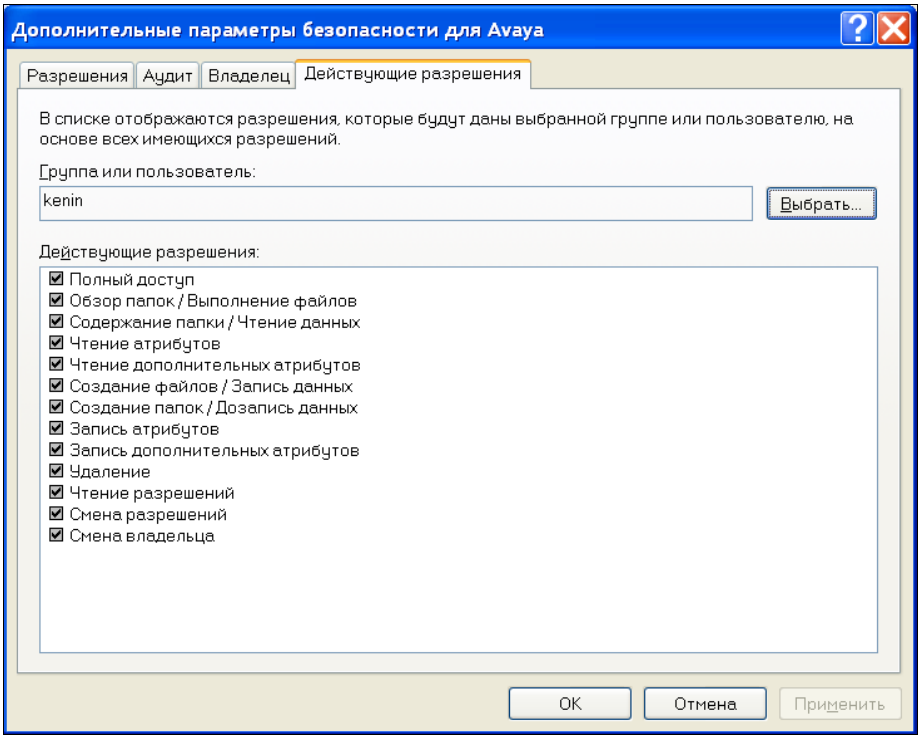


Рис. 5.14. Отображение действующих прав доступа к файлу для выбранного пользователя

Рекомендации по применению разрешений

Общая рекомендация при назначении прав доступа состоит в преимущественном использовании групп по сравнению с назначением прав для отдельных пользователей. Такой подход упрощает администрирование, позволяет гораздо быстрее, проще и понятнее устанавливать разрешения.

Например, для локального компьютера можно создать несколько локальных групп, объединить в них как пользователей данной системы, так и доменные учетные записи, после чего уже с использованием данных групп назначать разрешения на доступ к тем или иным объектам.

В общем случае рекомендуется придерживаться следующего порядка назначения разрешений. Необходимые учетные записи следует добавить в глобальные группы домена, глобальные группы домена включить в локальные группы домена и уже для этих локальных групп назначать желаемые разрешения.

Создание и удаление учетных записей

После установки операционной системы вы начинаете работу с правами учетной записи **Администратор** (Administrator — для интернациональных версий ОС). Пользователь **Администратор** обладает максимальными правами в данной операционной системе; используя права **Администратора** можно создавать, модифицировать, удалять другие учетные записи, выполнять любые операции по настройке системы и т. п.

Примечание

Обратите внимание, что после использования мастера установки Windows XP в режиме отображения страницы приветствий во время входа в систему название учетной записи администратора не показано на экране. Однако эта учетная запись может быть применена для работы с системой, причем обычно администраторы забывают о необходимости установки для нее пароля, что позволяет легко локально зайти в систему с правами администратора, предъявив "пустой" пароль.

Целесообразно назначить этой учетной записи длинный и сложный пароль, состоящий из цифр и символов только английского алфавита. Это упростит возможные операции по восстановлению операционной системы. Кроме того, в целях безопасности рекомендуется переименовать учетные записи администраторов[1] и запретить для анонимных пользователей просмотр базы идентификаторов безопасности.

Для управления учетными записями используются специальные оснастки (рис. 5.15): управления компьютером в локальном случае и оснастка управ-

[1] Сделать это в домене можно централизованно, используя групповую политику.

ления AD **Пользователи и компьютеры** при создании доменных пользователей.

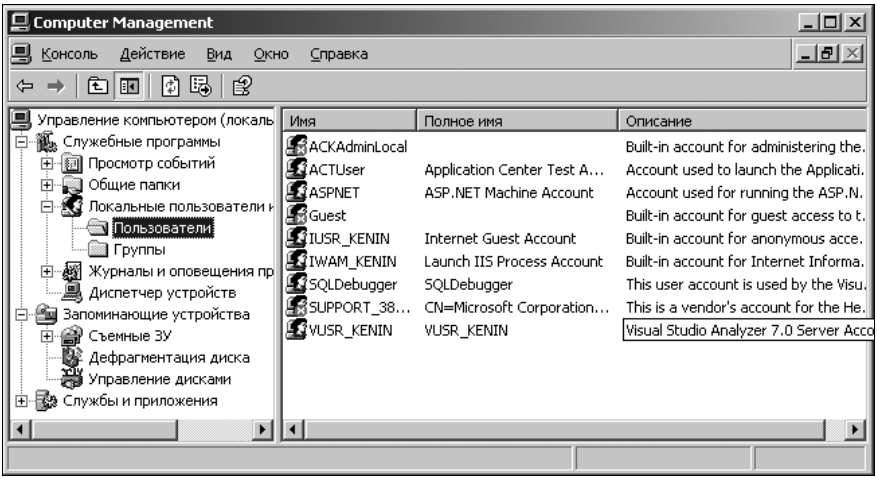


Рис. 5.15. Добавление нового пользователя локальной системы

При создании новых пользователей домена рекомендуется устанавливать для них требование смены пароля при первом входе в сеть.

Управлять учетной записью можно из командной строки. Так, добавить пользователя можно командой `NET USER <`*имя*`> <`*пароль*`> /ADD`, а удалить — `NET USER <`*имя*`> /DELETE`.

Опытные пользователи могут использовать сценарии Visual Basic для автоматизации типовых операций с учетными записями.

Примечание

В домене Windows учетные записи создаются и для компьютеров с операционными системами Windows NT/200*x*/XP/Vista. Эти учетные записи можно использовать для контроля доступа к сетевым ресурсам.

Если в организации используются дополнительные параметры учетной записи (название отдела, адрес и т. п.), то более удобно при создании нового пользователя перенести в его учетную запись максимум настроек, которые имеют аналогичные пользователи. Для этих целей служит операция *копирования учетной записи*. При копировании программа создает новую учетную запись, в настройки которой перенесены те параметры, которые не являются личными характеристиками. Например, новая учетная запись будет уже включена в те группы, в которые входила исходная учетная запись, но такой параметр, как номер телефона (который также может являться одной из характеристик пользователя), скопирован не будет.

Дополнительные параметры учетной записи

Каждая учетная запись имеет существенное количество дополнительных параметров, значения которых могут быть использованы в работе организации. Это дает администратору возможность объединять пользователей в группы, учитывая содержимое того или иного поля. Например, можно создать группу, объединяющую пользователей, находящихся в определенном офисе, и присвоить ей почтовый адрес.

Поля учетной записи могут заполняться с помощью окна свойств, вызываемого из оснастки управления службой каталогов (или управления компьютером — при правке локальных пользователей). Эти свойства можно запрашивать и устанавливать с помощью достаточно простых сценариев Visual Basic, однако более удобно выполнять соответствующие операции поиска и изменения данных на основе протокола LDAP *(см. разд. "LDAP-управление" ранее в данной главе)*, при этом администратору доступны практически любые критерии поиска необходимых записей.

Права учетной записи

В операционных системах класса Windows 9*x* любой пользователь системы мог выполнить любые действия. В системах на основе Windows NT при выполнении операций, которые могут повлиять на стабильность работы, осуществляется проверка наличия прав пользователя на выполнение этих действий.

Перечень контролируемых ситуаций крайне объемен. Например, проверяется наличие у пользователя разрешения на локальный вход в систему и на завершение работы компьютера, на установку нового оборудования и на удаление учетной записи, право на доступ к компьютеру по сети или право на отладку программ и т. д. Причем основная масса прав после установки системы даже не задействована: администратор может использовать имеющиеся параметры при последующей точной настройке системы.

Если файловая система на компьютере преобразована в NTFS, то дополнительно появляется возможность контролировать доступ к отдельным файлам и папкам, определяя соответствующие права доступа.

Права пользователей назначаются через оснастку **Локальная безопасность**, расположенную в группе административных задач. В случае работы в составе домена администраторы регулируют права пользователей с помощью соответствующих групповых политик. Использование этих инструментов достаточно очевидно, и мы не будем подробно описывать такие операции.

Восстановление параметров безопасности по умолчанию

В случае смены администраторов новому специалисту обычно не известны, например, те изменения прав доступа, которые выполнил прежний сотруд-

ник. В некоторых случаях некорректное назначение прав может повлиять на стабильность работы системы.

В Windows существуют специальные средства, которые позволяют вернуть параметры безопасности к тем значениям, которые определены для вновь устанавливаемой операционной системы. С этой целью используется оснастка **Анализ и настройка безопасности**. По умолчанию эта оснастка не включена в меню. Чтобы начать работу с ней, следует открыть консоль управления (команда `mmc`) и выполнить операцию добавления оснастки. В окне **Добавить изолированную оснастку** следует отметить строку **Анализ и настройка безопасности** и закрыть все последующие окна, нажимая на кнопки подтверждения операции.

В операционной системе хранятся шаблоны безопасности[1], разработанные поставщиком, для нескольких типовых конфигураций компьютера. Это шаблон настроек безопасности, соответствующий установке системы, шаблоны безопасности для компьютеров (отдельно для рабочих станций, серверов и контроллеров домена), соответствующие различным уровням защищенности: совместимого с программным обеспечением, разработанным до Windows 2000, и т. д.

Программа позволяет сравнить значения, определенные в этих шаблонах, с фактическими параметрами настройки системы. Полученные результаты сохраняются в виде базы данных, которая может быть проанализирована пользователем: все отличия настроек специально выделены в отчете программы.

Если администратор сочтет необходимым, то он может с помощью данной оснастки применить один из шаблонов безопасности — применение шаблона фактически означает установку соответствующих параметров системы (разрешений, прав) в те значения, которые определены в данном шаблоне.

Для анализа или применения настроек необходимо выполнить следующие действия:

1. Создать пустую базу данных.
2. Загрузить в нее желаемый шаблон.
3. Провести анализ и/или настройку системы.

Для применения шаблона следует выполнить команду **Настроить компьютер**. В завершение желательно проанализировать результаты операции.

Примечание

Обратите внимание на шаблон compatws.inf, который позволяет перейти в режим совместимости с Windows NT 4.0. В этом режиме учетным записям пользователей даются дополнительные права на доступ к ресурсам системы. В ре-

[1] Шаблоны по умолчанию размещены в папке %windir%\Security\Templates.

зультате появляется возможность запуска программ, не в полной мере совместимых с последними версиями операционной системы. Например, очень часто старые программы не запускаются именно потому, что они пытаются осуществить запись в реестр системы. Эта операция в новых ОС разрешена только администраторам, но после применения данного шаблона необходимые разрешения будут предоставлены.

Автоматически создаваемые учетные записи

При установке операционной системы автоматически создается несколько учетных записей пользователей. Ранее мы упоминали учетную запись **Администратор**. Эта учетная запись особая. Ранее ее нельзя[1] было даже удалить или исключить из группы администраторов. Сделано это было из соображений безопасности, чтобы пользователь случайно не удалил всех администраторов и система не стала неуправляемой.

Другая автоматически создаваемая учетная запись — это **Гость** (Guest). Она не имеет пароля и предназначена для обеспечения возможности работы с данным компьютером пользователя, у которого в системе нет учетной записи. К примеру, вы приезжаете со своим ноутбуком в другую организацию и хотите распечатать документ. Если в той организации принтер предоставлен в совместное использование и действует учетная запись **Гость**, то вы можете подключиться к принтеру и выполнить печать, в противном случае вам должны сообщить имя входа и пароль, которые можно использовать для подключения к серверу печати.

В рабочих станциях Windows NT 4.0 эта учетная запись по умолчанию была доступна. В серверных операционных системах и в версиях рабочих станций Windows 2000/XP/Vista учетная запись **Гость** по соображениям безопасности заблокирована. Однако если ваша сеть полностью автономна и объединяет немного компьютеров, то для облегчения использования сетевых ресурсов вы можете ее разблокировать.

Так делает, например, мастер конфигурирования домашней сети: если вы определили, что компьютер используется в рамках домашней сети, то мастер разрешает использование учетной записи **Гость**. В этом случае, если вы разрешите совместное использование ресурсов компьютера, то к ним будет возможно подключение любых пользователей, независимо от того, существуют ли для них учетные записи на вашем компьютере или нет.

Учетная запись **HelpAssisstant** применяется в случаях обращения к удаленному помощнику. Удаленный пользователь подключается к компьютеру с правами, предоставленными данной учетной записи.

---

[1] В версиях, более ранних чем Windows XP. В новых версиях Windows упомянутые операции допустимы.

Учетная запись **SUPPORT_*номер*** используется службами технической поддержки Microsoft. Обычно рекомендуют просто удалить эту учетную запись.

Если на компьютере устанавливается информационный сервер Интернета (Internet Information Server, IIS), то создаются две учетных записи. Это **IUSR_*имя_компьютера*** и **IWAM_*имя_компьютера***. Учетная запись **IUSR_*имя_компьютера*** применяется при предоставлении Web-ресурсов анонимному пользователю. Иными словами, если информационный сервер Интернета не использует аутентификацию пользователя (предоставляет ресурсы анонимно), то в системе такой пользователь регистрируется под именем **IUSR_*имя_компьютера***. Вы можете, например, запретить анонимный доступ к каким-либо ресурсам информационного сервера, если исключите чтение таких файлов данным пользователем. Пароль пользователя **IUSR_*имя_компьютера*** создается автоматически и синхронизируется между операционной системой и информационным сервером.

Пароли учетных записей **IUSR_*имя_компьютера*** и **IWAM_*имя_компьютера*** легко можно узнать при помощи сценария, имеющегося на компьютере. Найдите файл Adsutil.vbs (обычно он расположен в папке административных сценариев IIS, например, InetPub\AdminScripts), замените в текстовом редакторе строку сценария[1]

```
IsSecureProperty = True
```

на

```
IsSecureProperty = False
```

и выполните:

```
cscript.exe adsutil.vbs get w3svc/anonymoususerpass
```

для отображения пароля IUSR-пользователя или

```
cscript.exe adsutil.vbs get w3svc/wamuserpass
```

для показа пароля IWAM-пользователя.

Учетная запись **IWAM_*имя_компьютера*** используется для запуска процессов информационного сервера (например, для обработки сценариев на страницах с активным содержанием). Если вы случайно удалите какую-либо из этих записей и вновь создадите одноименную, то, скорее всего, столкнетесь с неработоспособностью информационного сервера. Конечно, можно обратиться к справочной базе разработчика, правильно настроить службы компонентов на использование новой учетной записи, синхронизовать с помощью специальных сценариев пароли учетных записей и т. п. Но гораздо эффективнее в этой ситуации будет просто удалить службу информационного сер-

[1] Иначе сценарий покажет пароль в виде звездочек.

вера и вновь добавить этот компонент, предоставив программе установки выполнить все эти операции.

Кроме перечисленных учетных записей новые бюджеты часто создаются прикладными программами в процессе их установки. Обычно создаваемые таким образом учетные записи имеют необходимое описание в своих свойствах.

Учетная запись *Система*

При необходимости можно настроить службы для старта от имени любого пользователя. Однако в этом случае вам необходимо установить соответствующей учетной записи постоянный пароль и предоставить ей достаточно большие права по отношению к локальному компьютеру. Из такого сочетания требований очевидно вытекает настоятельная рекомендация: не использовать учетные записи пользователей для запуска служб по соображениям безопасности.

Учетная запись **Система** (Local System) предназначена для запуска служб компьютера. Она обладает полными правами по отношению к локальному компьютеру и фактически является частью операционной системы. Ее права существенно выше, чем права любой учетной записи пользователя. Для учетной записи **Система** выполняется обход проверок безопасности, поэтому для нее *не существует пароля*, который можно было бы дешифровать или взломать. Учетная запись **Система** не может быть использована для доступа к сетевым ресурсам.

Использования учетной записи **Система** для запуска служб компьютера без особых на то причин следует избегать, поскольку данное решение понижает уровень безопасности. Например, если пользователю удастся подменить запускаемый файл службы на пакетный файл и затем прервать выполнение этого пакетного файла нажатием комбинации клавиш <Ctrl>+<C>, то он получит возможность запуска в этом командном окне задач с приоритетом **Системы**. Поэтому в последних версиях Windows (XP/Server 2003) для использования при запуске служб введены еще две учетных записи. Это **Local Service** и **Network Service**. Так же, как и учетная запись **Система**, эти учетные записи являются частью самой операционной системы и *не имеют паролей*. При этом они обладают гораздо меньшими правами, чем учетная запись **Система**[1]. Если **Local Service** используется также только при запуске локальных программ, то **Network Service** может осуществлять доступ к сетевым ресур-

[1] Но большими правами, чем пользователь. Обе учетные записи по умолчанию имеют права пользователя и аутентифицированного пользователя и привилегии **SE_AUDIT_NAME**, **SE_CHANGE_NOTIFY_NAME**, **SE_UNDOCK_NAME**.

сам. При этом данная учетная запись аутентифицируется в удаленной системе как учетная запись соответствующего компьютера.

Примечание

Следует быть внимательным при назначении прав доступа к локальным ресурсам компьютера. Автор неоднократно сталкивался с ситуацией, когда недостаточно опытные пользователи, желая ограничить доступ к ресурсам своего компьютера, работающего в составе сети, запрещали доступ к файлам на диске всем, кроме самого себя. Исключив специальных пользователей, они сделали невозможным запуск многих служб, необходимых для работы операционной системы.

Встроенные группы

При установке операционной системы на компьютере автоматически создается несколько групп. Для большинства случаев персонального использования этих групп достаточно для безопасной работы и управления системой.

- **Администраторы** (Administrators).

  Члены этой группы имеют все права на управление компьютером. После установки в системе присутствуют только пользователи-члены этой группы (в Windows XP в ходе установки можно создать несколько администраторов системы, в предыдущих версиях создается только одна запись).

- **Пользователи** (Users).

  Это основная группа, в которую надо включать обычных пользователей системы. Членам этой группы запрещено выполнять операции, которые могут повлиять на стабильность и безопасность работы компьютера.

- **Опытные пользователи** (Power Users).

  Эти пользователи могут не только выполнять приложения, но и изменять некоторые параметры системы. Например, создавать учетные записи пользователей, редактировать и удалять учетные записи (но только те, которые были ими созданы), предоставлять в совместный доступ ресурсы компьютера (и управлять созданными ими ресурсами). Но опытные пользователи не смогут добавить себя в число администраторов системы, не получат доступ к данным других пользователей (при наличии соответствующих ограничений в свойствах NTFS, у опытных пользователей отсутствует право становиться владельцем объекта), кроме того, они не смогут выполнять операции резервного копирования, управлять принтерами, журналами безопасности и протоколами аудита системы.

- **Операторы резервного копирования** (Backup Operators).

  В эту группу следует включить ту учетную запись, от имени которой будет осуществляться резервное копирование данных компьютера. Основное

отличие этой группы в том, что ее члены могут "обходить" запреты доступа к файлам и папкам при операции резервного копирования данных. Независимо от установленных прав доступа в резервную копию данных будут включены все отмеченные в операции файлы, даже если у оператора резервного копирования нет права чтения такого файла.

Примечание

Учетная запись с правами оператора резервного копирования является достаточно серьезной брешью в системе безопасности организации. Как правило, особое внимание "безопасников" уделяется пользователям, имеющим административные права. Да, они могут стать владельцами любой информации, доступ к которой для них явно запрещен. Но при этом такие действия протоколируются и контролируются службой безопасности предприятия. Пользователь, на которого возложена рутинная вроде бы обязанность резервного копирования, легко может выполнить резервную копию всех данных и восстановить секретную информацию из этой копии на другой компьютер, после чего говорить о наличии установленных прав доступа к файлам и папкам уже бессмысленно. Но есть и более простые способы копирования информации, право доступа к которой запрещено на уровне файловой системы. В составе Resource Kit имеется утилита для массового копирования файлов — *robocopy.exe*[1]. Эта программа может выполнять копирование данных в режиме использования права резервного копирования (естественно, что она должна быть запущена пользователем, состоящим в группе операторов резервного копирования). В результате в новую папку будут скопированы все файлы, причем пользователю даже не нужно становиться владельцем файлов — все запреты будут уже сняты.

- **Гости** (Guests).

  Эта группа объединяет пользователей, для которых действуют специальные права для доступа "чужих" пользователей. По умолчанию в нее включена только одна заблокированная учетная запись **Гость.**

- **HeplSevicesGroup.**

  Группа предоставляет типовой набор прав, необходимый специалистам службы техподдержки. Не следует включать в нее других членов, кроме учетной записи, созданной по умолчанию.

- **Remote Desktop Users.**

  Эта группа появилась в операционных системах Windows XP. Ее члены могут осуществлять удаленное подключение к рабочему столу компьюте-

[1] Robocopy предназначена для того, чтобы скопировать структуру файлов из одной папки в другую. Если на файлы наложены ограничения доступа, то выполнять такую операцию штатными средствами (через резервное копирование и восстановление данных) не всегда удобно. Robocopy позволяет переместить данные, сохранив всю структуру прав. Возможность "снятия" ограничений, описываемая в настоящем разделе, просто является одной из функций данной утилиты.

ра. Иными словами, если вы хотите иметь возможность удаленно подключиться к своему компьютеру, то необходимо включить в эту группу соответствующую учетную запись. По умолчанию членами этой группы являются администраторы локального компьютера.

- **DHCP Administrators.**

  Группа создается только при установке DHCP. Пользователи группы имеют право на конфигурирование службы DHCP (например, с помощью графической оснастки управления или командой `netsh`). Используется при делегировании управления DHCP-службой.

- **DHCP Users**, **WINS Users.**

  Группы создаются только при установке соответствующих служб. Пользователи групп имеют право только на просмотр параметров настройки служб DHCP (или WINS). Применяются при делегировании прав техническому персоналу (например, для сбора информации о состоянии сервисов).

- **Network Configuration Operators.**

  Пользователи группы имеют право изменения TCP/IP-параметров. По умолчанию группа не содержит членов.

- **Print Operators.**

  Члены группы могут управлять принтерами и очередью печати.

В системе присутствуют и другие группы, на описании которых мы не будем особо останавливаться (**Account Operators**, **Pre-Windows 2000 Compatible Access**, **Server Operators** и т. д.).

Специальные группы

В операционной системе существуют так называемые *специальные группы*, членством в которых пользователь компьютера управлять не может. Они не отображаются в списке групп в оснастках управления группами, но доступны в окнах назначения прав доступа.

Это группы **Все** (Everyone), **Интерактивные пользователи** (Local Users), **Сетевые пользователи** (Network Users), **Пакетные файлы** (Batch), **Прошедшие проверку** (Authenticated) и т. д. Предназначение групп ясно уже по их названию. Так, в группу **Интерактивные пользователи** автоматически включаются все пользователи, осуществившие вход в систему с консоли (клавиатуры). **Сетевые пользователи** — это те пользователи, которые используют ресурсы данного компьютера через сетевое подключение и т. п.

Данные группы предназначены для более точного распределения прав пользователей. Например, если вы хотите, чтобы с каким-либо документом была

возможна только локальная работа, то можно просто запретить доступ к нему сетевых пользователей.

Заострим внимание читателей на группе **Все**, поскольку именно с ней связано наибольшее количество ошибок в предоставлении прав доступа. Эта группа включает не любых пользователей, а только тех, кто имеет учетную запись на данном компьютере. Иными словами, если вы предоставили ресурс в общий доступ с правами чтения для группы **Все**, то использовать его могут только те, кто "прописан" на данном компьютере. Если вы предпочитаете, чтобы ресурс мог использовать действительно "кто угодно", то для этого нужно разрешить использование учетной записи **Гость.**

Примечание

В последних версиях Windows пересматривался состав группы **Все**. Во избежание ошибок следует уточнить состав данной группы в каждом конкретном случае.

Рекомендации по использованию операции *Запуск от имени...*

По соображениям безопасности не рекомендуется использовать для текущей работы учетную запись, обладающую административными правами. Смысл этого требования очень прост. Если на компьютере работает неопытный пользователь, то он не сможет что-либо испортить в настройках системы и привести ее в нерабочее состояние. Кроме того, в повседневной практике очень легко встретиться с какой-либо скрытой вредоносной программой. Если при запуске такой программы она не будет обладать административными правами, то возможностей нанести вред компьютеру у нее будет существенно меньше.

Однако на практике пользователям периодически приходится выполнять различные административные действия. Например, установить драйвер для нового внешнего устройства хранения информации, на котором вы принесли для просмотра взятый у приятеля видеофильм, и т. п. В операционной системе Windows NT 4.0 при возникновении такой проблемы нужно было завершить работу пользователя, войти в систему с правами администратора, выполнить операции, а потом вновь войти в систему под своей учетной записью.

Понятно, что несмотря на все рекомендации, большинство пользователей для удобства работали с правами учетной записи администратора. В операционных системах Windows 200*x*/XP предусмотрен специальный механизм для быстрого запуска программ с использованием административных прав. Это операция **Запуск от имени...** (Run As).

При использовании команды **Запуск от имени** текущий пользователь может запустить необходимую программу от имени любого пользователя, если ему известен соответствующий пароль входа в систему (или он имеет смарт-карту этого пользователя).

Примечание

Чтобы иметь возможность запуска программы от имени другого пользователя, на компьютере должен быть создан ярлык этой программы.

Команда запуска от другого имени появляется в свойствах ярлыка, если вызывать это окно при нажатой клавише <Shift>. Иными словами, нужно нажать клавишу <Shift> и щелкнуть по ярлыку правой кнопкой мыши, после чего в открывшемся меню появится строка с данной командой.

После вызова данной команды на экране отобразится окно, в котором необходимо определить учетную запись, от имени которой будет выполняться программа. Затем эта программа (и все программы, которые будут, в свою очередь, ею запущены) будет исполняться с правами выбранной учетной записи.

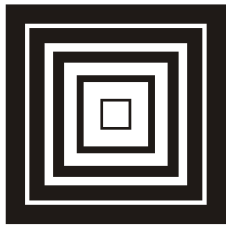
Примечание

Обратите внимание, что поскольку в меню системы представлены именно ярлыки соответствующих программ, то запустить нужную программу от имени другого пользователя можно, щелкнув правой кнопкой мыши по значку программы при нажатой клавише <Shift>.

Ролевое управление

Современные прикладные программы предусматривают работу с данными пользователей с различающимися функциональными обязанностями. Для регулирования прав доступа к возможностям программы принято использовать *ролевое управление*. Роль представляет собой предварительно настроенный набор прав пользователя, выполняющего определенные обязанности (директор, главный бухгалтер, кассир и т. п.). При подключении нового пользователя такой системы администратору достаточно предоставить ему тот или иной предварительно подготовленный набор прав.

С точки зрения администратора предпочтителен вариант, когда для предоставления пользователю какой-либо роли его необходимо включить в соответствующую группу безопасности. В этом случае появляется возможность распространить ролевое управление и за пределы прикладной программы (например, предоставить доступ к файловым ресурсам сервера также на основе ролей данной задачи).



ГЛАВА 6

Управление с помощью групповых политик

Одним из самых эффективных способов управления компьютерной сетью является использование *групповых политик*. Политика представляет собой набор настроек и правил, которые могут быть применены как к одному компьютеру, так и к целой группе.

При помощи политики возможно:

- установить на компьютер программное обеспечение;
- настроить права доступа к файлам и папкам на дисках с файловой системой NTFS;
- лимитировать членство пользователей в группах;
- изменить параметры реестра, внести настройки в режимы запуска служб компьютера;
- установить параметры использования прикладных программ

и т. п.

Количество настроек, которые можно регулировать при помощи групповых политик, растет с каждой версией операционной системы. Так, после выпуска SP2 для Windows XP администратору доступно более 1300 параметров, выпуск Vista увеличил это число еще более чем вдвое. Мы не будем описывать использование каждой возможности, каждого параметра групповой политики. Во-первых, объем этого материала в несколько раз превысит объем данной книги, а во-вторых, соответствующие описания легко найти в справочной системе компьютера.

Настраивать все параметры, существующие в групповой политике, не имеет смысла. После их применения работать на локальной системе станет практически невозможно из-за введенных ограничений. В каждой конкретной организации перечень параметров управления должен определяться индивиду-

ально. Например, если есть постоянный канал доступа в Интернет, то целесообразно централизованно настроить программу обозревателя на использование соответствующих параметров доступа. Таким образом, новому пользователю не придется вносить никаких индивидуальных настроек в систему.

Групповые и системные политики

Понятие "групповая политика" введено с появлением домена на основе Windows 2000. Однако возможность централизованной настройки пользовательских параметров существовала и в доменах на основе Windows NT 4.0, правда, тогда это называлось просто политикой (политикой учетных записей, политикой компьютеров домена) или системной политикой (system policy).

Если в вашей сети (домене) работают не только компьютеры на основе Windows 200*x*/XP/Vista, то групповые политики к системам на основе Windows NT 4.0, Windows 9*x* применяться не будут. Администратор может в этом случае использовать системные политики для настройки, хотя, конечно, перечень регулируемых с их помощью параметров весьма скромен.

Примечание

Список настраиваемых с помощью политики параметров отображается в редакторе. Администратор не имеет возможности добавить в него какие-либо иные настройки.

Для создания системной политики необходима программа Windows NT 4.0 System Policy Editor (poledit.exe, рис. 6.1). Она по умолчанию устанавливается на контроллеры домена и может быть также найдена на дистрибутивных дисках Windows (System Policy Editor в варианте для Windows 95/98). Программа позволяет определить настройки по умолчанию для компьютеров и пользователей, а также добавить индивидуальные настройки для систем.

После определения настроек нужно сохранить данные: для систем на основе Windows NT 4.0 в файле с именем Ntconfig.pol, а для систем Windows 95/98 — Config.pol. Затем эти файлы должны быть помещены в папку %systemroot%\SYSVOL\sysvol\<domain name>\SCRIPTS[1].

Для редактирования групповых политик в Windows 200*x*/XP/Vista используется специальная оснастка консоли управления. Как правило, все параметры снабжены подробными комментариями, и выполнение операций не требует дополнительных описаний (рис. 6.2).

[1] Для контроллеров домена на основе Windows NT 4.0 Server это должна быть папка %systemroot%\system32\Repl\Import\Scripts.

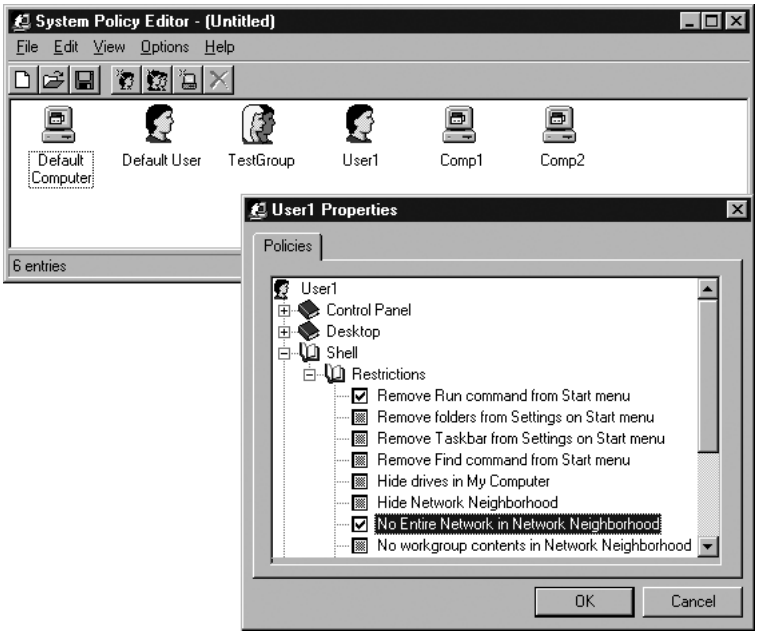


Рис. 6.1. Интерфейсы редактора системных политик Windows 9x/NT 4.0

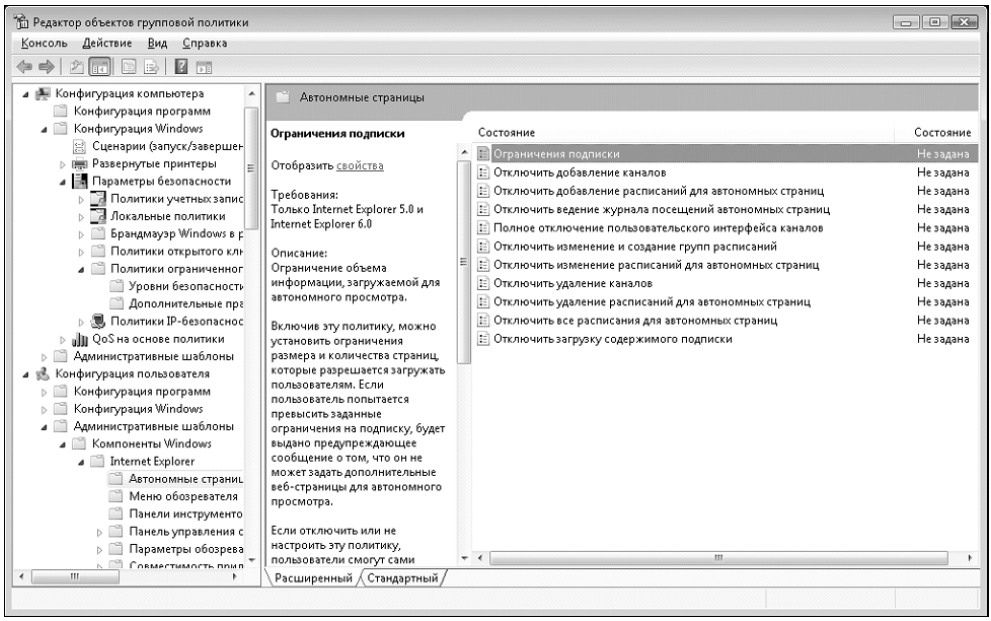


Рис. 6.2. Редактор групповой политики в Windows Vista

Порядок применения политик и разрешения конфликтов

Политики могут быть назначены для различных объектов: локальный компьютер, сайт, домен, любое организационное подразделение, причем на каждом уровне может быть создано несколько политик.

В разных политиках один и тот же параметр может быть определен с отличающимися значениями. Например, в связи со спецификой обрабатываемой информации администратор домена может потребовать использования более строгих правил создания паролей, чем те, которые заданы администратором родительского домена. Какие правила действуют при разрешении подобных ситуаций?

Во-первых, политики применяются в соответствии с иерархической структурой организации (структурой службы каталогов). Сначала используется локальная политика, а потом последовательно применяются политики с самого верхнего структурного уровня до самого нижнего (от общего к частному). При наличии на одном уровне нескольких политик, они применяются по очереди снизу вверх списка (самая верхняя политика в списке будет применена на данном уровне последней).

При этом при наличии конфликтующих значений будет использован параметр, задаваемой *следующей* по очереди политикой. На практике это соответствует применению политики подразделения — "непосредственного начальника". Если существует конфликт параметров политики *компьютер* и *пользователь* одного уровня, то обычно больший вес имеет параметр, заданный для компьютера.

Примечание

Из этого правила существуют некоторые исключения. Так, параметры политики паролей домена (максимальный срок действия, минимальная длина, требования к сложности и т. п.) могут определяться в политиках подразделений, однако будут использоваться *только* значения, заданные в политике домена по умолчанию. Тем не менее параметры паролей локальных учетных записей могут быть установлены *любой* примененной политикой.

Во-вторых, администраторы могут устанавливать для политик признаки запрета перезаписи и/или обязательного значения параметра. Если политика описана как не допускающая изменения параметров, то ее настройки будут иметь преимущество и не смогут быть изменены значениями следующей применяемой политики. Администратор может также указать, что значения политики не должны *наследоваться* от политики более высокого уровня. В этом случае "отсекаются" настройки политик, которые применялись *до* данного уровня.

Примечание

Если возникает конфликт требований "не переписывать" и "не наследовать", то преимущество имеет установка "не переписывать". Фактически это означает, что администратор подразделения более высокого уровня *всегда* сможет применить свои настройки.

В-третьих, для более точного регулирования применения параметров настроек администратор может использовать права доступа к политике. Так, если администратор хочет, чтобы политика домена по умолчанию не применялась к его собственной системе, то он может запретить применение параметров этой политики к конкретному компьютеру.

Кроме того, в доменах на основе Windows Server 2003 существует возможность уточнять область применения политики на основе WMI-фильтров. Администратор, знакомый с основами программирования и использования WMI *(см. разд. "Windows Management Interface" главы 13)*, может создать фильтры применения политики, учитывающие любые параметры конфигурации систем (как аппаратного, так и программного обеспечения).

"Обход" параметров пользователя

В некоторых случаях необходимо специальным образом учитывать параметры, задаваемые политиками для пользователей. Например, при работе на терминальном сервере не нужно устанавливать программное обеспечение, определенное групповыми политиками для каких-либо пользователей. Для таких случаев предназначен параметр **Loopback** свойств групповой политики.

Параметр позволяет задать два варианта "обхода" политики пользователя. В режиме **Merge** система применяет все предусмотренные для данного компьютера и пользователя политики, после чего еще один раз применяет *все политики компьютеров*. То есть, если для данного пользователя и компьютера должны быть применены по иерархии три политики, назовем их А1, А2, А3, то при выборе режима **Merge** параметра **Loopback** политики будут применены в следующем порядке: А1 (параметры компьютера + параметры пользователя), А2 (параметры компьютера + параметры пользователя), А3 (параметры компьютера + параметры пользователя), А1 (параметры компьютера), А2 (параметры компьютера), А3 (параметры компьютера).

Режим **Replacement** предусматривает применение *только* параметров политики, относящихся к компьютерам. Для приведенного выше примера при выборе данного режима были бы применены следующие политики: А1 (параметры компьютера), А2 (параметры компьютера), А3 (параметры компьютера).

Время применения политик

Политика компьютера применяется при каждом включении компьютера. Политика пользователя — при каждом входе в систему (после нажатия комбинации клавиш <Ctrl>+<Alt>+<Del>). По умолчанию политики применяются *синхронно*[1]. Это значит, что на экране не появится приглашение нажать заветные три клавиши до тех пор, пока не будет применена политика компьютера, а пользователь не увидит своего рабочего стола (после ввода пароля) до завершения применения пользовательской политики.

Во время работы компьютера система проверяет наличие изменений групповых политик. По умолчанию это происходит каждые полтора часа. Если политика изменена, то она будет вновь применена к системе. Если изменений не обнаружено, то никаких действий не производится.

Примечание

Поскольку политики меняются редко, то пользователь, обладающий соответствующими правами на локальном компьютере, может изменить параметры, задаваемые групповой политикой, на свои значения, которые — при условии невыключения компьютера — будут продолжать действовать весьма длительное время[2].

Для того чтобы вручную обновить политику на локальном компьютере, следует воспользоваться командой `gpupdate /force`[3]. Для ускорения процесса возможно использовать дополнительный ключ (`target`), определяющий часть применяемой политики (компьютер или пользователь).

Последствия отключений политик

Параметры политик условно можно разделить на две группы. Первая группа — это параметры настройки, существующие во временных ключах реестра системы. Действует политика — есть ключи. Политика отключена — ключи не создаются[4]. Иными словами, отключение политики осуществится "безболезненно".

---

[1] При желании можно переопределить порядок применения, например сменить синхронный вариант на асинхронный и т. д.

[2] Администратор может задать правило обязательного применения политики при каждой очередной проверке. Однако такое решение приводит к существенному росту затрат вычислительной мощности и не применяется в обычной практике.

[3] Для систем на базе Windows 2000 (и Windows XP без SP1) необходимо использовать команду `secedit` (`secedit /refreshpolicy {machine_policy user_policy} /enforce`).

[4] Точнее, при отключении политики связанные с ней ключи реестра удаляются.

Вторая группа параметров задает значения *существующих*[1] ключей реестра. В первую очередь это свойственно настройкам, импортируемым из файлов *административных шаблонов* (с расширением adm).

Если политика устанавливает такой параметр, то снятие политики *ничего не меняет в настройках* системы. Ведь параметр реестра уже создан, а отсутствие политики означает просто сохранение его в том значении, которое было установлено политикой. Чтобы восстановить значения по умолчанию для таких параметров, администратору недостаточно просто снять политику. Нужно создать новые настройки, которые соответствуют значениям настройки по умолчанию, и *применить* их к компьютерам (пользователям).

Поэтому если необходимость применения какой-либо политики отпала, то рекомендуется просто отключить привязку (link) данной политики к конкретному подразделению, а саму политику не удалять. Во-первых, эти настройки могут вам опять понадобиться. А во-вторых, наличие ранее выполнявшихся настроек может помочь проанализировать действующие в подразделении параметры компьютеров и пользователей.

Рекомендации по применению политик

Главная рекомендация состоит в том, чтобы *не изменять политику по умолчанию*. Не стоит вносить изменений в действующую политику по умолчанию. Если возникнет какая-либо серьезная ошибка в политике, то возврат к начальному состоянию приведет к удалению не только последних настроек, но и всех других параметров, тщательно настраиваемых в течение долгого времени.

Поэтому создавайте *новые политики* для основных административных действий по управлению системой. В результате для изменения настроек вам необходимо только отключать/включать привязку политик к организационной структуре.

Если ваши настройки относятся только к параметрам компьютера или только к пользователю, то не забывайте устанавливать признак применения лишь соответствующей части политики. Это повысит скорость обработки политик на компьютере.

Контейнеры *Computers* и *Users*

После установки службы каталогов в структуре присутствует контейнер **Computers**, в котором по умолчанию создаются объекты типа *компьютер*, и

[1] Или создает такие ключи при первом применении. Главное, что такие параметры не будут удалены при снятии политики.

Users с объектами учетных записей пользователей и групп домена. Это такие же контейнеры, как и другие в структуре каталогов, за исключением того, что для них *не могут быть созданы групповые политики*. Иными словами, к объектам в этих папках применяются политики домена и предприятия.

Все остальные OU, создаваемые администратором, могут иметь связанные с ними групповые политики. При необходимости в этих OU могут создаваться объекты компьютеров и пользователей (или переноситься в них из других OU).

Рекомендации по применению групповых политик

Работа с групповыми политиками, определяющими параметры настройки оборудования или программ, обычно не вызывает сложностей. Параметры хорошо комментированы (см. рис. 6.2), поэтому эффект от их включения вполне предсказуем. Сложности обычно вызывает использование групповых политик для установки программного обеспечения и ограничения запуска прикладных программ. Рассмотрим подробнее данные групповые политики.

Примечание

В случае ошибочных действий при редактировании групповых политик домена их можно вернуть к исходным значениям (соответствующим состоянию после установки системы) с помощью утилиты `dcgpofix` (только на Windows 2003 Server). Подробности запуска можно получить, запустив команду `dcgpofix /?`.

Политики по установке программного обеспечения

С помощью групповых политик можно устанавливать программы на локальные системы. Использование таких возможностей интуитивно понятно. Необходимо создать соответствующий пакет установки и включить его в групповую политику.

Что необходимо учесть администратору при работе с такими политиками.

Во-первых, в качестве установочного пакета можно использовать файл либо в формате MSI, либо в формате ZAP. ZAP-формат используется для продуктов третьих фирм и является текстовым файлом с описанием особенностей предполагаемой установки. Формат файла приведен в KB231747. Мы просто процитируем часть данной статьи с рекомендациями по созданию соответствующих строк. По приведенному образцу читатель легко сможет создать zap-файл для любой программы.

```
[Application]
; Only FriendlyName and SetupCommand are required,
; everything else is optional.

; FriendlyName is the name of the program that
; will appear in the software installation snap-in
; and the Add/Remove Programs tool.
; REQUIRED
FriendlyName = "Microsoft Excel 97"

; SetupCommand is the command line used to
; run the program's Setup. With Windows Server 2003
; and later you must specify the fully qualified
; path containing the setup program.
; Long file name paths need to be quoted. For example:
; SetupCommand = "\\server\share\long _ ; folder\setup.exe" /unattend
; REQUIRED SetupCommand = "\\server\share\setup.exe"

; Version of the program that will appear
; in the software installation snap-in and the
; Add/Remove Programs tool.
; OPTIONAL
DisplayVersion = 8.0

; Version of the program that will appear
; in the software installation snap-in and the
; Add/Remove Programs tool.
; OPTIONAL
Publisher = Microsoft
```

Во-вторых, установка программы должна проводиться в "тихом" режиме, т. е. без диалога с пользователем. Например, не должен запрашиваться серийный номер продукта. Подготовка такого инсталляционного пакета в общем случае является далеко не тривиальной задачей *(см. главу 14)*.

В-третьих, установка программ может быть включена в политику как в раздел *компьютер*, так и *пользователь*. В первом случае установка программ будет произведена на систему, они будут доступны для любого пользователя. Обратите внимание, что программы, установленные в режиме *для пользователя*, обычно не могут быть обновлены с помощью средств автоматического обновления программного обеспечения. Также следует учитывать возможность работы подобного пользователя на терминальном сервере. В этом случае администратору следует либо дорабатывать политику ограничений для терминального сервера, либо включать опцию **lookback** *(см. разд. "„Обход"*

параметров пользователя" ранее в этой главе) для того, чтобы исключить установку программ на терминале.

Примечание

Если политика предусматривает установку программного обеспечения *для компьютера* из общей сетевой папки, то доступ к такой папке будет осуществляться от имени компьютера. При назначении прав доступа обратите внимание, что учетные записи компьютеров не входят в группу пользователей домена, а являются только членами группы компьютеров домена. Поэтому следует разрешить доступ к подобным общим папкам, по крайней мере учетным записям, прошедшим проверку (аутентифицированным пользователям).

Другая особенность использования групповой политики касается режимов установки: *публикация* или *назначение*. *Опубликованные* программы по умолчанию просто появляются в перечне задач, которые можно установить через задачу **Установка/удаление программ** в Панели управления. В случае использования *назначенных программ* в системе в меню **Пуск** появляется ярлык к ним, при первом вызове которого производится установка соответствующего программного обеспечения.

Политики ограниченного использования программ

В Windows XP/Vista и Windows 2003 Server[1] групповые политики позволяют регулировать перечень программ, запускаемых на пользовательских компьютерах. Кроме реализации корпоративной политики в части "запрещенных" и "разрешенных" программ, данный механизм позволяет эффективно защищать компьютеры от троянских коней и других вирусов, блокируя запуск неизвестных кодов.

Политика ограниченного использования программ состоит из двух частей: *политики по умолчанию* и *политики исключений*.

Политика по умолчанию определяет поведение системы в случае отсутствия явных указаний: либо все запрещать, либо все разрешать. Если администратор компьютера заранее знает перечень программ, с которыми будет работать пользователь, то удобнее использовать запрет по умолчанию и явно разрешить запуск программ по списку. В противном случае следует разрешить запуск программ по умолчанию и запретить запуск "подозрительного" или нежелательного для организации ПО.

Варианты политик ограниченного использования

Разрешения/запреты на запуск конкретных программ могут формироваться на основе следующих критериев.

[1] Для систем Windows 2000 политики программных ограничений игнорируются.

Примечание

В качестве исполняемых файлов в правилах могут указываться не только файлы программ, но и все файлы с расширениями, зарегистрированными для автоматического запуска программ на основе ассоциаций. Этот перечень можно видоизменить при формировании политики ограничений программного обеспечения.

- **Хэш.**

  При старте программы проверяется хэш ее программного кода и сравнивается со значением, записанным во время создания правила. В случае совпадения запуск программы разрешается (или запрещается, если правило создается для блокировки), иначе — блокируется (соответственно разрешается).

  Данное правило жестко регулирует возможности использования ПО и не разрешает пользователю "собственными силами" обойти это ограничение. Например, запрет на основе хэш-правила не даст использовать программу даже в случае переименования ее исполняемого файла, копирования его в другую папку и т. д.

  Недостаток критерия — некоторое замедление *каждого* запуска программы из-за подсчета ее хэша и сравнения полученного значения с контрольным. Кроме того, в случае обновления версии программного обеспечения администратору придется переопределять данное правило (поскольку хэш запускаемого файла новой версии программы будет отличен от прежнего).

- **Сертификат.**

  В этом случае система при попытке запуска программы проверяет наличие у нее цифровой подписи — соответствующего сертификата от доверенного удостоверяющего центра. Так же, как и в случае использования правила контроля хэша, система затрачивает некоторые ресурсы при запуске программы. Однако данный подход более гибок, поскольку позволяет администратору производить обновления программного обеспечения при условии наличия у новых программ цифровых подписей.

  Недостаток критерия — в отсутствии в настоящее время сертификатов у большей части используемых программ. В то же время у администратора системы имеются в распоряжении средства для создания цифровой подписи к сценариям или ПО собственной разработки *(см. разд. "Создание подписей к макросам MS Office" главы 13)*.

- **Путь.**

  Правило, создаваемое на основе указания пути к исполняемому файлу, является самым удобным в использовании, но одновременно и самым "ненадежным".

При создании правила необходимо указать путь к программным файлам. Причем возможно указание как пути к папке (в этом случае правило будет действовать для всех файлов в этой папке и во всех вложенных в нее каталогах), так и к конкретному файлу. Допускается указание UNC-путей и использование в записи масок и переменных. Кроме того, правило допускает указание в качестве переменной пути ветви реестра. Так, переменная

```
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
ProgramFilesDir%
```

указывает на папку, в которую по умолчанию производится установка программ.

Эти переменные используются, например, при создании правил запуска для тех программ, путь установки которых выбирает пользователь, а система использует при запуске информацию из реестра (программы Microsoft Office и т. д.).

Примечание

Переменная реестра записывается следующим образом: `%[Registry Hive]\[Registry Key Name]\[Value Name]%`. При использовании переменных реестра не допускаются сокращения (например, вместо `HKEY_LOCAL_MACHINE` — `HKLM`); после переменной (знака `%`) не может сразу следовать символ `\`. Кроме того, при указании правила пути реестра можно использовать только значения `REG_SZ` или `REG_EXPAND_SZ`.

Контроль выполнения данного правила совершенно не сказывается на производительности системы, однако у опытного пользователя имеются многочисленные возможности для "обхода" контроля. Во-первых, пользователь может копировать и переименовывать исполняемые файлы программ, чтобы обойти ограничения запрета по конкретному пути. Во-вторых, используя возможности переопределения переменных, можно также обойти наложенные ограничения.

- **Зона Интернета.**

Одно из самых неудачных, на взгляд автора, данное правило вводит ограничения на запуск программ в зависимости от того, из какой зоны произведена установка. На момент подготовки книги данное правило могло устанавливаться только для msi-пакетов (Windows Installer Packages).

В правиле используется типовой для систем Windows перечень зон безопасности: **Интернет**, **местная интрасеть**, **Ограниченные узлы**, **Надежные узлы**, **Мой компьютер**.

Опции настройки применения политик ограниченного использования программ

Существует несколько дополнительных опций настройки применения политик ограничения программного обеспечения. Прежде всего, это возможность применения политик к библиотекам программ (DLL Checking). В обычной практике применение такой проверки не имеет смысла, поскольку приводит к существенной деградации производительности компьютера[1], а эффект может быть наложен ограничениями только на собственно исполняемые файлы. Использование данной возможности оправдано только в тех случаях, когда администраторам необходимо осуществлять проверку целостности библиотек программ.

Опция **Для всех пользователей, кроме администраторов** позволяет не применять политики ограничения для администраторов локальных компьютеров. Необходимость ее использования определяется конкретной ситуацией.

Опция разрешения всем пользователям включать сертификаты в список доверенных, хотя и установлена по умолчанию, является не лучшим выбором. Предпочтительнее при работе в составе управляемой сети передать эти функции администраторам того или иного уровня.

Опция **Назначенные типы файлов** позволяет регулировать перечень расширений имен файлов, для которых будут применяться политики ограничения. Обычно этот список включает наиболее распространенные типы файлов, которые могут быть использованы для запуска программного кода.

Когда ограничения не действуют

Разработка политики ограничения ПО обычно не бывает без ошибок. Поэтому важно знать, как можно "вернуть" возможность управления системой администратору, если в результате применения неверной политики у него отсутствует возможность запуска программ.

Правила ограничения программного обеспечения не применяются в безопасном режиме, поэтому достаточно перегрузить систему, нажать клавишу <F8>, выбрать безопасный режим и выполнить необходимые действия.

Имейте также в виду, что правила ограничений программного обеспечения не применяются для программ, запускаемых от имени учетной записи **Система.**

К сожалению, на практике у автора был случай, когда в системе с Windows XP SP2 после применения политики по умолчанию "запрет" и удаления правил исключения для системных папок запреты продолжали действовать для

[1] Обычно при запуске одной программы загружается несколько десятков библиотек, причем одна и та же библиотека может вызываться несколько раз.

системной учетной записи даже в безопасном режиме. В этом случае помогло прямое редактирование реестра.

Политики ограничения ПО сохраняются в реестре в ветви

`HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers`

Параметр `DefaultLevel` определяет тип политики по умолчанию: значение `"0"` соответствует запрету, а `"40000"` — разрешению. Изменение этого параметра (на `40000`) и перезагрузка компьютера помогли восстановить доступ к системе.

Следует также учитывать, что правила ограничений не применяются при запуске драйверов (и вообще всех процессов уровня ядра системы), любых макросов в составе документов MS Office, а также программ, созданных с учетом Code Access Security Policy (на основе common language runtime).

Последовательность применения политик ограниченного использования программ

Порядок применения политик ограниченного использования программ имеет некоторые особенности. При наличии явных противоречий между правилами двух наследуемых политик (одна политика запрещает запуск данной программы, а другая — разрешает) используется типовая последовательность применения настроек. Однако политики ограниченного использования программ могут содержать различные правила: например, одно разрешает запуск *всех* программ для данной папки, а другое — запрещает загрузку *определенных* типов файлов. В этих случаях правила применяются в соответствии с их *старшинством*.

Во-первых, "старшинство" требований устанавливается в зависимости от типа правил[1]:

- ❒ хэш-правило;
- ❒ правило на основе сертификата;
- ❒ правило "пути";
- ❒ правило на основе зоны Интернета;
- ❒ правило по умолчанию.

Во-вторых, правила пути могут описывать требования к различным папкам, в которых находится исполняемый файл программы. В этом случае превалирует то правило, которое относится к *наиболее конкретному указанию пути*.

[1] Правило, написанное в первой строке, превалирует над правилом второй строки и т. д.

Ниже приведены примеры правил ограничений, расположенные *от наиболее конкретного к наиболее общему*:

- C:\Мои документы\Отчеты\Отчет за май.doc;
- C:\Мои документы\Отчеты*.doc;
- *.doc;
- C:\Мои документы\Отчеты\;
- C:\Мои документы\.

Примечание

При отличающихся значениях необходимости применения политики ограниченного использования программ к административным учетным записям в политиках компьютера и пользователя применяется значение, определенное политикой компьютера.

Некоторые рекомендации применения политик ограниченного использования программ

Составление политик ограниченного использования программ требует от администратора определенного опыта. Кроме тщательного продумывания вариантов политик, администратору необходимо принимать во внимание различные факторы.

Так, запуск конкретной программы может зависеть от другого исполняемого файла, и если на этот файл будет наложено ограничение, то запуск основной программы станет невозможным. Внимательно следует изучить ситуацию, когда необходимо использовать пути к папкам, а когда — пути с переменными реестра. Необходимо учесть такие факторы, как разрешение сценариев входа в систему, не заблокировать случайно запуск антивирусного программного обеспечения и т. п. Поэтому имеет смысл предварительно проанализировать на компьютерах сети состав автоматически загружаемого программного обеспечения *(см. разд. "Автоматически загружаемые программы" главы 9)*.

Сведения о пути к исполняемым файлам проще всего получить, если запустить желаемую программу и открыть задачу **Сведения о системе** (**Программы | Стандартные | Служебные**). Можно также набрать[1] в командной строке `wmic` и нажать клавишу <Enter>, а потом в появившемся окне ввести `process` и нажать клавишу <Enter>. Вы увидите пути к исполняемым файлам запущенных в текущий момент программ.

[1] Более подробно использование технологии WMI и ее командного интерпретатора `wmic` описано в *главе 13*, начиная с *разд. "Windows Management Interface"*.

Определить *зависимые* программы в общем случае достаточно тяжело. Обычно приходится экспериментировать. Можно только посоветовать внимательно просмотреть файлы из папки установки соответствующей программы и файлы из папки %ProgramFiles%\Common Files.

Нельзя забывать и то, что "благодаря" защите системных файлов на компьютере в папке %windir%system32\dllcache хранятся копии исполняемых служебных файлов и пользователь, которому запрещено запускать исходные файлы по исходному пути, может воспользоваться их копиями, указав точный путь к данной папке.

Примечание

Обратите внимание, что самый простой способ запретить запуск конкретного приложения состоит в назначении политики ограниченного использования, запрещающей запуск программы по ее хэшу.

Административные шаблоны

Количество регулируемых групповой политикой параметров можно менять. Проще всего добавлять настройки различных значений реестра системы. Для этого используются *административные шаблоны*.

Примечание

По образцу файлов шаблонов администратор легко может создать свои дополнительные настройки, которые он сможет распространить при помощи групповой политики. Понятно, что для создания такого файла администратору необходимы соответствующие знания, которые он может получить из технической документации на операционные системы и настраиваемое программное обеспечение.

Административный шаблон представляет собой текстовый файл, в котором по достаточно простым правилам записаны возможные настраиваемые значения реестра программного обеспечения[1]. Обычно административные шаблоны копируются на локальный диск после установки соответствующего программного обеспечения. Поэтому администратору для добавления нового шаблона достаточно открыть для изменения групповую политику и выполнить операцию добавления нового шаблона.

В завершение следует настроить необходимые параметры и привязать групповую политику к соответствующему подразделению.

---

[1] Описание синтаксиса данного файла весьма объемно. При необходимости администратор легко найдет необходимые рекомендации на сайте производителя, воспользовавшись, например, поиском по следующей строке "using administrative template files with group policy".

Редактирование параметров безопасности

Администратор достаточно легко может добавить в групповую политику и собственные настройки параметров безопасности. Изменение шаблонов, определяющих параметры паролей, политику Kerberos, параметры аудита и системного журнала, значения реестра и права доступа к нему, права пользователей и ограничения членства в группах, настройки запуска служб компьютера, — все это необходимо выполнять с помощью программы Security Configuration Manager (SCM).

SCM регистрирует настройки, содержащиеся в файле sceregvl.inf (расположен в папке %windir%\inf). После регистрации их можно использовать в консоли управления групповой политикой для распространения новых параметров.

Новые настройки необходимо включить в файл sceregvl.inf в любом текстовом редакторе. В самом файле содержится небольшая подсказка по правилам редактирования; более подробное описание можно найти в KB214752.

После завершения правки файла внесенные изменения следует зарегистрировать с помощью команды `regsvr32 scecli.dll`.

Для восстановления первоначальных значений достаточно удалить файл secedit.sdb и выполнить команду обновления групповой политики *(см. разд. "Время применения политик" ранее в этой главе)*.

GPO-консоль

Существующая оснастка для работы с групповыми политиками, которая присутствует в системе после установки, позволяет только изменять параметры политики и привязывать ее к подразделению. Но она не оказывает никакой помощи администратору, если в организации используется несколько политик. Целесообразно загрузить с сайта Microsoft консоль управления групповыми политиками, которая позволяет прогнозировать и оценивать результаты применения нескольких политик к конкретному подразделению, компьютеру, пользователю.

Оснастка **Group Policy Management** существенно облегчает работу администратора с групповыми политиками. Так, четко видна иерархическая структура политик и становится более удобно назначать ("привязывать") политики к подразделениям. Можно воспользоваться специализированными интерфейсами, которые покажут, какие параметры политики реально заданы администратором (в отличие от параметров по умолчанию). При наличии разветвленной структуры групповых политик определить результирующие значения параметров без данной оснастки крайне затруднительно. На рис. 6.3 показан

пример отображения параметров отслеживания электронной почты, заданных для данной организации в групповой политике.

Кроме того, оснастка **Group Policy Management** позволяет смоделировать параметры групповой политики, увидеть, какие параметры будут применены к конкретному пользователю, группе и т. п. в любом подразделении предприятия.

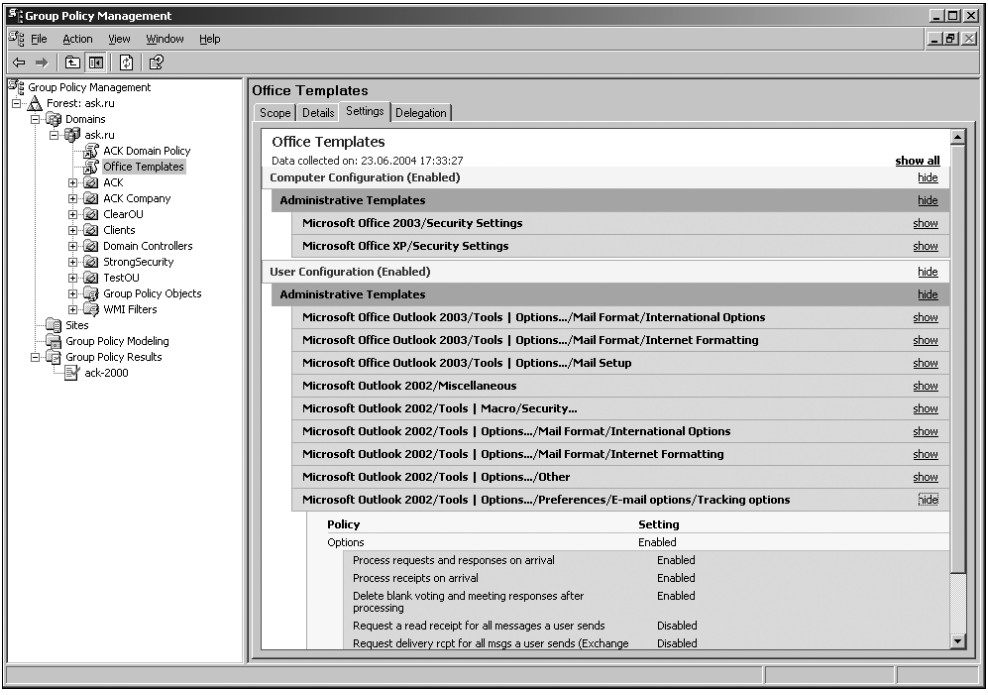
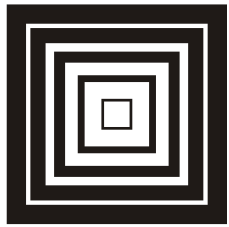


Рис. 6.3. Оснастка GPO-консоли



ГЛАВА 7

Организация почтового обслуживания

Без электронной почты в настоящее время трудно представить себе современный офис. Хотя существует много вариантов электронной почты: корпоративная, обслуживающая сотрудников какой-либо организации; специализированные службы доставки сообщений (например, в банковских структурах), любительская сеть FIDO и т. п., практическим стандартом стала *почта Интернета*.

Основы пересылки почтовых сообщений

Электронный адрес в Интернете всегда имеет вид:

`postbox@host.domain1.domain2....domainn`

где `postbox` — это имя почтового ящика адресата. Оно может быть произвольным, но не должно содержать специальных символов[1]. Обычно это имя создается на основании данных владельца ящика (имени и фамилии пользователя). За знаком логического "и" (`@`), часто называемого "собачкой", следует название домена Интернета, в котором создан данный почтовый ящик.

Для каждого домена Интернета можно организовать почтовое обслуживание. Чтобы можно было отправить сообщение на почтовый ящик в каком-либо домене, почтовая система должна знать, *куда* такое сообщение следует пересылать. Для этого используются *MX-записи*[2] данных DNS соответствующего домена. MX-запись сообщает адрес узла, на котором работает *почтовый сервер* соответствующего домена.

В целях резервирования для домена создаются несколько MX-записей. Каждая MX-запись имеет некоторый "вес", а почтовый сервер пытается передать

---

[1] В том числе не может содержать символы кириллицы.

[2] Mail eXchanger. *См. разд. "Основные типы записей DNS" главы 3.*

сообщения сначала на адрес, соответствующий MX-записи с меньшим весом, в случае ошибки (этот адрес не отвечает) — делается попытка отправить письмо на адрес, соответствующий MX-записи с весом, следующим по возрастанию, и т. д.

Определить адреса почтовых систем домена очень легко с помощью команды `nslookup`. После открытия окна программы следует дать команду показа MX-записей (`set type=mx`) и запросить информацию по желаемому домену:

```
>set type=mx
>ask.ru
Server:  frw.ask.ru
Address:  195.161.192.251

ask.ru  MX preference = 10, mail exchanger = mail.ask.ru
ask.ru  MX preference = 50, mail exchanger = relay.unets.ru
ask.ru  MX preference = 20, mail exchanger = frw.ask.ru
mail.ask.ru     internet address = 195.12.72.148
frw.ask.ru      internet address = 195.161.192.251
```

Как видно, для домена предусмотрены три почтовых сервера; по умолчанию почта будет приниматься системой **mail.ask.ru**, как имеющей минимальный вес среди этих записей.

Можно указывать и одинаковые веса для различных записей, как, например, для домена **microsoft.com**:

```
Non-authoritative answer:
microsoft.com   MX preference = 10, mail exchanger = maila.microsoft.com
microsoft.com   MX preference = 10, mail exchanger = mailb.microsoft.com
microsoft.com   MX preference = 10, mail exchanger = mailc.microsoft.com

maila.microsoft.com     internet address = 131.107.3.125
maila.microsoft.com     internet address = 131.107.3.124
mailb.microsoft.com     internet address = 131.107.3.122
mailb.microsoft.com     internet address = 131.107.3.123
mailc.microsoft.com     internet address = 131.107.3.126
mailc.microsoft.com     internet address = 131.107.3.121
```

В этом примере домен имеет не только несколько равнозначных почтовых серверов, но и каждый сервер принимает почту по двум IP-адресам[1].

[1] Описание методик выбора почтового сервера в подобной ситуации выходит за рамки данного издания. Например, сервер DNS может сообщать адреса почтовых систем по очереди (новому запросу — следующий по списку адрес) или такую балансировку осуществляет сетевой коммутатор и т. п.

Примечание

Как будут взаимодействовать почтовые серверы домена между собой, например, как резервному серверу передать сообщение основному после его восстановления, настраивается администраторами в каждом конкретном случае. Например, резервный сервер может самостоятельно проверять работоспособность основного сервера через заданные промежутки времени или же ожидать команды на пересылку сообщений.

Как только письмо попадает на почтовый сервер, оно обрабатывается в порядке общей очереди писем и передается в пункт назначения. В зависимости от загрузки почтового сервера и пропускной способности канала связи для доставки письма может потребоваться от двух-трех секунд до десятков минут и более.

Если при передаче письма по каналам связи возникают задержки (например, сервер назначения не работает или возникли проблемы с каналом связи), то почтовая система предпринимает повторные попытки передачи сообщения через определенные в ее настройках промежутки времени. Обычно первый повтор производится через пять-десять минут. При отсутствии результата через некоторое время (4—12 часов в зависимости от настройки конкретной почтовой системы) отправитель извещается о возникших трудностях, но попытки пересылки письма не прекращаются. Если письмо не удается передать в течение 1—3 дней (также зависит от конкретных настроек), то оно возвращается отправителю с описанием причин неудачи.

Путь письма и время его обработки каждым почтовым сервером документируются. С этими данными можно познакомиться, выведя на экран соответствующую служебную информацию письма.

Каждое письмо хранит в себе путь, по которому оно было доставлено получателю. Чтобы просмотреть его, следует открыть пункт меню **Параметры сообщения | Заголовки Интернета** (или **Свойства письма** — для других версий почтового клиента). В листинге приведена часть такого заголовка:

```
Microsoft Mail Internet Headers Version 2.0
Received: from 200-210-122-220.papalegua.com.br ([200.210.122.220] RDNS
failed) by ask.ru with Microsoft SMTPSVC(6.0.3790.0);  Sat, 10 Apr 2004
11:33:42 +0600
Received: from [112.125.38.24] by 200-210-122-220.papalegua.com.br with
ESMTP id CDFF67DFBDA; Sat, 10 Apr 2004 21:19:56 +0200
Message-ID: <d17nv-q0-i$-xz7-22-e8$z87@7z9cszi>
From: "Sophia Valentin" <robert@finklfan.com>
Reply-To: "Sophia Valentin" <robert@finklfan.com>
To: kenin@ask.ru
...
```

Из этого заголовка видно, что, хотя отправитель представился как `"Sophia Valentin" <robert@finklfan.com>`, на самом деле письмо было получено с ад-

реса другого домена. Поскольку обратное разрешение имени сообщило об ошибке, есть все основания подозревать, что это письмо — спам, а указанный адрес отправителя (112.125.38.24) — фиктивный.

Обмен сообщениями между почтовыми серверами Интернета производится по протоколу SMTP. В соответствии с этим протоколом почтовые серверы не обязаны проверять данные системы и пользователя, отправляющего сообщение, в том числе такие поля письма, как **От**, **Кому**, **Тема** и т. п., которые являются *внутренним* текстом принимаемого сообщения. Поэтому при передаче почтового сообщения злоумышленнику не составляет труда представиться любым человеком *(см. разд. "Безопасность электронной почты" далее в этой главе)*. Пример такого сообщения приведен в листинге выше. Единственные реальные данные, которые могут быть запротоколированы в процессе обмена сообщениями, — это IP-адрес передающей сообщение системы.

Примечание

Многие вирусы, использующие данные адресной книги, подставляют в качестве адреса отправителя "чужие" данные, при этом сообщение о недоставке письма придет не системе, с которой было отправлено сообщение, а тому пользователю, данные которого указаны в качестве отправителя. В этом случае подтвердить руководителю организации факт отсутствия вирусов в локальной сети можно, только показав служебные параметры сообщения о пути доставки письма.

Используемые протоколы

SMTP

SMTP (Simple Mail Transfer Protocol, простой протокол передачи почты) — протокол, описывающий правила обмена сообщениями между почтовыми серверами. Предусматривает передачу команд в виде текстовой строки на порт 25. Клиенты используют протокол SMTP, как правило, только для отправки своих сообщений на почтовый сервер. Описание SMTP-команд легко найти в Интернете, а смоделировать "общение" почтовых серверов можно с помощью команды `telnet` *(см. разд. "Отправка сообщений по протоколу SMTP" далее в этой главе)*.

Обычно взаимодействие по протоколу SMTP ведется анонимно, хотя существует вариант протокола (SMTPS), предусматривающий аутентификацию и шифрование трафика.

Следующие протоколы используются клиентами для работы с почтовым сервером. Какие протоколы допустимы для пользователей при работе с конкретным почтовым сервером, зависит от его программной реализации и административных настроек.

POP3

POP3 (Post Office Protocol 3, протокол обслуживания почтового офиса) — наиболее часто используемый протокол для чтения сообщений с почтовых серверов Интернета. При типовых установках почтового клиента используется пакетный прием сообщений электронной почты: все письма копируются на компьютер пользователя и затем удаляются с сервера. Такой способ уменьшает время работы почтовой программы при подключении к сети, что экономит средства при повременной оплате соединения. По умолчанию протокол предполагает передачу учетных данных пользователя на почтовый сервер в открытом виде. Позволяет загружать письма только из папки **Входящие**.

Вариант протокола POP3S использует шифрование трафика.

IMAP

При подключении по протоколу IMAP (Internet Message Access Protocol, протокол доступа к сообщениям Интернета) пользователь может не только читать входящую почту, но и создавать дополнительные папки на почтовом сервере, просматривать информацию, содержащуюся в других папках почты (если таковые созданы на сервере). С установками по умолчанию почтовый клиент обычно загружает только заголовки сообщений. Само сообщение копируется на компьютер пользователя в момент обращения к нему (открытия).

Данный вариант подключения более удобен по сравнению с POP3: дает возможность организовать структуру папок с сообщениями, "читать" папки специальной конфигурации — контакты и т. п., выбирать отображаемую на локальной машине структуру папок и т. д., а также позволяет настраивать почтовый ящик на использование электронной подписи и шифрования сообщений.

Примечание

При использовании протокола IMAP обратите внимание на настройки почтового клиента при приеме сообщений. Например, если настройками предусмотрено только копирование всех новых сообщений на локальный компьютер пользователя без удаления с почтового сервера, то через некоторое время вы можете столкнуться с отказом в приеме новой почты из-за переполнения ящика.

HTTP

Основное преимущество использования протокола HTTP (HyperText Transfer Protocol, протокол передачи гипертекста) — возможность работы с почтовым

ящиком через программу обозревателя Интернета (Mozilla's Firefox, Opera, MS Internet Explorer и т. п.).

При работе по протоколу HTTP объем передаваемой и принимаемой информации существенно выше, чем при чтении почты с помощью POP3 или IMAP. Кроме того, каждое сообщение необходимо индивидуально загружать в окно программы для прочтения. Все это существенно снижает скорость работы с почтовым ящиком (по сравнению с использованием традиционного почтового клиента). Однако данный протокол обычно открыт в программах межсетевых экранов, что позволяет получить доступ к почтовому ящику практически из любого места.

Протокол используется преимущественно при работе с бесплатными общедоступными почтовыми серверами. В то же время HTTP является, например, основным протоколом для взаимодействия клиентов с сервером корпоративной работы Openexchange.

В целях безопасности пересылаемых данных целесообразно использовать вместо HTTP защищенный вариант — HTTPS.

RPC

Для подключения к почтовому серверу Microsoft Exchange используются функции удаленного вызова процедур (RPC, Remote Procedure Call). Этот вариант обозначается в настройках Outlook как "поддержка MS Exchange". Протокол используется практически только в локальных сетях, поскольку требует динамического открытия большого числа портов. Начиная с Windows 2003/Exchange 2003, предусмотрена возможность работы RPC поверх протокола HTTP. Это позволяет использовать полнофункциональные[1] версии программы Outlook при доступе к корпоративной сети через Интернет. Такой вариант требует большого количества дополнительных настроек почтового сервера, прокси-сервера RPC и описан подробно в KB833401 и в специальном руководстве "Exchange Server 2003 RPC over HTTP Deployment Scenarios" (**http://www.microsoft.com/downloads/details.aspx?FamilyId=EF58395D-3710-49CF-9698-938E2BEF39E8&displaylang=en**).

Пример "прямой" проверки почтового сервера

Проверить базовую функциональность почтового сервера проще всего непосредственно из командной строки, используя программу `telnet`. Это позволя-

[1] MS Exchange Server, так же как и почтовый сервер на базе Linux — SuSe Openexchange *(см. разд. "Установка корпоративного почтового сервера Интернета" далее в этой главе)*, является не только сервером почты, но и сервером организации совместной работы сотрудников организации. Это предполагает такие дополнительные возможности, как планирование рабочего дня, назначение задач и т. п.

ет при проверке сервера исключить влияние настроек клиентской почтовой программы.

Приведем примеры отправки сообщений по протоколу SMTP и просмотра личного почтового ящика по протоколу POP3.

Отправка сообщений по протоколу SMTP

Ниже приведена простейшая процедура отправки электронного сообщения из командной строки[1] по протоколу SMTP на почтовый сервер с именем `exchange`. Строки, которые вводятся с клавиатуры, дополнительно помечены знаком >.

```
>telnet exchange 25
220 ask.ru Microsoft ESMTP MAIL Service, Version: 5.0.2195.5329 ready at
Wed, 28 Aug 2002 22:42:27 +0600
>helo
250 ask.ru Hello [192.168.0.68]
>mail from:test@test.ru
250 2.1.0 test@test.ru....Sender OK
>rcpt to:mail@ask.ru
250 2.1.5 mail@ask.ru
>data
354 Please start mail input.
>subject: Это просто тест
>bcc: kenin@ask.ru
>
>Это тестовое письмо.
>Все.
>
>.
250 Mail queued for delivery.
>quit
221 Closing connection. Good bye.
```

Первая строка примера — это команда подключения telnet-клиента к почтовому серверу на 25-й порт (SMTP-протокол). В ответ сервер сообщает свое имя, версию программы и текущую дату. Далее, по правилам, системы должны обменяться приветствиями — клиент посылает "Helo", на что получает соответствующий ответ от сервера. Затем следует сообщение, от кого посылается письмо (строка начинается с `mail from:`), на которое сервер отвечает

[1] Обратите внимание, что протокол telnet, использованный в примерах главы, передает пароль пользователя по сети в открытом виде. В результате этот пароль может быть легко обнаружен программами просмотра *(снифферами)*.

согласием. После чего сообщается адресат корреспонденции (строка с `rcpt to:`) и наконец следует сам текст письма, который начинается с команды клиента `data`.

В теле письма может содержаться служебная информация для почтовых клиентов — заголовки (в нашем случае это строки `subject` и `bcc`), а завершиться сообщение должно пустой строчкой, за которой последует строка только с одним символом — точкой. После получения символов конца сообщения почтовый сервер выдает информацию о том, что сообщение поставлено в очередь на доставку.

Примечание

Строки ответов от почтового сервера не регламентированы, они могут отличаться от данных в примере (единственное исключение: ответ на `helo` после кода должен информировать об имени почтового домена). Поэтому для почтовых программ важны в первую очередь коды, с которых начинаются ответы сервера: они определены специальными рекомендациями и свидетельствуют об успехе или ошибке в обработке каждой полученной строки.

Среди SMTP-команд отмечу еще `RSET` — сброс соединения, `VRFY` — проверка почтовым сервером адреса получателя без отправки сообщения, `NOOP` — команда просто вызывает ответ сервера с кодом 220 (отсутствие ошибки).

Существуют *расширения* команд SMTP. При использовании расширений клиент может предварительно информировать о размере сообщения, запрашивать подтверждение приема сообщения, прочтения его получателем и т. п. В этом случае в качестве приветствия используется ключевое слово `ehelo`. Если сервер возвращает код ошибки, то системы переходят на стандартный набор. Стандартный набор должен обрабатываться любым почтовым сервером.

Чтение сообщений по протоколу POP3

Самый простой способ прочесть сообщение из командной строки — это воспользоваться командами протокола POP3.

```
>telnet exchange 110
+OK Microsoft Exchange 2000 POP3 server version 6.0.6249.0 (exchange.ru)
ready.
>user mail
+OK
>pass test_password
+OK User successfully logged on.
>list
+OK 3 3188
```

```
1 2381
2 394
3 413
.
>retr 3
+OK
Received: from ([192.168.0.68]) by ask.ru with Microsoft
SMTPSVC(5.0.2195.5329)
;
Wed, 28 Aug 2002 22:44:53 +0600
subject: Это просто тест
bcc: kenin@ask.ru
From: test@test.ru
Return-Path: test@test.ru
Message-ID: ANGEiR9Odut000001cc@exchange.ru
X-OriginalArrivalTime: 28 Aug 2002 16:44:53.0708 (UTC)
FILETIME=[3BF878C0:01C24EB2]
Date: 28 Aug 2002 22:44:53 +0600

Это тестовое письмо.
Все.

.
>dele 3
+OK
>list
+OK 2 2775
1 2381
2 394
.
```

Первой строкой мы подключаемся к почтовому серверу (порт протокола POP3 — 110). После получения от него приветствия вводим свои идентификационные данные (сначала имя — в строке после команды `user`, а затем пароль — в строке после команды `pass`). Следующим шагом посылаем команду — показать список сообщений в почтовом ящике (`list`). Сервер сообщает список с указанием объема каждого сообщения (цифра после номера сообщения). После чего мы просим показать сообщение с заданным номером (`retr 3`, самое "свежее" сообщение имеет наибольший номер). В заключение мы удаляем это сообщение с сервера (`dele 3`) и снова просматриваем список, убеждаясь в успешном выполнении команды.

Установка почтового сервера организации

Существует несколько вариантов организации почтового обмена в малых и средних организациях. Если организация зарегистрировала в Интернете свое доменное имя, то возможно организовать почтовый обмен сообщениями как между сотрудниками организации, так и с внешним миром на основе реальных адресов электронной почты. В противном случае администратору необходимо реализовать тот или иной механизм внутреннего обмена сообщениями. Для получения внешней почты в таких организациях обычно заводят почтовые ящики либо на бесплатных почтовых серверах, либо у провайдера Интернета. При этом администратору следует предусмотреть способы автоматизации получения почты с этих почтовых ящиков клиентами локальной почтовой системы.

Создание внутрикорпоративной почты малых организаций

Почтовая программа, предназначенная для использования в малых организациях, должна быть достаточно "легкой" и в то же время функциональной. Иными словами, не требовать много ресурсов для своей работы, позволяя как организовать обмен сообщениями внутри организации, так и предоставить доступ к почте Интернета. Администратор легко может найти целый перечень как бесплатных, так и коммерческих программ, реализующих эти функции. Автор берет на себя смелость на основе собственного опыта рекомендовать для использования программу The Bat![1] от Ritlabs S.R.L (**http://www.ritlabs.com/**).

The Bat! может выступать как почтовым сервером, так и клиентом. Программа позволяет работать со всеми форматами почтовых сообщений, в том числе с зашифрованной почтой (PGP, SMIME). Имеется модуль для фильтрации спама и антивирусного контроля сообщений. Пользователь может импортировать данные адресных книг всевозможных форматов и т. п.

The Bat! включает в себя мощные средства автоматизации. Даже неопытный пользователь легко создаст шаблоны для автоматизации обработки сообщений, для загрузки писем с сервера Интернета и т. п. Эти функции настолько

[1] Программа The Bat! завоевала огромную популярность своей "легкостью", удобными настройками, позволяющими оптимизировать почту организации. Отличительной особенностью программы является то, что внутри организации не используются почтовые протоколы. Сообщения сохраняются в структуре совместно используемых папок.

легко настраиваются, что на их основе можно достаточно просто создать, например, полностью автоматизированный список рассылки.

Другой почтовый сервер, который могут использовать владельцы Windows 2003, — это виртуальный SMTP-сервер из состава операционной системы. Этот сервер позволяет принимать почту по протоколу SMTP и предоставлять ее пользователям по протоколу POP3. Его установка производится добавлением службы SMTP через функцию добавления компонентов Windows (**Сервер приложений** | **Службы IIS** | нажать на кнопку **Состав** | добавить **службу SMTP**). Сервер может обслуживать несколько почтовых доменов. Основные его настройки выполняются через меню свойств виртуального почтового сервера (рис. 7.1).

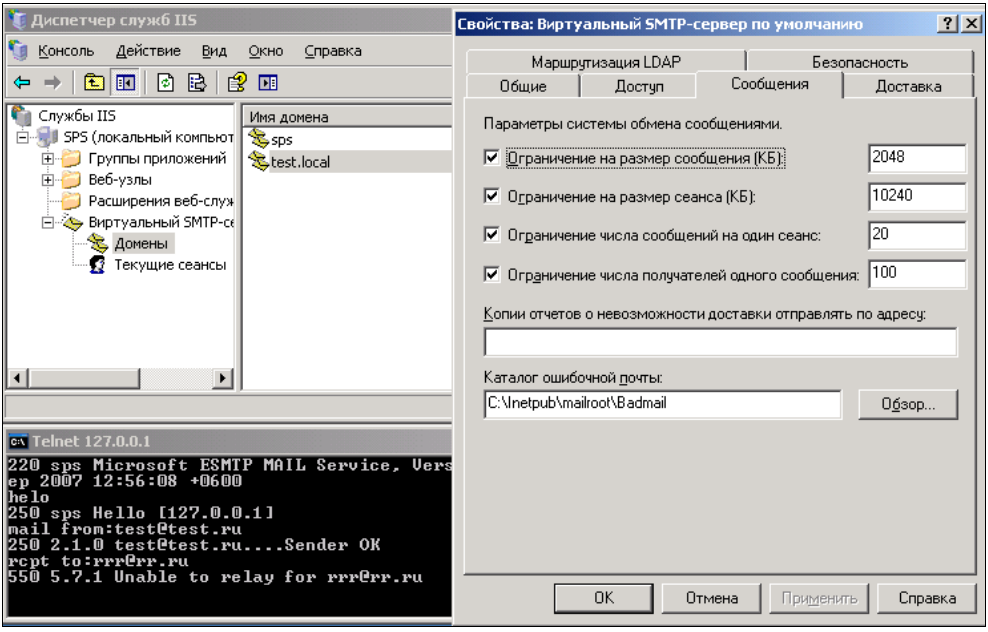


Рис. 7.1. Встроенный почтовый сервер Windows 2003.
На рисунке представлены окна настройки почтового сервера из состава Windows 2003. Также виден telnet-сеанс обмена с данным почтовым сервером, в котором сервер сообщает о невозможности пересылки сообщений для другого почтового домена

Данный почтовый сервер может быть использован в том числе и для работы с почтой Интернета. При этом администратору необходимо обеспечить регистрацию его в DNS и постоянную работу. К недостаткам данного решения следует отнести отсутствие средств корпоративной работы (общие папки и т. п.), использование только протоколов POP3/SMTP, а также невозможность собственными средствами получить почту с других серверов Сети.

Установка корпоративного почтового сервера Интернета

Если организация имеет свое доменное имя, то каждый ее сотрудник может получить реальный адрес электронной почты. В таком случае удобнее осуществлять обмен сообщениями и внутри организации на основе стандартов электронной почты Интернета.

Для крупных предприятий наиболее известны два почтовых сервера. Это фактически являющаяся стандартом программа Lotus Notes от IBM (**www.lotus.com**) и Microsoft Exchange Server (**www.microsoft.com**). Продукты предназначены для крупных предприятий и обслуживания большого числа пользователей, достаточно дороги и используют серьезные вычислительные мощности. Применять их в условиях небольших предприятий с несколькими десятками пользователей экономически и технически неоправданно.

Существуют различные программы почтовых серверов, которые можно использовать для организации переписки нескольких десятков или сотен пользователей. Однако следует отметить, что в последнее время от систем обмена сообщениями ожидают не только простой пересылки писем, но и функций *групповой работы*, таких как ведение общих папок, группового и индивидуального календаря с возможностями планирования заданий (с соответствующими напоминаниями) и т. п. Поэтому следует оценивать наличие у программ и указанных функций.

Администратор может выбрать, например, популярный сервер MDaemon от Alt-N Technologies (**http://www.altn.com/**) вместе с модулем групповой работы GroupWare, который позволяет совместно использовать календари, контакты и задания Outlook. В Pro-версии присутствуют также общие папки, блокировка спама, фильтрация писем по содержимому, антивирусная защита, связь со службами каталогов и т. п.

Аналогичный по возможностям вариант (пересылка сообщений, календарь, планирование и напоминание, папки общих документов и т. п.) для систем с открытым кодом на базе Linux представлен фирмой Novell. Это SUSE Linux Openexchange Server (**www.suse.org**), предназначенный для обслуживания от 10 до 2500 пользователей[1]. Причем базовая функциональность — пересылка сообщений электронной почты — бесплатна, в случае необходимости оплачиваются лицензии *групповой работы*, стоимость которых в несколько раз ниже других аналогичных продуктов.

[1] В поставке Openexchange Server просто нет лицензии на групповую работу менее чем на 10 пользователей.

Регистрация почтового сервера в DNS. Резервный сервер почты

Как уже говорилось, для работоспособности почтового сервера, который будет принимать из Интернета почту организации, необходимо зарегистрировать соответствующие MX-записи домена предприятия. Не забудьте также зарегистрировать записи зоны обратного разрешения для вашего почтового сервера, чтобы по его IP-адресу другие системы могли восстановить DNS-имя.

Обычно каналы доступа в Интернет, имеющиеся в организации, по своей надежности существенно уступают качеству каналов провайдера. Кроме того, в малых и средних организациях часто недостаточно средств для создания отказоустойчивого почтового сервера. Поэтому если по каким-либо причинам почтовый сервер окажется недоступным (нет связи с ним, технические проблемы и т. п.), то другие системы поставят отправку сообщений для организации в *очередь*. Если сервер не будет восстановлен, то по истечении некоторого периода (обычно сутки) письмо вернется отправителю с сообщением о невозможности доставки.

Поэтому при установке своего почтового сервера, обслуживающего домен организации, следует позаботиться о создании *резервного* почтового сервера, который мог бы в подобных аварийных ситуациях обрабатывать почту вместо основного. Этот сервер должен быть также зарегистрирован в DNS, но уже с большим значением параметра MX-записи.

Чтобы вторичный почтовый сервер смог передать основному принятые за время аварии сообщения, администратору необходимо выполнить соответствующие настройки. Конкретная реализация (кто будет инициировать отправку сообщений — первичный или вторичный сервер, периодичность отправки и т. п.) зависит от используемой программы почтового сервера.

Примечание

Поскольку обычно необходимо обеспечить доступ к почтовому серверу сотрудников организации как с рабочих мест, так и с мобильных устройств, то в целях неизменности настроек клиентских компьютеров применяется разделение DNS *(см. разд. "Разделение DNS" главы 3)*.

Защита почтового сервера

Данные рекомендации относятся ко всем типам почтовых серверов (в том числе и серверам малых предприятий, о которых шла речь выше).

Почтовый сервер должен быть защищен межсетевым экраном как от внешней сети, так и от внутренней.

Брандмауэр должен обеспечить публикацию 25-го порта сервера в Интернете: все пакеты, направленные на внешний IP-адрес на 25 порт, должны перенаправляться на 25 порт локального адреса, закрепленного за почтовым сервером. И наоборот, исходящие от него пакеты на 25 порт должны свободно пропускаться брандмауэром.

В случае необходимости доступа почтовых клиентов извне к почтовым ящикам на сервере необходимо открыть порты, используемые клиентами для операций доступа к почте (например, 110 и 25 при чтении писем по протоколу POP3 и для отправки сообщений по протоколу SMTP). Какие порты следует открыть для доступа к почтовому серверу *изнутри* сети, определяется используемыми сотрудниками организации почтовыми клиентами.

Поскольку часть атак на почтовые серверы использует нестандартные команды, то рекомендуется использовать на межсетевых экранах специальные фильтры, блокирующие подобные попытки.

Антивирусная защита почтовых сообщений

Сегодня основным источником проникновения вирусов в организации являются почтовые сообщения. Само почтовое сообщение не может содержать какой-либо вирус, поскольку оно является обычным текстом. Вредоносный код встраивается как тот или иной вариант вложения: через оформление письма (коды формата HTML); как исполнимый файл, к запуску которого тем или иным способом побуждается пользователь; как иллюстрация, включающая специальный код, задействующий при отображении ее на экране уязвимость Windows[1].

Примечание

В этой связи следует отметить, что использование режима предварительного просмотра в MS Outlook не является полностью безопасным вариантом работы с сообщениями.

Пересылка файлов в письме

Сценарии могут содержаться в документах различных форматов и программ. Это могут быть сами сценарии, маскируемые отправителями под безобидные файлы (например, путем присвоения имени *имя*.txt.vbs, которое система отобразит на экране как *имя*.txt), файлы документов, содержащие сценарии (документы Word, Excel и т. д.), так и просто иллюстрации, открытие которых

[1] См. бюллетень на сайте Microsoft по безопасности MS04-028.

вызывает ошибку переполнения буфера и позволяет злоумышленнику исполнить вредоносный код.

Поэтому следует постоянно напоминать пользователям, чтобы они не открывали *никакие* вложенные в письмо файлы, полученные как от незнакомых авторов, так и от своих друзей[1]. Если нужно переслать какой-либо файл, следует *предварительно* обменяться обычными текстовыми сообщениями.

Современные версии почтовых программ, например MS Outlook, блокируют открытие тех файлов, которые потенциально могут содержать исполняемые коды. Перечень блокируемых файлов может быть уточнен администратором. Если перечень определен в групповой политике организации, то пользователь уже не может выполнить самостоятельные настройки. Если варианты блокирования вложений не определены централизованно, то они легко модифицируются редактированием реестра локальной системы (см. статью KB837388).

Администратор может применить различные средства для снятия блокировки вложений, что позволит избежать возможных ошибок при ручных операциях, например использовать бесплатную утилиту DetachOL (**http://www.mcdev.com/**).

В любом случае не рекомендуется разрешать пользователям открывать блокированные файлы. Целесообразно назначить ответственное лицо, которое, приняв необходимые меры предосторожности, проведет первичный контроль вложения и передаст принятые файлы пользователю.

Примечание

Если необходимо отправить файл Word, то такой документ предварительно следует сохранить в формате RTF. Этот формат файла *не может* содержать макросов.

Проверка сообщений на почтовом сервере

Поскольку электронная почта стала основным разносчиком вирусной инфекции и в организации не исключена возможность подключения к сети компьютера с неустановленной антивирусной программой (например, ноутбук пользователя), то целесообразно наряду с установкой антивирусных программ на каждом клиентском компьютере проверять и всю проходящую через сервер почту. Для всех типов почтовых серверов разработаны соответствующие антивирусные программы для проверки сообщений. Например, для MS Exchange Server 2003, который имеет специальный интерфейс для анти-

[1] В последнее время вирусы часто используют отправку писем, подставляя фиктивные данные автора из адресной книги. А поскольку в одной адресной книге часто содержатся данные знакомых между собой людей, то вероятность получения такого письма якобы от знакомого весьма велика.

вирусных программ, можно использовать такой продукт, как Symantec Mail Security, и т. п.

Примечание

Не следует использовать на серверных станциях антивирусные программы, предназначенные для рабочих станций *(см. главу 9, разд. "Антивирусные программы")*.

Спам

Практика массовой рассылки по электронной почте нежелательной для получателя информации (прежде всего рекламной) получила название *спам*[1]. Количество спама непрерывно увеличивается и уже превысило объем "нормальной" переписки.

Спам существует прежде всего благодаря дешевизне пересылки сообщений по электронной почте и возможности осуществлять массовую рассылку одновременно в сотни тысяч адресов. При этом затраты на такую рекламу существенно ниже расходов на размещение публикаций в средствах массовой информации или на прямую почтовую рассылку[2]. Несмотря на то, что большинство пользователей удаляет такую корреспонденцию, даже не читая ее, данный тип рекламы имеет определенную эффективность. В итоге появляются фирмы, специализирующиеся на такой рассылке, организации, собирающие и продающие адреса электронной почты, и... совершенствуются способы борьбы со спамом.

Способы борьбы со спамом

Юридические аспекты

Казалось бы, в чем проблема: взять и запретить спам. Тем более что инициаторами борьбы выступают сами интернет-провайдеры, включающие в договоры с клиентами пункты о недопустимости спама. Поэтому в большинстве случаев организаторы массовой рассылки рекламы скрывают свои следы тем или иным способом, используя почтовые серверы других стран для пересыл-

---

[1] Spam — это термин, обозначающий популярное на Гавайях блюдо (см. **http://www.hormel.com/**). Американцы, ассоциирующие данное блюдо с чем-то непривлекательным и вредным, но очень надоедливо предлагаемым, перенесли это название и на описываемый вид электронной рассылки писем. В российской практике произошло простое заимствование названия.

[2] При этом, в отличие от других способов распространения рекламы, спам во многом "оплачивается" самим пользователем, а не рекламодателем. Пользователь оплачивает время работы в Интернете, в течение которого эти рекламные письма загружаются на компьютер. На обработку, хранение такой корреспонденции затрачиваются ресурсы личного компьютера и т. п.

ки корреспонденции, возможности анонимного доступа в Интернет (по разовым карточкам) и т. п.

Хотя "заказчик" спама очевиден — в том или ином виде координаты рекламодателя содержатся в электронном письме, но юридическая база нашей страны не позволяет организовать действенную борьбу с данным явлением. Между тем за рубежом уже известны многочисленные судебные прецеденты.

Программные способы противодействия спаму

Для того чтобы пресечь спам, необходимо определить, по каким правилам программа будет сортировать корреспонденцию, выделяя из нее несанкционированную рекламу.

- **По адресу отправителя.**

  Организаторы спама используют для рассылки или фиктивные почтовые адреса, или бесплатные почтовые ящики. В принципе можно настроить почтовые серверы (и индивидуальные программы пользователей) так, чтобы они не принимали почту от таких адресатов. Однако вероятность повторного спам-сообщения с одного и того же адреса крайне мала. Поэтому подобная фильтрация практически бесполезна.

  Можно, конечно, запретить прием почты со *всех* бесплатных почтовых служб. К примеру, Symantec Mail Security по умолчанию предлагает отфильтровывать корреспонденцию, отправленную с таких популярных бесплатных почтовых серверов, как Yahoo, AOL и др. Но, согласно опыту, фильтрация бесплатных почтовых серверов не приносит большого эффекта, к тому же многие корреспонденты организаций используют в работе подобные службы.

  Другой способ контроля отправителя состоит в проверке регистрации адреса системы, с которой осуществляется попытка передачи сообщения. Ряд фирм и организаций "продвигает" технологию *SenderID*, предполагающую наличие в DNS специальных записей об адресах систем, которые могут отправлять почтовые сообщения от имени данного домена (см., например, мастер, формирующий данные для DNS — **http://www.antispamtools.org/SenderIDEmailPolicyTool/Default.aspx**). Поскольку IP-адрес передающей сообщение системы известен, то достаточно проверить соответствующие DNS-записи и разорвать соединение в случае попыток передачи сообщений "неуполномоченными" хостами.

  Несмотря на активное лоббирование рядом крупных вендоров, данная технология пока не нашла широкой поддержки, поскольку сужает правила отправки и приема сообщения по протоколу SMTP. Например, вместо основного набора команд SMTP необходимо использовать расширенный, что поддерживается не всеми почтовыми серверами, и т. п.

Спамеры часто пытаются использовать для своих рассылок чужие почтовые серверы, например, почтовые системы, на которых не отключена возможность *пересылки* сообщений[1]. Обычно такая пересылка является следствием ошибок в настройке программного обеспечения. Существует специальная общественная организация, которая проверяет почтовые серверы на возможность пересылки чужой корреспонденции. При обнаружении такого факта сервер включается в специальный список "запрещенных" почтовых серверов (Open Relay DataBase, ORDB, который иногда на сленге называют также "черным" списком DNS — *black DNS*). Многие почтовые программы имеют возможность использовать данный список[2] и полностью блокировать корреспонденцию с таких серверов. Например, рекомендация по использованию списка ORDB для практически самого популярного (и притом бесплатного) почтового сервера Postfix заключается в добавлении в конфигурацию одной строки (см. **http://www.ordb.org/faq/**).

Аналогичные списки (Real-time Spam Black Lists, RBL) формируются из адресов систем, замеченных в использовании спамерами. Перечень служб, предоставляющих такие списки, легко найти в Интернете (например, **www.email-policy.com/Spam-black-lists.htm**).

Перед включением данного метода защиты от спама необходимо изучить правила формирования списка соответствующей службой, поскольку различные списки могут быть недостаточно строгими или, наоборот, очень строгими. Так, Arbitrary black hole list запрещает прием почты с популярных бесплатных серверов, на которых могут быть ящики клиентов вашей организации.

Примечание

Если по каким-либо причинам ваш почтовый сервер был использован для рассылки спама или в качестве сервера пересылки сообщений, то он может попасть в соответствующий "черный" список. В этом случае на имя администра-

[1] Имеется в виду функция `relay`. Под пересылкой понимают такую настройку почтового сервера, которая разрешает прием сообщений, адресованных в домен, не обслуживаемый данной системой. Иными словами, сервер принимает сообщения только для того, чтобы отослать их на другой сервер. В большинстве случаев `relay` должен быть отключен, хотя в некоторых ситуациях, например в настройках резервного сервера, допускается прием писем для пересылки на конкретный домен.

[2] При небольшом объеме электронной корреспонденции можно использовать запросы непосредственно к серверам служб (для получения данных о принадлежности узла к "черному" списку применяются специально сформированные DNS-запросы). При очень большом числе писем, получаемых организацией, эти списки нужно копировать на локальные системы (реально это происходит как перенос зоны DNS). Обычно такой перенос оправдан только в организациях-провайдерах Интернета.

тора сервера[1] приходит письмо от данной службы, в котором сообщаются причины такого решения и приводятся необходимые действия, которые следует предпринять для исключения из "черного" списка. Например, в случае попадания в ORDB нужно, после устранений причин ошибки, инициировать процедуру проверки, заключающуюся в отправке с сайта службы проверочных сообщений.

Данный вариант защиты является одним из наиболее эффективных методов, хотя технически реализован не для всех почтовых серверов[2]. Следует также учесть, что такой способ не является стандартизованным и что существуют различные черные списки, формируемые и поддерживаемые независимыми организациями.

Кроме того, спамеры все активнее используют почтовые серверы, обслуживающие пользователей. Для этого на компьютер[3] устанавливается троянская программа, которая пересылает сообщения, учитывая пользовательские параметры настройки почты. Против такого способа в настоящее время практически нет действенных вариантов защиты, поскольку операции осуществляются от имени и с правами реального пользователя.

- **По содержимому письма.**

Возможный способ определения спама состоит в анализе содержимого текста письма. Используя различные алгоритмы, каждому сообщению автоматически присваивается некий уровень спама (на момент подготовки книги выделялось семь уровней "спамоопасности"). Администратор почтовой системы определяет правила обработки для каждого уровня: пропускать сообщения, маркировать их, архивировать в специальные папки или просто удалять.

Конечно, такой автоматизированный анализ достаточно условен. Если первые массовые рассылки можно было успешно формально определить по используемым оборотам (например, часто употреблялось подряд несколько знаков доллара), то современные авторы становятся все более и более изобретательными. Причем рекламодатели сами активно изучают способы и методы вычленения спама и оперативно корректируют свои тексты. Например, пересылают необходимый текст в виде вложенной в письмо картинки (при оформлении письма в формате HTML), вносят специальные ошибки в ключевые слова, которые не позволяют обнаружить рекламное содержимое, и т. п.

---

[1] Обратите внимание, что, в соответствии со стандартами Интернета, в организации должен существовать адрес **postmaster@*домен.организации***, принадлежащий администратору сервера. Кроме того, следует проверить, что в записях DNS домена организации существуют реальные контакты ответственных лиц (запись RP, *см. разд. "Основные типы записей DNS" главы 5*).

[2] Так, он присутствует в MS Exchange Server начиная только с версии 2003.

[3] В целом пользовательские системы менее надежно защищены, чем корпоративные.

По заявлениям разработчиков, новые спам-фильтры используют обучающиеся алгоритмы, которые позволяют довести эффективность обнаружения рекламы до уровня 90% и более. В любом случае при использовании данной технологии администратору следует архивировать подозрительные сообщения в специальные папки и регулярно просматривать их, чтобы не потерять служебную переписку. Конечно, это серьезно увеличивает нагрузку специалиста по сопровождению почтовой системы.

Примечание

В качестве курьезного примера приведу тот факт, что рассылка, осуществляемая фирмой Microsoft своим партнерам, периодически детектируется как нежелательная почта и помещается в соответствующую папку клиентской почтовой программой опять же их собственной разработки — MS Outlook — с минимальным уровнем фильтрации.

По мнению автора, использование в организации фильтров по содержанию на сегодня нецелесообразно. После случая, когда ответное письмо заказчика подобной системой было отправлено в папку нежелательной почты, результатом чего явился срыв сроков работы, функции фильтрации пришлось отключить.

Но если вы посчитаете целесообразным использовать эту технологию, то обратите внимание на необходимость постоянного обновления и настройки фильтров, иначе данный метод быстро теряет свою эффективность.

- **По "известности" автора отправления.**

Один из самых простых и эффективных способов сортировки писем — это разделение их на две группы — свой и чужой автор. Если письмо пришло от автора, включенного в некий заранее составленный список, то оно будет считаться "разрешенным", в противном случае такое письмо можно удалить. Хотя следует учесть, что данный способ отнесет к нежелательной корреспонденции и письмо старого школьного товарища, и деловое предложение, которое прислал неизвестный бизнесмен, получивший адрес от вашего знакомого.

- **По дополнительным действиям отправителя.**

Отличить письмо массовой рассылки от индивидуального можно, если запросить от отправителя выполнение неких действий. Если автоматизированная реакция по тем или иным причинам затруднена, то наличие верного действия является признаком отсутствия спама. По такому принципу, в том числе, работает программа WinAntiSpam (**http://www.winantispam.com/**), предлагающая отправителю выслать подтверждение[1] отправки на специ-

[1] Поэтому если спамер укажет в качестве обратного адреса систему с автоответчиком, то такое письмо "просочится" через эту защиту.

альный адрес. Недостаток подобных решений — это, прежде всего, замедление получения письма. Кроме того, отправитель, не зная о наличии у получателя такой технологии, может длительное время считать письмо доставленным, не работая со своим почтовым ящиком.

Предупреждение спама

Таким образом, на сегодня действенных способов пресечения спама нет, все методики обеспечивают отсечение только части нежелательной корреспонденции. При этом до половины спама все-таки попадает в почтовый ящик пользователя. Поэтому самым верным решением будет соблюдение правил профилактики, изложенных ниже.

Выбор адреса электронной почты

Одним из распространенных в последнее время способов массовой рассылки является отправка корреспонденции по почтовым ящикам, адреса которых совпадают с именами или наиболее употребительными терминами. Программа автоматизированной рассылки пытается отправить письма на почтовые серверы для пользователей, адреса электронной почты которых имеют вид **anna@server.ru**, **dima@server.ru**, **alexandr@server.ru**, **info@server.ru** и т. п. Например, на почтовый сервер организации, в которой работает автор книги, ежедневно приходит более тысячи писем, сформированных по данному принципу. В листинге, представленном ниже, приведена часть реального SMTP-протокола почтового сервера, иллюстрирующая подобные попытки массовой рассылки писем. В соответствии с этим протоколом, 18 декабря 2004 года в 3 часа хост с IP-адресом 69.153.81.161 пытался передать несколько писем. Причем ясно видно, что адресаты выбирались на основе перебора типовых имен (после команды `RCPT TO:` следует адрес получателя). Каждый раз почтовый сервер отвечал, что такого адресата нет в организации (код ответа 550 в соответствии со стандартами Интернета).

```
...
2004-12-18 03:01 69.153.81.161 RCPT — +TO:+<sergey@ask.ru>   550
2004-12-18 03:01 69.153.81.161 RCPT — +TO:+<sergeym@ask.ru>  550
2004-12-18 03:01 69.153.81.161 RCPT — +TO:+<serg@ask.ru>     550
2004-12-18 03:01 69.153.81.161 RCPT — +TO:+<scorpion@ask.ru> 550
2004-12-18 03:01 69.153.81.161 RCPT — +TO:+<sergei@ask.ru>   550
2004-12-18 03:01 69.153.81.161 RCPT — +TO:+<serge@ask.ru>    550
2004-12-18 03:01 69.153.81.161 RCPT — +TO:+<ruslan@ask.ru>   550
2004-12-18 03:01 69.153.81.161 RCPT — +TO:+<sasha@ask.ru>    550
...
```

Анализируя ответы почтового сервера, спамеры могут достаточно быстро протестировать организацию на наличие типовых адресов (соответствующие

программы легко найти в Сети) и осуществлять в дальнейшем рассылку только по существующим адресам почты.

Поэтому, создавая почтовый ящик, никогда не используйте тривиальные адреса. В крайнем случае при создании адреса добавьте к имени первую букву фамилии или используйте иной вариант.

Периодическая смена почтового адреса

Единственный способ радикального устранения спама в вашем почтовом ящике — это периодическая смена адреса электронной почты. Если адрес попал в базу "спамеров", то избавиться от нежелательной корреспонденции уже невозможно. Поэтому используйте в своей работе несколько почтовых адресов, периодически меняя общеизвестные и максимально защищая адреса, предназначенные для узкого круга общения.

Защищайте адреса электронной почты

Существует несколько источников пополнения базы адресов для использования в спаме. Прежде всего, адреса электронной почты получают путем автоматизированной обработки открытой информации — электронных писем в конференциях и страниц информационных серверов Интернета.

"Вычисление" электронных адресов из сообщений конференций — один из наиболее используемых методов. Сообщения конференций публично доступны на многих серверах Интернета. Существуют специальные программы, которые просматривают сообщения и автоматически формируют списки их авторов.

Поэтому первая предупредительная мера защиты от спама состоит в использовании фиктивных адресов при работе в конференциях Интернета. Никогда не пишите письма в конференции Интернета со своего почтового ящика. Зарегистрируйте бесплатный ящик на любом доступном сервере и осуществляйте работу от его имени. Если на него начнет поступать спам, то вы легко сможете удалить данный почтовый ящик и продолжить работу от имени нового бесплатного ящика.

Если необходимо сохранить возможность прямого ответа на ваше сообщение в конференцию, то модифицируйте личный адрес так, чтобы автоматизированная программа не могла его использовать. Например, вместо **al@mail.ru** запишите: **al@mail_*удалите*_.ru**. Читающий легко восстановит исходный адрес, а программа "получит" реально отсутствующее значение.

Еще один открытый источник адресов электронной почты — это страницы информационных серверов Интернета. Размещая на них контактную информацию, мы не предполагаем, что она будет использована для автоматизированной рассылки рекламы. Однако роботы в автоматическом режиме могут

собирать такие контакты. Существует простой способ скрытия адресов электронной почты от большинства средств автоматического отслеживания: это использование Java-сценариев при создании страницы. Например, если в ссылке вместо электронного адреса записать вот такой сценарий:

```
document.write("Ivanov")
document.write("@")
document.write("test.ru")
```

то адрес электронной почты будет скрыт от программ автоматического просмотра, хотя для пользователей страница будет функционировать в полном объеме. На странице будет показана ссылка с верным адресом, при щелчке по ней откроется почтовая программа, в поле **Кому:** будет занесено верное значение адреса.

Если вы собираетесь сообщить свой адрес...

Часто посещаемые страницы информационных серверов требуют введения тех или иных регистрационных данных. Несмотря на все заверения в сохранении конфиденциальности данной информации, можете ли вы быть уверены в том, что эта организация не будет использовать полученные данные в каких-либо иных целях? Или в том, что хакеры, воспользовавшись ошибками защиты информации, не получат доступ к этим секретам? Известно множество примеров, когда в Интернете публиковались даже данные кредитных карточек, полученные с сайтов весьма солидных организаций. Не лишне вспомнить и случай, когда данные миллионов пользователей America Online (AOL, крупнейший интернет-провайдер США) были просто проданы техническим специалистом.

Поэтому, если нет веских оснований, *никогда ни на каком сайте* не вводите свои реальные данные. Если регистрация проводится для того, чтобы получить, например, доступ к определенным ресурсам (в результате вам вышлют ссылку на необходимый файл или пароль доступа), то используйте адрес бесплатного почтового ящика, от которого легко будет отказаться впоследствии.

Примечание

Практикуются и иные варианты сбора адресов. Например, вы можете получать сообщения, в которых анонсируется тот или иной проект и пользователю предлагается поддержать его, направив письмо по соответствующему адресу. В большинстве случаев это вариант сбора реальных адресов пользователей Интернета.

Подумайте не один раз, прежде чем сообщите какому-либо открытому источнику свой электронный адрес!

Не отвечайте на письма спама

Часто в письмах массовой рассылки содержится фраза: "если вы не хотите получать в дальнейшем данную информацию, пошлите письмо с просьбой исключить этот адрес из списка рассылки". Если это только не письмо от известной фирмы — никогда не отвечайте на подобные предложения. Адрес вашего ящика уже попал к спамерам, а такой ответ будет только подтверждением реальности адреса.

Безопасность электронной почты

Обладая рядом удобств, электронная почта не является вполне безопасным средством передачи информации.

Во-первых, текст электронного письма передается по каналам связи в открытом виде. Любой оператор системы передачи данных может получить доступ к той информации, которая содержится в электронном письме. А учитывая возможности современной техники, совсем не сложно организовать сплошной контроль информации на основе поиска тех или иных ключевых слов.

Во-вторых, каждый может создать письмо и подписать его именем и электронным адресом другого человека. Или же "перехватить" письмо, внести в него небольшие, но очень важные изменения и отправить дальше по назначению. Так, вы можете получить письмо, в котором говорится, что "в связи с такими-то техническими неполадками произошло разрушение данных; приносим извинения и просим сообщить по обратному адресу то-то и то-то" (например, пароль входа в Интернет), или сообщение об обнаружении неисправности в программном обеспечении с приложением файла-заплатки и предложением его установки. В подобных случаях, если в письме содержатся определенные просьбы или от вас пытаются получить любую значимую информацию, необходимо быть абсолютно уверенным в подлинности письма.

Учитывая вышесказанное, в особо ответственных случаях используется электронная подпись и шифрование текста письма. При получении письма, имеющего тот или иной вариант защиты, почтовая программа покажет состояние сообщения (изменялось ли письмо по пути или дошло в целости и сохранности) и подтвердит подлинность автора сообщения.

Получение сертификата

Описание методов защиты почтовых сообщений предполагает знакомство читателя с основами технологии PKI, более подробно освещенной в *главе 12*.

Чтобы защитить свои отправления, необходимо получить сертификат, предназначенный для использования в электронной переписке. Для внутренней переписки достаточно сертификата от удостоверяющего центра самой орга-

низации. Если использовать такой сертификат для подписания сообщения в другую организацию, то у его получателя появится предупреждение почтовой системы об отсутствии доверия к системе, сформировавшей электронную подпись. Поскольку при этом отображается знак предупреждения (опасности), то в большинстве случаев пользователи просто не будут даже и пытаться открыть такое письмо, хотя возможность выяснить причину такого предупреждения существует: достаточно только прочесть описание событий.

Если необходимо использовать защищенную переписку между двумя организациями, то существует два варианта решения. Первый — это обменяться сертификатами удостоверяющих центров своих организаций и установить к ним доверие в каждой организации. Недостаток подобного решения — такие "обмены" придется осуществлять с *каждой* организацией, с сотрудниками которой необходимо осуществлять защищенную переписку.

Второй способ заключается в использовании сертификатов от удостоверяющих центров, к которым по умолчанию существуют доверительные отношения в операционной системе. В большинстве случаев получение подобного сертификата является платной услугой, хотя некоторые центры предоставляют возможность получения бесплатных сертификатов[1].

Примечание

При получении сертификатов удостоверяющих центров в Интернете требуется разрешение на запуск соответствующих модулей ActiveX и, как следствие, наличие административных прав у текущего пользователя.

После получения сертификата вы можете включить шифрование почты и электронную подпись. Настройка использования сертификата в программе MS Outlook производится с помощью опций, содержащихся на вкладке **Безопасность**. Достаточно просто указать сертификат, который будет использован при работе с безопасными сообщениями.

Работа с безопасными сообщениями не представляет сложности. Система автоматически шифрует или декодирует сообщение, пользователю достаточно только включить соответствующую опцию (рис. 7.2).

Электронная подпись

Электронная подпись гарантирует, что текст письма написан конкретным пользователем и по пути следования в него не было внесено никаких изменений.

[1] Например, **www.thawte.com** и др. Обычно такие сертификаты не предполагают возможности строгого шифрования сообщения и фактически удостоверяют только сам адрес электронной почты.

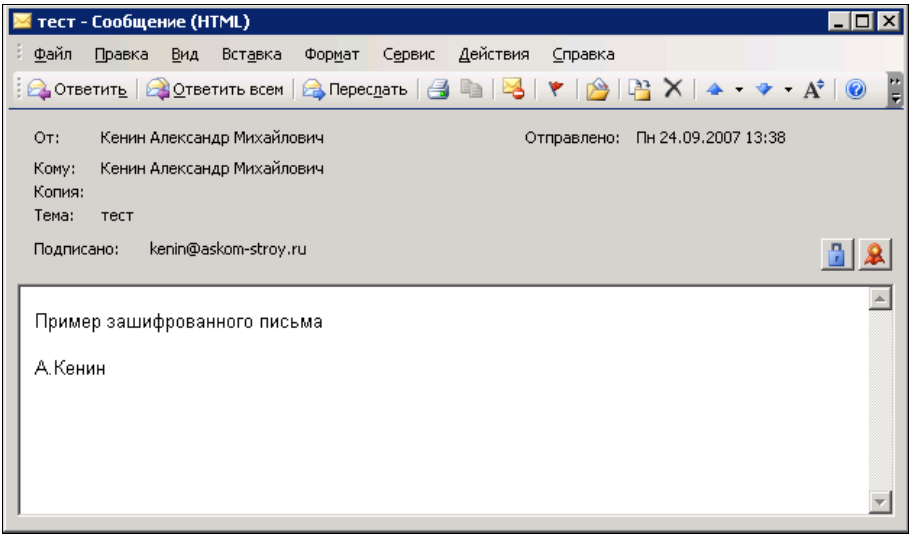


Рис. 7.2. Образец почтового сообщения с электронной подписью и шифрованием текста. О том, что письмо зашифровано, сообщает только пиктограмма замочка в панели инструментов. Сам текст автоматически расшифрован программой в момент открытия сообщения. Уточнить параметры шифрования и электронной подписи можно, если щелкнуть по соответствующим пиктограммам

Подпись формируется следующим образом. Для текста сообщения (и вложений) вычисляется *хэш*, который шифруется с помощью *закрытого ключа пользователя*. Полученный код добавляется к электронному сообщению.

В точке приема почтовая программа, во-первых, вычисляет хэш полученного сообщения. Во-вторых, пытается дешифровать хэш, вложенный в письмо при его отправке. Если программе удается дешифровать хэш (его расшифровка производится с помощью открытого, т. е. публично доступного ключа пользователя), то это означает, что письмо действительно получено от этого автора. Если расшифрованный хэш совпадает с тем, который вычислен для принятого письма, то это подтверждает отсутствие изменений в сообщении.

Шифрование текста

Шифрование текста предполагает его специальное кодирование для того, чтобы текст письма не был доступен постороннему лицу как при передаче сообщения по каналам связи, так и в случае хранения письма на локальном компьютере или почтовом сервере.

Можно использовать различные варианты шифрования сообщений, но одним из самых удобных является стандарт SMIME[1]. Почтовая программа шифрует

[1] Часто используется также вариант шифрования по технологии PGP *(см. разд. "Pretty Good Privacy" главы 10)*.

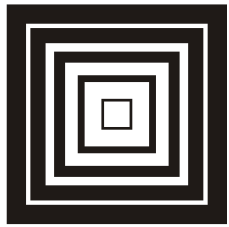
текст письма и пересылает полученный код в виде файла, вложенного в обычное почтовое сообщение, поэтому шифрованные письма могут без каких-либо дополнительных настроек пересылаться обычными почтовыми системами.

Примечание

Почтовой программе может быть не известен формат SMIME, и тогда вместо текста письма будет показан файл вложения с расширением p7m. Если получатель "видит" подобный файл, то ему следует установить новую версию почтового клиента.

Шифрование сообщения производится с помощью открытого ключа получателя письма. Поэтому расшифровано оно может быть только тем пользователем, у которого имеется соответствующий закрытый ключ. А это только тот пользователь, *кому* адресуется сообщение.

Поскольку для шифрования требуется знать открытый ключ получателя, то его необходимо иметь *до отправки письма*. В рамках организации (домена Windows) открытые ключи пользователей доступны через службу каталогов. Если же вы хотите написать письмо внешнему адресату, то предварительно следует получить его открытый ключ, например, запросив письмо с электронной подписью.



ГЛАВА 8

Взаимодействие с глобальной сетью

Основное правило при подключении компьютеров к Интернету заключается в обязательном использовании межсетевого экрана (брандмауэра) для защиты локальных ресурсов. Большинство малых и средних организаций имеют только один канал доступа к Интернету, поэтому классическим решением является установка брандмауэра между каналом доступа в Интернет и локальной сетью. В этом случае в локальной сети используются частные адреса *(см. разд. "IP-адрес" главы 3)*, а для *преобразования сетевых адресов* применяется, в том или ином варианте, технология Network Address Translator (NAT). Настройка компьютеров локальной сети на реальные адреса Интернета имеет смысл в весьма редких ситуациях, когда невозможно использовать трансляцию адресов *(см. ниже)*, но и в этом случае компьютеры должны быть защищены от доступа извне с помощью брандмауэра.

Примечание

Конечно, технически возможно просто маршрутизировать локальную сеть, если для нее выделены реальные адреса Интернета. Однако такое подключение *крайне не рекомендуется*, поскольку меры по обеспечению безопасности данных при подключении к Интернету необходимо будет реализовать в этом случае на *каждом* компьютере.

Для доступа мобильных сотрудников из глобальной сети к ресурсам локальной, как правило, применяется технология *виртуальных частных сетей (см. разд. "VPN" далее в этой главе)*. В этом случае для компьютера создается виртуальный канал подключения к локальной сети, причем передаваемые по нему данные шифруются и недоступны для злоумышленника.

Защита информационных систем

В современной информационной системе объединяются различные задачи с отличающимися категориями информации, а опасность часто исходит не из-

за периметра организации, а от имеющих доступ пользователей. Поэтому *каждая* автоматизированная система в составе общей информационной системы должна быть защищена межсетевым экраном.

Традиционно существовало понятие *демилитаризованной зоны* (Demilitarized zone, DMZ), которым обозначали компьютеры, чьи ресурсы должны быть опубликованы в Интернете.

DMZ представляет собой специально организованную подсеть локальной сети, которая отделена межсетевыми экранами как от Интернета, так и от компьютеров локальной сети (рис. 8.1). При этом внутренний периметр настраивается без публикации ресурсов, в крайнем случае настраиваются фильтры *только* для пакетов, соответствующие нормальной работе пользователей с серверами DMZ-зоны. При такой конфигурации сети злоумышленнику, сумевшему взломать компьютер с опубликованной службой, крайне сложно, если не совсем невозможно получить доступ к другим локальным ресурсам.

DMZ-зону можно создать с использованием двух брандмауэров (рис. 8.1, *а*) или одного, но имеющего три сетевых адаптера (рис. 8.1, *б*). Второй вариант хотя и несколько дешевле, но более трудоемок в настройке и требует повышенного внимания администратора.

По этим принципам (используя межсетевой экран) необходимо защищать *все* автоматизированные системы.

Примечание

Автоматизированная система может быть изолирована путем создания VLAN. Таким образом фильтрация трафика между различными системами будет осуществляться при его маршрутизации из одной VLAN в другую.

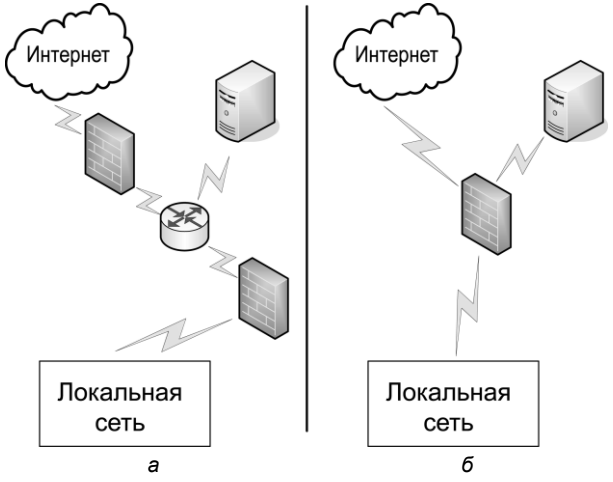


Рис. 8.1. Варианты создания демилитаризованной зоны:
а — с использованием двух брандмауэров; *б* — с использованием одного брандмауэра

NAT

Технология трансляции адресов (Network Address Translator, NAT) позволяет осуществить подключение к Интернету практически любого числа компьютеров, использовав при этом всего лишь один или несколько реальных адресов глобальной сети. Фактически NAT — это IP-маршрутизатор, который способен преобразовывать (транслировать) адреса и номера портов TCP/UDP-пакетов в процессе их пересылки.

Логика работы NAT достаточно проста. При получении от локального компьютера пакета, предназначенного для внешней сети, маршрутизатор пересылает пакет, заменив в нем частный IP-адрес на реальный IP-адрес, выделенный провайдером Интернета, и TCP-порт (или UDP-порт) источника на другой, *перенумерованный* порт. Информация об этом преобразовании сохраняется программой. После получения ответа NAT ищет в своих записях, для какого локального запроса был выделен соответствующий порт. Если такая информация обнаружена, то NAT пересылает пакет локальному компьютеру, заменяя в пакете перенумерованный порт на исходный. Если NAT не находит у себя записи о перенумерованном порте, то пакет отбрасывается.

Таким образом, сервер NAT заменяет в пакетах адреса источника (назначения), номера портов и пересчитывает контрольную сумму пакета. Для большинства приложений такие изменения не вызывают каких-либо осложнений. Однако некоторые протоколы, например FTP, передают информацию о IP-адресах в своих данных, поэтому для корректной работы таких протоколов NAT модифицирует и сами TCP-последовательности. Так, в Windows 2000 встроены редакторы для протоколов FTP, ICMP, PPTP, NetBIOS поверхTCP/IP. Если в организации на каком-либо компьютере применяется протокол, для которого необходимо внести аналогичные изменения в сам пакет, а соответствующего редактора в операционной системе не предусмотрено, то работа через NAT будет невозможна без использования для такой системы реального адреса.

NAT применяется в Windows при включении совместного использования подключения к Интернету *(см. разд. "Совместное использование интернет-подключения" далее в этой главе)*. Для серверных систем его настройка осуществляется через оснастку RRAS.

Примечание

NAT от Windows Server может осуществлять трансляцию как на частные адреса локальной сети, так и на реальные адреса. Если доступно несколько реальных адресов, то NAT сопоставляет частный IP-адрес с реальным. В этом случае трансляция портов не осуществляется. При исчерпании реальных адресов NAT включает трансляцию портов.

Для настройки NAT после установки данной службы в RRAS следует добавить интерфейсы подключения к Интернету и локальной сети к протоколу маршрутизации NAT, для чего на вкладке **Общие** (General) свойств интернет-интерфейса установить переключатель **Общий интерфейс подключен к Интернету** (Public Interface connected to the Internet), а для интерфейса локальной сети — **Частный интерфейс подключен к частной сети** (Private interface connected to private network). При использовании одного адреса подключения к Интернету нужно установить переключатель **Преобразовать TCP/UDP-заголовки** (Translate TCP/UDP headers) для свойств интернет-интерфейса.

Примечание

Для упрощения конфигурации малых сетей NAT включает в себя DHCP-распределитель и DNS-прокси. Эти компоненты позволяют выделять клиентам локальной сети IP-адреса, а сам NAT-сервер выступает в качестве DNS-сервера.

Из описания работы NAT видно, что он защищает сеть предприятия от злоумышленника, "принимая" только *ответы* на запросы из локальной сети. Если вам необходимо опубликовать некоторые ресурсы локальной сети в Интернете, то следует создать соответствующие правила в оснастке NAT, которые определят, на какой частный адрес пересылать заданные протоколы.

Такой алгоритм работы достаточно эффективен и подходит в большинстве случаев. Однако он может приводить к неработоспособности отдельных функций программ, если они активируются внешними запросами. Например, почтовый клиент MS Outlook при работе с сервером MS Exchange использует протокол RPC. Пройдя регистрацию на почтовом сервере, клиент находится в состоянии ожидания сигнала о приходе новой почты. Поскольку инициатором такого сигнала является не клиент, а внешняя система, то брандмауэр блокирует эти пакеты. Поэтому в данном примере клиент не будет получать автоматические сообщения о приходе новой почты, хотя сможет принимать и отправлять сообщения по команде пользователя.

Межсетевой экран (брандмауэр)

Межсетевой экран, или брандмауэр (firewall), — это комплекс технических, программных и организационных мер по безопасному подключению одной сети к другой. В зависимости от решаемых задач и конфиденциальности защищаемой информации это может быть просто небольшая программа, установленная на компьютере, а также специализированные аппаратные средства, реализующие требования конкретной организации.

Обычно по общим соображениям безопасности в качестве брандмауэра рекомендуется использовать автономное устройство. Иными словами, в случае

программной реализации брандмауэра на этот компьютер не следует возлагать решение никаких других задач.

Что может брандмауэр и чего не стоит от него ожидать?

Брандмауэр осуществляет фильтрацию как передаваемых данных, так и принимаемой информации. Он позволяет отсечь те пакеты, которые нежелательны для данной сети, и направлять внешний трафик только к назначенным компьютерам. Брандмауэры скрывают внутреннюю структуру локальной сети.

В то же время брандмауэр никоим образом не защищает от "дыр", которые могут быть в разрешенных сервисах и которыми может воспользоваться злоумышленник для проникновения в локальную сеть. Так, широко известен пример, когда в одну из версий популярного бесплатного FTP-сервера был встроен троянский вирус, позволяющий перехватывать управление сервером. Кроме того, возможен вариант перехвата управления над компьютером в локальной сети путем внедрения трояна, открывающего соединение с сервером управления изнутри.

Учитываемые параметры фильтрации

В зависимости от конкретной системы брандмауэра могут быть реализованы различные варианты фильтрации проходящих данных, в частности, возможно:

- открывать или запрещать прохождение данных в зависимости от времени суток и дней недели;
- разрешать прохождение явно заданных протоколов;
- фильтровать информацию в зависимости от адреса отправителя/адреса получателя;
- разрешать передачу данных в зависимости от результатов аутентификации отправителя;
- фильтровать получение данных в зависимости от содержания информации.

Возможны различные комбинации этих параметров: можно запретить работу с определенным перечнем хостов Интернета некоторому кругу сотрудников в рабочее время или заменить рекламу, формируемую баннерными системами, "пустыми" местами на страницах. В качестве примера на рис. 8.2 представлено окно настройки параметров межсетевого экрана Kerio WinRoute Firewall

6.4, в котором определяются ключевые слова, по которым будут блокированы запросы к страницам Интернета.

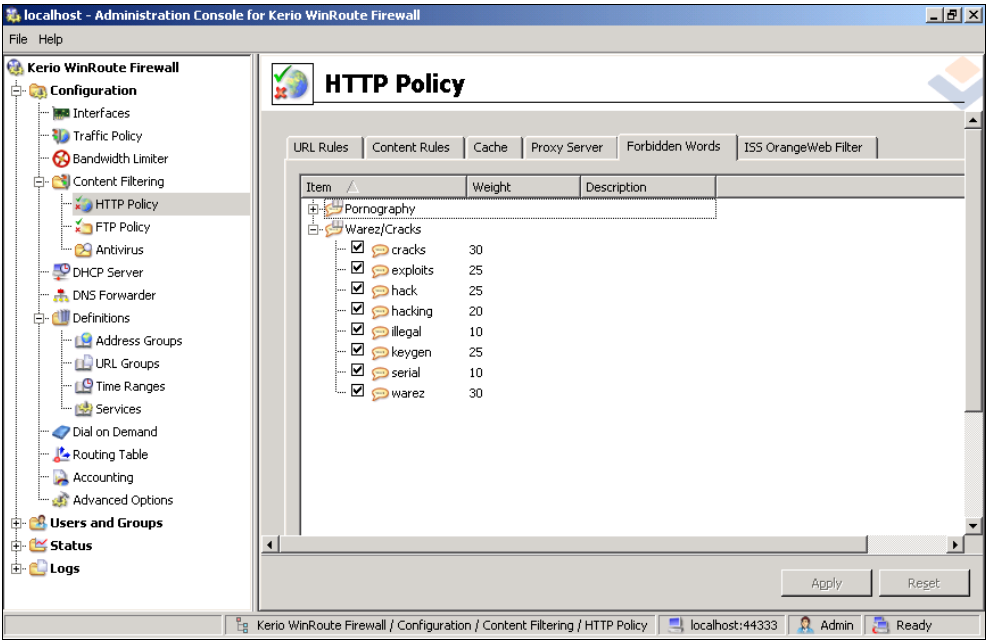


Рис. 8.2. Фильтрация контента средствами межсетевого экрана

Кроме того, обычно брандмауэры имеют ряд дополнительных сервисных возможностей: позволяют организовать протоколирование работы (учет трафика Интернета по пользователям, адресам, объему и т. п.), выявлять атаки со стороны внешней сети и направлять сообщения об этом администратору для принятия соответствующих мер, управлять используемой полосой доступа в Интернет и т. п.

Варианты организации брандмауэров

Все способы фильтрации, применяемые в традиционных брандмауэрах, условно можно разделить на фильтрацию пакетов и использование шлюзов уровня сессии или уровня приложения. В большинстве случаев реальные системы комбинируют эти варианты.

Фильтрация пакетов

При фильтрации пакетов разрешения на прием/передачу данных выдаются только на основе анализа IP-адреса и номера порта источника пакета и его

назначения. Хотя настройка фильтрации пакетов несколько трудоемка и требует знания основных параметров протоколов и особенностей функционирования системы, данный вариант является самым простым и быстрым способом реализации брандмауэра.

Примечание

Принципиально существуют возможности "обмануть" такой брандмауэр, например, фальсифицируя адреса в пакетах.

Шлюзы

Шлюзы уровня сессии организуют временные соединения между клиентом и хостом Интернета на основе некоторых заданных правил. После создания такого канала вся информация, передаваемая по нему, свободно пропускается. После завершения сессии канал уничтожается.

Более совершенным считается другой способ организации шлюзов — шлюзы уровня приложения (часто называют *прокси-серверами*). Прокси-серверы обычно принимают запросы (как извне сети, так и изнутри), аутентифицируют пользователя, анализируют запросы и перенаправляют их в зависимости от содержимого (например, заблокируют определенный запрос на внутренний WWW-сервер, а другой отошлют на соответствующее устройство). Фактически между клиентом и хостом Интернета образуется цепочка из двух соединений: от клиента до прокси и от прокси до хоста Интернета. Таким образом, запрещается прямой доступ к внутренним ресурсам организации, а весь трафик считается исходящим (входящим) от имени прокси-сервера.

Прокси-серверы имеют развитые возможности аутентификации пользователей, хорошие механизмы протоколирования своей работы и обеспечивают наибольший уровень защиты локальной сети.

Intrusion Prevention Systems

Описанные выше способы фильтрации трафика в конечном итоге разрешают по тем или иным правилам доступ "хорошим" пользователям (или службам) и запрещают "плохим". Такая практика постепенно теряет свою эффективность, поскольку вредоносные коды все больше и больше "подстраиваются" под существующие методы защиты. Например, что мешает какой-либо программе воспользоваться разрешением доступа в Интернет для передачи "подсмотренных" на компьютере данных на какой-либо сервер глобальной сети, маскируясь при этом под обычную работу пользователя? А если деятельность компании тесно связана с глобальной сетью, то сетевые атаки на ее серверы, имеющие целью вызвать отказ в обслуживании клиентов, могут повлечь за собой миллионные убытки.

Для предотвращения подобных вторжений в инфраструктуру предприятия стали применяться аппаратные и программные решения, *контролирующие содержание* передаваемых по сети пакетов с целью обнаружения подозрительной активности. Первоначально такие системы контролировали сеть параллельно основным устройствам и выдавали сигналы опасности при обнаружении подозрительных данных. Они получили название Intrusion Detection Systems (IDS).

Современные системы предотвращения атак — Intrusion Prevention Systems (IPS) — выполняют активную функцию. Они не только обнаруживают атаку, но и сразу же блокируют подозрительный трафик. Подобные системы могут обнаружить подготовку DoS-атаки, блокировать трафик программ, используемых для передачи данных между пользователями (типа Kazaa, Gnutella, ICQ и т. п.), обнаруживать сетевые черви, активность эксплойтов и т. п. (рис. 8.3).

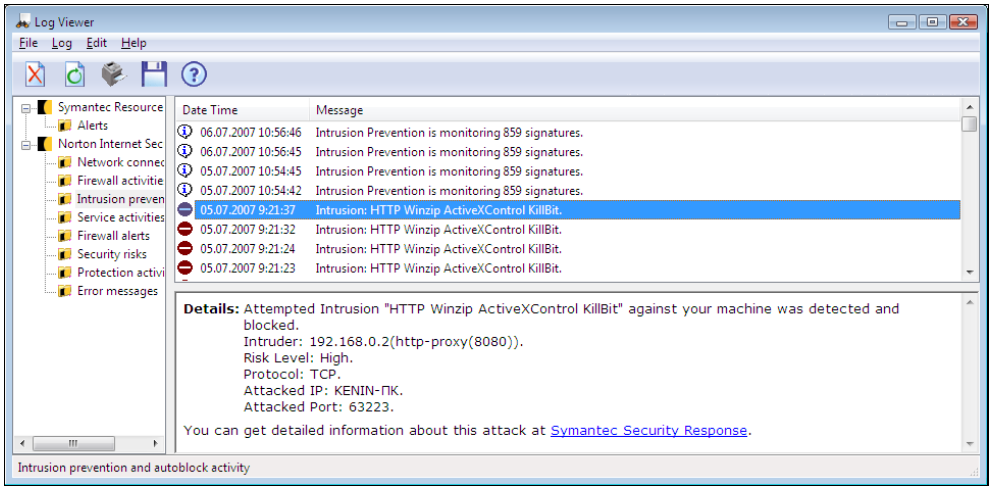


Рис. 8.3. Программа Norton Internet Security 2007 блокировала вторжение на пользовательский компьютер

Принцип действия IPS основан, прежде всего, на сравнении информации, передаваемой по сети, с заранее известными сигнатурами, которые присутствуют в пакетах, передаваемых червями, в пакетах программ, использующих те или иные уязвимости программного обеспечения, и т. п. Состав сигнатур постоянно обновляется с сайтов разработчиков IPS. Кроме того, IPS могут обнаруживать аномальные изменения трафика (например, резкое увеличение пакетов определенного типа) и сохранять пропускную способность канала для "полезных" данных.

Понятно, что с увеличением количества сигнатур, учитываемых при анализе содержимого пакета данных, растет нагрузка на устройство и, в конечном итоге, снижается его пропускная способность, поэтому надежно защитить весь сетевой трафик организации практически[1] невозможно. IPS применяют в пограничных точках: на стыке Интернета и локальной сети организации, между серверным сегментом и пользовательской частью.

Как уже говорилось, технологии предотвращения атак могут быть программными или аппаратно-программными. Можно отметить, например, новое поколение Check Point — брандмауэр, используемый большинством крупнейших компаний мира для защиты своих ресурсов, который включает в себя технологию *SmartDefense*, предназначенную для анализа проходящего трафика. Существуют и специализированные решения от Tipping Point (**www.tippingpoint.com**), Internet Security Systems (**www.iss.net**), Radware (**www.radware.com**), TopLayer (**www.toplayer.com**) и др.

Использование решений данного класса чувствительно увеличивает расходы предприятия с одной стороны и предъявляет повышенные требования к уровню подготовки администратора с другой стороны. Поскольку подобные дополнительные расходы для небольших предприятий обычно не оправданы, то в них используются традиционные программы брандмауэров. В то же время данная функциональность стала включаться в антивирусное программное обеспечение ведущих вендоров (например, Symantec Norton Internet Security 2007, Trend Micro Office Scan и т. п.).

Защищенный доступ в сеть

В условиях корпоративной сети состояние компьютера достаточно хорошо контролируется администраторами. Но при автономной работе мобильных устройств существуют серьезные риски отступлений от корпоративной политики: необновления антивирусных баз, установки зловредного программного обеспечения и т. п. Для исключения негативного влияния подобных компьютеров на информационную систему стали разрабатываться различные технологии. И хотя их использование не стало стандартом, уже в Windows Vista внедрена технология[2] безопасного доступа к сети (Network Access Protection, NAP).

---

[1] Хотя функция Cisco Intrusion Detection Systems и включена в ПО коммутаторов Cisco, начиная с IOS Software Release 12.0.(5), производитель предупреждает о снижении производительности устройства при увеличении числа сигнатур в используемых политиках предотвращения атак.

[2] Технология NAP предусматривает взаимодействие клиента Windows Vista с новой версией сервера Windows, на момент написания книги находящейся еще на этапе разработки. Поэтому вполне возможно, что компоненты NAP существенно изменятся к моменту выпуска сервера и к моменту выпуска ее пакета обновления в Vista будут заменены.

Технология NAP предусматривает ограничение использования ненадежными системами следующих сетевых служб:

- ❒ служб IPsec (Internet Protocol security protected communication);
- ❒ подключений с использованием протокола 802.1x;
- ❒ создания VPN-подключений;
- ❒ получения конфигурации от DHCP-сервера.

Идея проверки проста. Клиент, желающий получить один из перечисленных выше сервисов, должен предоставить о себе определенные данные. На момент написания книги существовала только возможность проверки выполнения параметров, определяемых центром безопасности сервера: наличия антивирусной программы, обновлений, настроек брандмауэра и т. п. Эти данные предоставляются специальной программой с клиентского компьютера (агентом) и анализируются службами сервера. В случае прохождения проверки (соответствия настроек параметрам, заданным администратором) клиентский компьютер получает сертификат, дающий право на использование запрашиваемых услуг. Если проверка не прошла, то дальнейшее поведение будет зависеть от выбранных администратором настроек: либо будет проведено обновление до нужного уровня безопасности, либо введены некоторые ограничения в работе и т. п. На рис. 8.4 представлено сообщение, которое получает

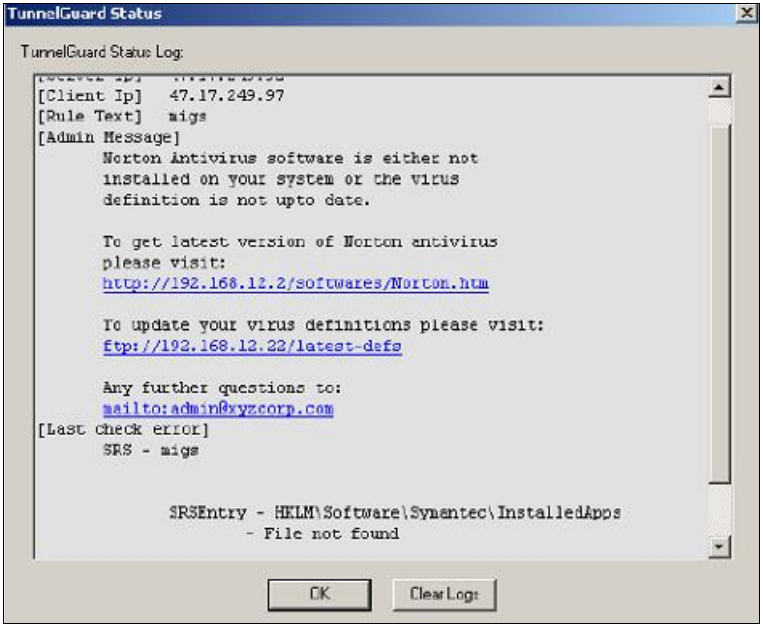


Рис. 8.4. Сообщение системы безопасного доступа о действиях, требуемых от пользователя для подключения к сети

пользователь от системы безопасного доступа к сети, реализованной на оборудовании Nortel: программа предлагает посетить указанный сайт и установить отсутствующее программное обеспечение.

Примечание

Сходная технология ограничения была предусмотрена и для подключения клиентов удаленного доступа (помещение клиентов в карантин с ограниченным доступом во внутреннюю сеть). На практике эта технология не нашла распространения, поскольку требовала разработки специальных программ, проверяющих выполнение условий, предъявляемых к подключаемым системам.

Варианты брандмауэров

В распоряжении администраторов имеются как *аппаратные* брандмауэры, так и *программные* решения. Различие между этими двумя вариантами достаточно условно. Аппаратный модуль — это фактически специализированная под определенную задачу та или иная вычислительная система. Обычно для него создается операционная система (например, IOS у Cisco) или используется бесплатная версия Linux.

Программные варианты предполагают установку на типовые операционные системы, например: на Linux, операционные системы от Microsoft и т. п.

Аппаратные решения

На сегодня для малых предприятий наиболее дешевым решением являются аппаратные брандмауэры (стоимость их менее $200).

Такие модели выпускают практически все производители коммутационного оборудования. Имеются комплексные решения, например ADSL-модем и брандмауэр в одном корпусе.

В зависимости от сложности устройства доступны различные уровни защиты сети. Но даже самые дешевые модели включают в себя такие функции, как статическую фильтрацию пакетов, наличие DMZ-портов, возможность создания VPN-подключений, NAT-трансляцию с сервером DHCP, средства предупреждения администратора (отправка e-mail и т. п.).

Встроенный брандмауэр Windows XP/Server 2003

В операционных системах Windows XP/Server 2003 для локальной сети можно использовать встроенные возможности защиты подключения к Интернету.

Примечание

Начиная с версии Windows XP SP2, брандмауэр включается по умолчанию.

Для включения защиты достаточно установить флажок на вкладке **Дополнительно** окна свойств соединения, с помощью которого осуществлен доступ в Интернет. Если соединение применяется для совместного доступа к Интернету *(см. разд. "Совместное использование интернет-подключения" далее в этой главе)*, то брандмауэр будет защищать *все* компьютеры, работающие с глобальной сетью через данное подключение.

Принцип работы встроенного брандмауэра аналогичен описанной выше технологии NAT.

Если внутри защищаемой брандмауэром сети (на локальном компьютере или на компьютерах, осуществляющих выход в Интернет через данное совместно используемое подключение) имеются службы, к которым необходимо разрешить доступ извне, то администратору следует осуществить *публикацию* этих ресурсов. Для этого нужно нажать кнопку **Параметры** в окне включения брандмауэра. Появится окно, где следует определить параметры служб, которым разрешен доступ в локальную сеть.

Расширенные возможности межсетевого экрана Windows Vista

В Windows Vista расширены возможности фильтрации трафика встроенными средствами. Теперь пользователи могут создавать правила не только для входящего, но и для *исходящего* трафика. Кроме того, в системе существуют три *профиля* брандмауэра. Один соответствует подключению к частной сети, другой — к публичной сети, третий используется при работе в составе домена Windows. Профили представляют собой наборы правил, оптимизированные для работы в условиях соответствующей сети. Количество профилей изменить нельзя, но пользователь может изменить состав и настройку правил, составляющих тот или иной профиль.

Каждый профиль имеет правила по умолчанию для входящего и исходящего трафика. Они применяются в случае отсутствия для пакета данных явно определенного правила. Для исходящего трафика правило по умолчанию для всех профилей разрешает все, для входящего трафика — все блокирует. Вы можете изменить эти установки, например, запретить передачу данных из компьютера в сеть. В этом случае необходимо создать разрешающее правило для передачи необходимых данных вовне.

По умолчанию в профиле созданы наборы разрешающих правил, которые обеспечивают работу компьютера в составе сети Microsoft. Наборы правил довольно объемны, но на начальных этапах настройки Windows Vista можно сохранить предложенные изготовителем настройки.

Операции выполняются под руководством мастера (рис. 8.5); их выполнение не представляет особой сложности.

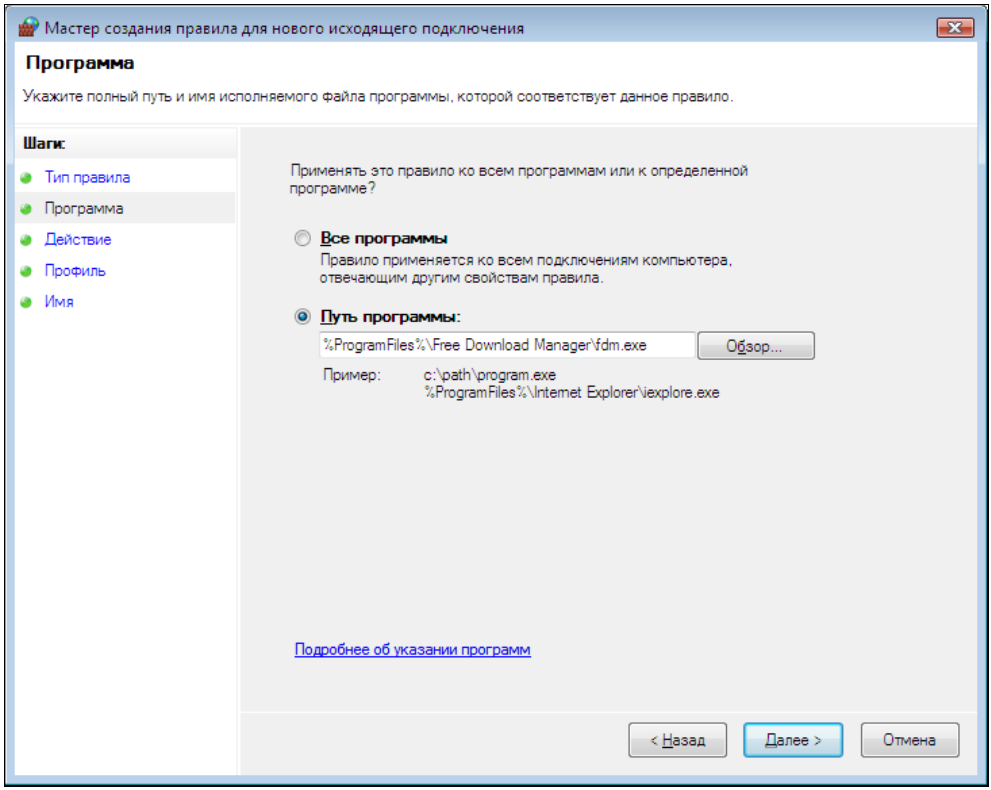


Рис. 8.5. Мастер создания правила для *исходящего* трафика в Windows Vista

Хотелось бы обратить особое внимание на следующие моменты.

Правило можно создать для программы, службы или порта. Если есть возможность, нужно выбирать программу или службу. Дело в том, что порт открывается созданным правилом на все время работы брандмауэра, а если правило создано для программы, то порт будет открыт только в период активности соответствующей программы. Это более безопасная ситуация.

Примечание

Брандмауэр может использовать эти настройки только для программ, работающих через Windows Socket. Поскольку особенности построения конкретной программы заранее не известны, то после создания правила следует проверить его работоспособность и при наличии ошибок выполнить настройку на основе протокола (порта).

Выбор настраиваемого правила необходимо сделать, если предполагается фильтровать трафик в зависимости от адресов источника и назначения. Правило позволяет определить как один адрес, так и диапазон IP-адресов. Кроме

того, можно указать в правиле группу компьютеров по их функциональному назначению: WINS-, DHCP- или DNS-серверы, шлюз или локальная подсеть. Такое назначение позволяет более точно настроить правила с учетом возможного переноса данных ролей на другие компьютеры сети.

Программные комплексы

На рынке существует большое количество предложений межсетевых экранов. Администратор имеет возможность выбрать решения, обладающие большей или меньшей функциональностью. В любом случае перед тем, как внедрять решение, администратор должен тщательно взвесить желаемые требования и возможные стоимостные оценки реализации.

В Сети существует большое количество программ, предназначенных для защиты индивидуальных компьютеров. Например, можно отметить такие персональные брандмауэры, как AtGuard, BlackICE Defender, Jammer, Kerio Personal Firewall, Outpost Firewall, Sygate Personal Firewall, Tiny personal firewall, Zone Alarm и др. Часть этих продуктов — коммерческие программы, часть имеет версии, доступные для бесплатного использования.

Обычно такие программы сочетают в себе возможности блокировки трафика с дополнительными сервисами: например, запрет всплывающих окон, отсечение рекламных баннеров, фильтрация по вызывающему приложению и т. п. Часто программы имеют так называемый режим обучения, позволяющий неопытному пользователю осуществить точную настройку защиты. В этом режиме программа сообщает обо всех попытках передачи информации в Интернет. Анализируя представленную брандмауэром информацию, пользователь принимает решение о полной блокировке передачи, о разовом или постоянном разрешении. Таким образом, можно в результате обучения создать нужную конфигурацию доступа в Интернет.

Продукты, предназначенные для использования на уровне предприятий (Microsoft ISA Server, Check Point, Trend Micro Internet Gateway и т. п.), обычно носят комплексный характер: с их помощью можно создавать правила, фильтровать контент, предотвращать атаки определенного типа и т. д.

Фильтрация пакетов средствами операционной системы

В Windows 200*x*/XP/Vista предусмотрена возможность фильтрации пакетов. Опции фильтрации настраиваются через дополнительные свойства TCP/IP. По умолчанию система пропускает пакеты любых типов; при необходимости ввода ограничений следует указать разрешенные протоколы и допустимые номера портов. Например, с помощью фильтров легко защитить специализированный сервер (почтовый или аналогичный).

Хотя в окне настройки свойств фильтров можно создать необходимые правила, ограничивающие трафик с/на данное устройство, по мнению автора, более удобно настраивать опции фильтрации пакетов протокола TCP/IP с помощью настроек IPSec *(см. главу 12, разд. "Internet Protocol security")*. При помощи настройки фильтров политики IPSec легко создать правила, запрещающие или разрешающие трафик на конкретные узлы сети (рис. 8.6.). При этом политики IPSec могут быть распространены на компьютеры сети с помощью групповой политики. Таким способом штатными средствами можно создать инструмент быстрого повышения уровня безопасности системы: достаточно предварительно разработать групповые политики IPSec, сводящие к минимуму сетевое взаимодействие, и включить их в случае вирусной атаки или признаков вторжения в сеть.

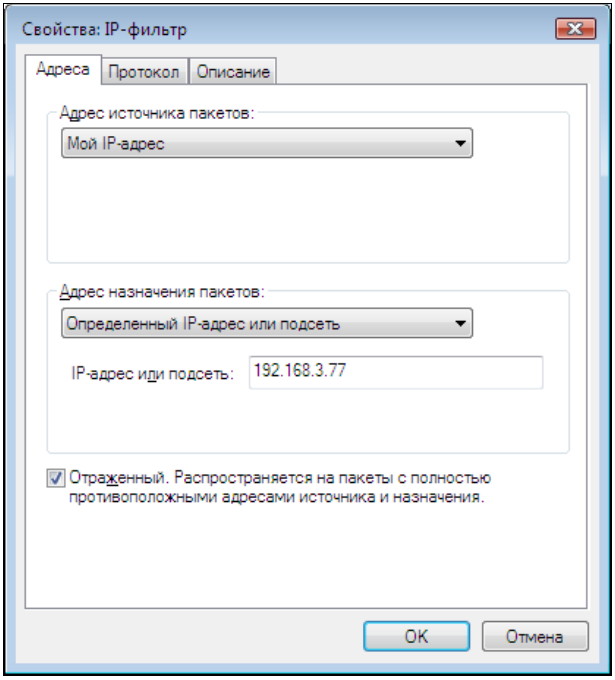


Рис. 8.6. Фильтры IPSec позволяют очень точно настроить разрешения на передачу того или иного трафика системы

Настройка параметров МСЭ при помощи групповой политики

Версии Windows с последними обновлениями безопасности предусматривают включение брандмауэра по умолчанию. При этом используются парамет-

ры, оптимальные для некоторого "среднего" варианта: защита активна, но задействованы исключения, обеспечивающие работу компьютера в локальной сети. Это, с одной стороны, неудобно в локальной сети с развернутыми системами управления: межсетевой экран блокирует доступ таких программ к компьютерам. С другой, — не обеспечивает должного уровня защиты в публичных сетях. Поэтому встроенные брандмауэры Windows нуждаются в централизованной настройке с помощью групповых политик.

Групповые политики межсетевого экрана

Примечание

Практически все настройки брандмауэра в групповой политике относятся к операционным системам Windows XP с установленным вторым пакетом обновления. Данный факт следует учитывать при планировании группового управления межсетевыми экранами в организации.

Параметры настройки групповой политики брандмауэра Windows расположены по следующему пути: **Конфигурация компьютера | Административные шаблоны | Сеть | Сетевые подключения | Брандмауэр Windows** (рис. 8.7). Настройки снабжены подробным пояснением, поэтому обратим внимание только на основные моменты конфигурирования.

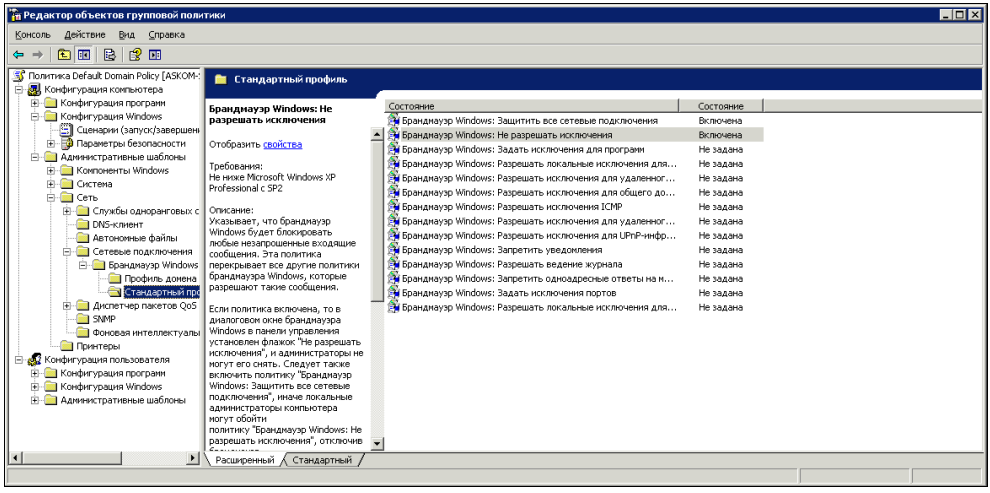


Рис. 8.7. Настройка параметров МСЭ при помощи групповых политик

В политике предусмотрено два контейнера: *профиль домена* и *стандартный профиль*. Параметры профиля домена используются в случае работы компьютера в сети домена (работа в составе домена определяется по параметрам сетевого адреса и доступности контроллера домена). Если компьютер, напри-

мер, ноутбук, включен в другую сеть, то настройки брандмауэра будут выполнены согласно параметрам, содержащимся в контейнере стандартного профиля.

Какие настройки могут быть рекомендованы для применения в обоих случаях? Во-первых, наиболее безопасным вариантом является задействование брандмауэра как в условиях работы в домене, так и в публичной сети. Во-вторых, должна быть определена политика исключений защиты. При работе в домене, естественно, должны быть включены правила, относящиеся к работе в локальной сети. Кроме того, необходимо *создать* исключения и отразить их в групповой политике для тех программ управления, которые эксплуатируются на предприятии. Например, если вы используете корпоративную антивирусную программу, то должны разрешить доступ к компьютерам по тем портам, которые она использует[1]. А если на предприятии внедрена система удаленного мониторинга, то должны быть открыты порты для данной программы или включена опция **Разрешать исключения для удаленного управления** для возможности управления через удаленную консоль. В каждом конкретном случае перечень таких исключений индивидуален, а их количество должно быть минимально разумным.

Для стандартного профиля правилом должен стать *запрет* использования всех исключений брандмауэра, поскольку такой вариант наиболее безопасен для публичной сети.

В табл. 8.1 приведены возможные настройки параметров групповой политики для межсетевого экрана Windows XP SP2.

Таблица 8.1. *Рекомендуемые параметры настройки МСЭ*

Параметр	**Рекомендуется для профиля**	
	домена	**стандартного**
Защитить все сетевые подключения	Включен	Включен
Не разрешать исключения	Не задан	Включен, и настроены исключения для используемых программ
Задать исключения для программ	Включен, и настроены исключения для используемых программ	Включен, и настроены исключения для используемых программ

[1] Например, для антивируса от Symantec используемые порты описаны в документе **http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2005033011582148?OpenDocument&src=ent_hot&dtype=corp&seg=ent&prod=Symantec%20Client%20Firewall&ver=8.0&tpre=**.

Таблица 8.1 *(окончание)*

Параметр	Рекомендуется для профиля	
	домена	**стандартного**
Разрешать локальные исключения для программ	Отключен	Отключен
Разрешать исключения для удаленного управления	Отключен	Отключен
Разрешать исключения для общего доступа к файлам и принтерам	Отключен	Отключен
Разрешать исключения ICMP	Отключен	Отключен
Разрешать исключения для удаленного рабочего стола	Включен	Включен
Разрешать исключения для UPnP-инфраструктуры	Отключен	Отключен
Запретить уведомления	Отключен	Отключен
Разрешать ведение журнала	Не задан	Не задан
Запретить одноадресные ответы на многоадресные или широковещательные запросы	Включен	Включен
Задать исключения портов	Отключен	Отключен
Разрешать локальные исключения для портов	Отключен	Отключен

Совместное использование интернет-подключения

Самый простой способ подключения к Интернету локальной сети организации на основе Windows, который не требует установки и настройки никаких дополнительных программ, — это использование *совместного подключения к сети Интернет*. Такая возможность предусмотрена уже в Windows 2000 Professional (операционной системе для рабочих станций).

Организовать совместное использование подключения к Интернету можно при любом способе связи, будь это подключение через модем или локальную сеть (если провайдером проложен к вам выделенный канал). Соответствующую настройку легко выполнить аналогично описываемому ниже примеру подключения к Интернету с использованием модема.

Если компьютер имеет настроенное подключение к Интернету, то в папке задач **Сетевые подключения** есть значок, соответствующий данному подключению. Щелкните по нему правой кнопкой мыши и выберите команду **Свойства**. На вкладке **Дополнительно** в опции включения совместного использования доступа в Интернет поставьте соответствующий флажок.

Примечание

Если вы не хотите, чтобы соединение с Интернетом автоматически устанавливалось каждый раз, когда кто-либо из локальной сети обращается к Сети (пытается открыть страницу Интернета, принять почту и т. п.), то уберите соответствующий флажок в опциях настройки.

При выборе совместного использования подключения IP-адрес сетевой карты компьютера автоматически изменяется на 192.168.0.1. Компьютер становится для других членов локальной сети сервером DHCP (диапазон 192.168.0.*x*) и сервером DNS, поэтому на остальных компьютерах настройка протокола TCP/IP должна быть выполнена с параметрами по умолчанию, которые предполагают автоматическое получение всех необходимых данных.

Публикация компьютеров в Интернете при совместном использовании подключения

Для публикации внутренних ресурсов в Интернете при совместном использовании подключения достаточно создать соответствующее правило. Покажем на примере, как выполнить публикацию внутреннего FTP-сервера в сети Интернет при совместном использовании подключения.

1. Откройте свойства соединения с Интернетом, для которого организовано совместное использование, перейдите на вкладку **Дополнительно** и нажмите кнопку **Настройки**. Появится окно с перечнем типовых сервисов Интернета, которым разрешен доступ во внутреннюю сеть через данное подключение.
2. Выберите нужный сервис и отметьте флажок, разрешающий его публикацию в Интернете (рис. 8.8). Появится окно, в котором нужно указать компьютер, где в локальной сети работает данный сервис. Обратите внимание, что можно указать как имя, так и IP-адрес компьютера. Если отдается предпочтение IP-адресу, то целесообразно прописать его на соответствующем компьютере статически, чтобы он не изменялся впоследствии, поскольку стандартно при совместном использовании подключения к Интернету адреса компьютерам выдаются динамически и могут изменяться. После завершения операций закройте все окна настройки, нажав кнопку **OK**.

В результате подобных настроек, например, на FTP-запрос, поступающий из внешней сети, будет отвечать не непосредственно подключенный к Интернету компьютер, а указанный вами при описанных выше операциях.

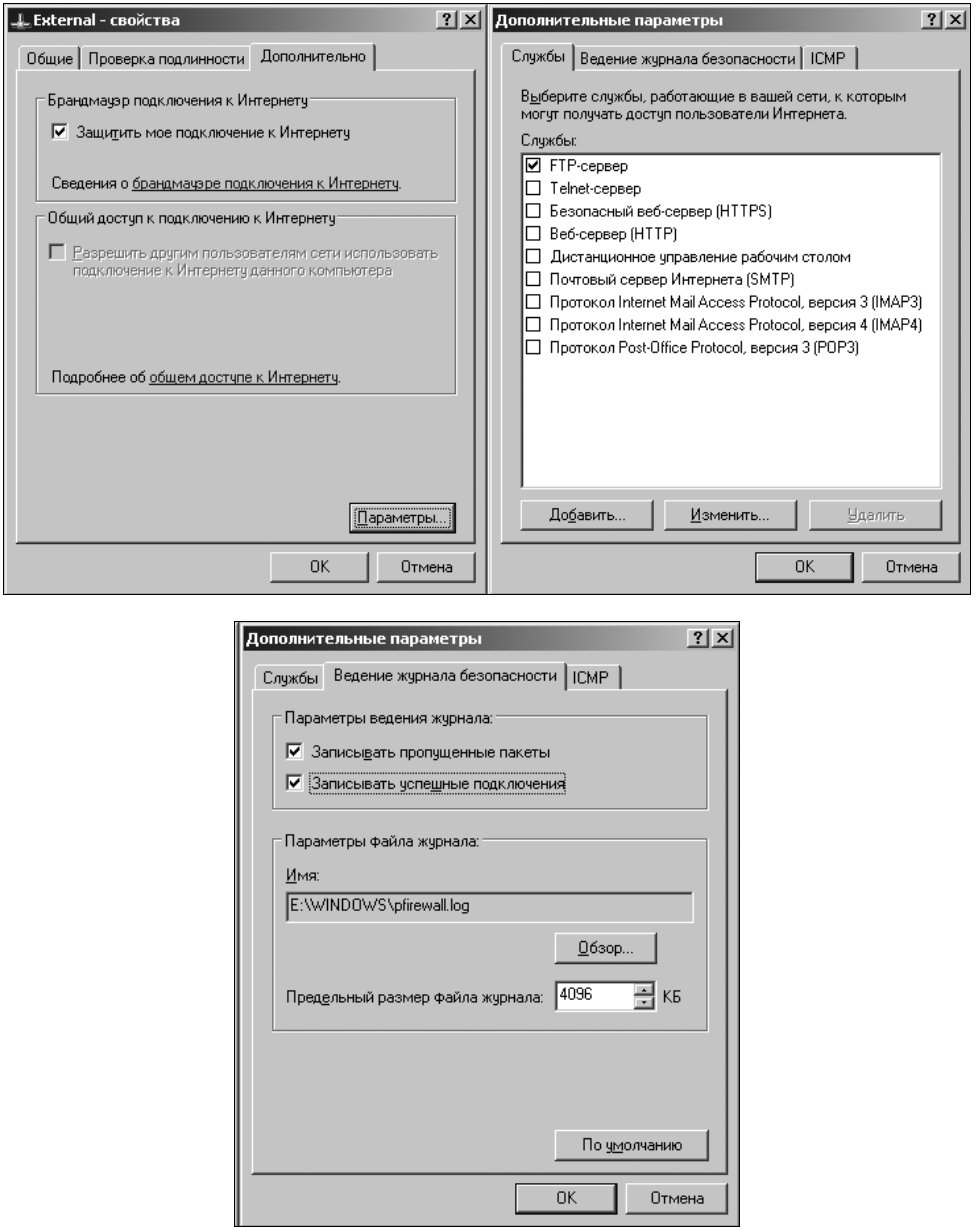


Рис. 8.8. Настройка параметров совместно используемого подключения

Использование соединения может быть протоколировано (записаны пропущенные или отклоненные пакеты, рис. 8.8), однако в связи с большим объемом файла протокола для его анализа необходимо использовать программные продукты других разработчиков.

Таким же способом можно настроить публикацию в Интернете любых сервисов, которые реализуются на локальных компьютерах сети. Если нужного сервиса нет в стандартном списке, вы можете его добавить, воспользовавшись соответствующей опцией. При введении нового сервиса необходимо указать тип используемого протокола и номера портов.

Главная проблема, которая будет подстерегать вас при подобном решении, — это возможное отсутствие статического IP-адреса компьютера, подключенного к Интернету. Иными словами, если вы имеете в локальной сети информационный сервер и используете сеансовое подключение к Интернету, то его реальный адрес подключения будет меняться при каждом сеансе связи с провайдером, что, естественно, не позволит кому-либо обратиться к опубликованным ресурсам.

Ограничения совместного использования подключения к Интернету

Из технических особенностей реализации совместного использования подключения к Интернету вытекают ограничения его применения.

Совместное использование подключения позволяет быстро и с минимальными затратами обеспечить работу компьютеров локальной сети в Интернете через одну точку подключения. Однако такое решение применимо только для домашней сети или сети малого офиса, потому что данный вариант подключения создает неконтролируемый доступ в Интернет для *всех* компьютеров локальной сети. В сети организации необходимо вести контроль доступа к ресурсам Интернета, иметь возможность выборочно предоставлять доступ одним сотрудникам и запрещать другим и т. п., в связи с чем в средних и крупных организациях применяются серверные решения, позволяющие реализовывать принятую политику предоставления доступа в Интернет.

Кроме того, можно использовать в локальной сети только диапазон адресов 192.168.0.0/24, причем адрес 192.168.0.1 может быть только у компьютера, обеспечивающего совместное подключение к Интернету. Данное ограничение также осложняет задачу настройки безопасного соединения между несколькими площадками организации (или настройку VPN-подключения пользователя к ресурсам другой организации в случае совпадающих диапазонов адресов локальных сетей).

Как снизить затраты на доступ в Интернет?

В режиме постоянного подключения к Интернету основная доля оплаты услуг провайдера формируется за счет объема загруженных файлов. В этом случае можно рекомендовать следующие действия для снижения расходов по оплате канала доступа к Интернету.

- **Установка локального прокси-сервера и увеличение объема для кэширования файлов.**

  Существуют различные решения для прокси-серверов: от бесплатных полнофункциональных вариантов на базе Linux-систем до аналогичных коммерческих систем типа MS ISA Server. Объем кэширования данных следует выбирать, основываясь на объеме интернет-трафика организации. Обычно под кэш следует отводить дисковое пространство, примерно соответствующее объему закачиваемой за месяц информации или больше. В зависимости от типа наиболее часто посещаемых ресурсов Интернета, использование прокси-сервера позволяет получать с локального сервера, а не из глобальной Сети до 40—50% трафика.

- **Настройка маршрутизации внешнего трафика в зависимости от тарифов провайдера.**

  Если стоимость трафика через прокси-сервер провайдера выше расценок городского трафика и ниже междугороднего, то вы имеете возможность настроить маршрутизацию так, чтобы городской трафик "шел" напрямик, а междугородный использовал подключение к прокси-серверу провайдера.

Примечание

Объем трафика с местных сайтов, конечно, зависит от города, специфики организации и т. п. В среднем его доля может достигать 10% от общего объема трафика.

- **Отключение рекламных баннеров, запрет порносайтов и т. п.**

  Объем рекламы на большинстве популярных сайтов составляет до 2/3 объема информационной страницы (если учитывать все загружаемые данные). Поэтому отключение рекламы не только резко повысит скорость работы с информацией, но и существенно снизит объемы трафика.

  Функцию блокировки загружаемого содержимого в зависимости от адреса страницы и типа файла имеют многие программы брандмауэров. Например, персональные брандмауэры имеют возможности блокировки графики по размерам, стандартным для баннерных систем, а в случае использования серверных брандмауэров администратор может создать правило, которое запрещает загрузку данных с определенных адресов Интернета. На-

пример, сценарий для брандмауэра Microsoft ISA Server, который позволит выполнить данную операцию автоматически и при этом включит в список несколько сотен порносайтов и сайтов с рекламным содержимым, доступен по ссылке **http://www.isatools.org/ISA_Ads.zip**. На этом же сайте вы можете найти дополнения к данному перечню, например, по ссылке **http://www.isastuff.mine.nu/** содержатся данные по более чем двум тысячам рекламных сайтов и более чем шести тысячам порносайтов.

Исходя из личной практики автора, вместо полной блокировки содержимого таких сайтов следует перенаправить запросы к ним на внутренний сервер, отвечая пустым изображением на прозрачном фоне.

Примечание

Конечно, любой такой список будет неполным. Администратору следует периодически анализировать по файлам протокола список наиболее часто посещаемых сайтов и добавлять новые рекламные ссылки в блокирующий список, причем для блокировки различных динамических реклам следует запрещать получение с данных сайтов не только мультимедийного содержимого, но и всего трафика.

- **Организационные меры.**

  Обычно наиболее эффективны организационные меры снижения трафика Интернета, например, установление лимитов работы с последующей оплатой превышения трафика или отключением мультимедийного содержимого.

С точки зрения автора, наиболее рациональным способом ограничения входящего трафика является отключение отображения графики на страницах. Например, такая возможность очень удобно реализуется в обозревателе Opera: кнопка включения/отключения графики находится на панели программы, а сама операция выполняется за доли секунды, в отличие от MS IE.

Удаленная работа

С повышением мобильности пользователей все чаще возникает необходимость обеспечить удаленный доступ к определенным ресурсам и реализовать полноценную работу в составе корпоративной сети. При этом администратору приходится решить несколько задач:

- обеспечить безопасное подключение к компьютерной сети организации (через публичные сети — Интернет или через модем);
- обеспечить приемлемую производительность для удаленных пользователей при работе по достаточно медленным каналам связи.

Удаленное подключение пользователей

Удаленный пользователь может подключиться к корпоративной сети двумя способами: через модемное подключение к одному из компьютеров сети или общедоступные сети (Интернет). В обоих случаях это решение реализуется через настройку *сервера удаленного доступа и маршрутизации* (RRAS). При модемном подключении пользователь создает физический канал связи с RRAS, при работе из Интернета реализуется *логическое* подключение к RRAS через VPN.

Прием входящих подключений

Обеспечить подключение внешнего пользователя к системе можно как для рабочей станции, так и для сервера. Обычно практическое значение имеют два варианта: подключение через сеть Интернет и подключение через модем на данном компьютере.

Настройка рабочей станции

На прием входящих модемных соединений можно настроить даже рабочие станции Windows 2000/XP/Vista. Например, если вы хотите скопировать файлы с компьютера своего приятеля или поиграть с ним в сетевую игру, то совсем не обязательно создавать такое подключение через провайдера Интернета: достаточно один компьютер настроить для приема входящих соединений, а на другом использовать обычный вариант подключения к внешней сети.

Для создания входящего соединения следует запустить мастер создания новых подключений и выбрать опцию **Установить прямое подключение к другому компьютеру**. На следующем шаге необходимо включить опцию **Принимать входящие соединения** и отметить устройство, через которое будет осуществляться подключение. На завершающем этапе следует установить разрешения для тех пользователей, которые будут подключаться к данной системе.

Настройка сервера

При наличии подключенного модема после активизации сервера RRAS никаких дополнительных настроек администратора не требуется. Необходимые порты подключения модема создаются автоматически. Возможность доступа пользователей во внутреннюю сеть при таком подключении определяются политиками сервера RRAS (или службы RADIUS) — *см. разд. "Политики подключений" далее в этой главе*.

VPN

VPN (Virtual Private Network) представляет собой способ расширения локальной компьютерной сети за счет включения в нее удаленных компьютеров через общедоступные сети. При подключении по VPN удаленный компьютер становится как бы участником локальной сети. Данные, которые должны быть переданы по VPN через открытые каналы связи, предварительно шифруются, "вкладываются" (инкапсулируются) в обычные пакеты и пересылаются серверу корпоративной сети. Все эти процессы происходят незаметно для пользователя. Внешнее впечатление такое, что создан специальный канал связи с корпоративной сетью и компьютер напрямик подключен к локальной сети.

Такой канал связи, предусматривающий инкапсулирование данных и их шифрование в процессе передачи, называется *VPN-соединением*. При работе по VPN на компьютере создается новое подключение к сети со своими параметрами настройки IP-протокола: IP-адрес из состава корпоративной (локальной) сети, данные внутренних DNS-, WINS-серверов и т. п. В качестве шлюза по умолчанию для компьютера при этом указывается шлюз удаленной локальной сети.

Примечание

В случае необходимости одновременного использования нескольких VPN-подключений целесообразно отключить вариант использования шлюза по умолчанию, определенного в подключаемой сети. Таблицу маршрутизации в этом случае следует сформировать вручную, особенно если подключаемая сеть состоит из нескольких сегментов.

На практике используются различные варианты организации VPN-каналов. Вы можете просто купить "готовый канал VPN" (такие услуги предлагаются провайдерами, но они весьма до́роги) или использовать встроенные опции маршрутизаторов (при наличии соответствующих моделей). Однако наиболее простым и дешевым вариантом является создание программных VPN-подключений на базе операционных систем Linux или Windows.

Примечание

VPN-канал можно применять в рамках одной локальной сети при подключении отделов, работающих с особо конфиденциальной информацией. Так, можно связать, например, отдел кадров и бухгалтерию для передачи данных о доходах сотрудников.

Настройки входящих VPN-подключений для Windows

Входящее VPN-подключение можно создать как для рабочей станции Windows, так и для серверной операционной системы. Следует отметить, что на

рабочей станции одновременно может быть задействовано *только одно подключение*.

Настройка VPN-подключения на базе операционной системы рабочей станции

В качестве примера рассмотрим процесс настройки операционной системы Windows XP/Vista[1] для организации возможности приема удаленных VPN-подключений. Можно выполнить одно подключение по любому из следующих интерфейсов: модемное соединение (рис. 8.9), инфракрасный порт, параллельный порт.

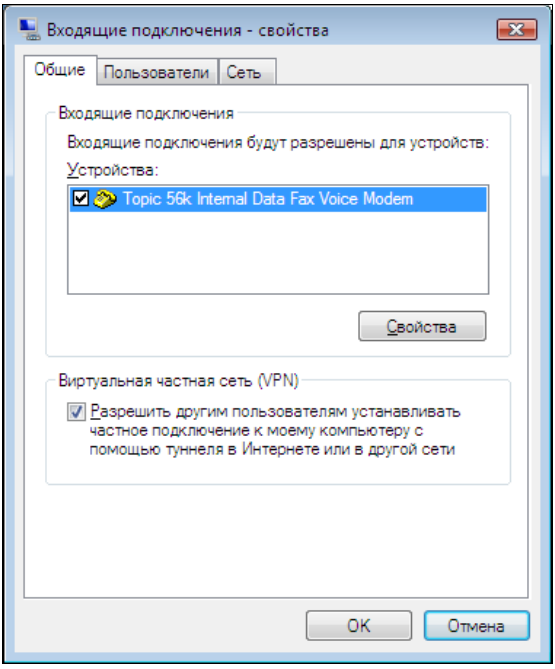


Рис. 8.9. Настройка параметров входящего подключения в Windows Vista

Создание VPN-подключения выполняется при помощи мастера новых подключений в следующей последовательности:

1. В мастере создания новых подключений выберите вариант **Установить прямое подключение к другому компьютеру**.

[1] В Windows Vista возможность создания входящего подключения несколько скрыта. Чтобы выполнить операцию, необходимо открыть задачу **Управление сетевыми подключениями** и отобразить меню, нажав клавишу <Alt>. После этого в меню **Файл** станет доступна команда *Новое входящее подключение*.

2. Отметьте, что соединение должно обрабатывать входящие соединения (опция **Принимать входящие подключения**).
3. На вкладке о VPN-подключениях укажите, что вы хотите разрешить VPN-подключение, и выберите пользователей, которым будет разрешено использовать данное подключение.
4. На вкладке программного обеспечения в меню определения свойств IP-протокола настройте опции подключения удаленных пользователей к локальной сети: либо только к данному компьютеру (снят флажок **Разрешить звонящим доступ к локальной сети**), либо ко всем компьютерам локальной сети (флажок установлен). Также нужно определить параметры TCP/IP-протокола[1], которые будут использованы внешним клиентом.

Настройка VPN-подключений на базе серверной операционной системы

VPN-доступ в серверных операционных системах реализуется через службу RRAS. Администратору необходимо добавить столько портов для VPN-подключений, сколько потребуется в работе организации. Эта операция выполняется либо с помощью мастера настройки RRAS, либо вручную — простым добавлением нужного числа портов.

Примечание

Обратите внимание, что удаленное подключение разрешено только тем пользователям, которым политикой сервера маршрутизации и удаленного доступа разрешены *входящие звонки (см. разд. "Политики подключений" далее в этой главе)*.

VPN-подключения и брандмауэры

На практике могут быть реализованы различные варианты расположения VPN-сервера и брандмауэра организации. Можно расположить VPN-сервер за брандмауэром, внутри локальной сети, тогда брандмауэр будет перенаправлять весь VPN-поток на локальную систему. Это является безопасным решением, поскольку на сервере VPN производится аутентификация пользователя и несанкционированные данные просто отбрасываются. Такая конфигурация наиболее распространена и, например, реализуется мастером создания VPN-подключений для ISA-сервера.

Если расположить VPN-сервер *перед* брандмауэром, то необходимо выполнить настройку брандмауэра, разрешающую пересылку пакетов с VPN-сервера вовнутрь локальной сети.

---

[1] Адрес, получаемый VPN-клиентом, должен входить в подмножество адресов внутренней сети; как правило, на компьютерах сети в качестве шлюза используется адрес сетевой карты внутреннего интерфейса VPN-сервера.

Фильтрация трафика VPN

В системах Windows VPN-канал создается службой маршрутизации и удаленного доступа. Поскольку RRAS проводит аутентификацию пользователя, то весь VPN-трафик безопасно может быть перенаправлен на такой сервер. Для обеспечения безопасности сервера (предотвращения атак на другие службы) в этом случае достаточно установить фильтры, которые пропускают к нему *только* трафик VPN и отсекают иные пакеты.

Подобную настройку легко выполнить штатными средствами, не устанавливая дополнительно программы брандмауэра. Следует настроить следующие фильтры на интернет-интерфейсе сервера:

- для подключения по PPTP:
  - по умолчанию игнорировать все пакеты, кроме явно разрешенных[1];
  - разрешить IP-протокол на порт 1723 (разрешает передачу управляющего трафика PPTP);
  - разрешить IP-протокол с идентификатором 47 (разрешает передачу данных по PPTP);
  - разрешить IP-протокол на порт 1723 в варианте **TCP [established]** (настройка нужна, если инициатором соединения выступает сам VPN-сервер);
- для подключения по L2TP:
  - по умолчанию игнорировать все пакеты, кроме явно разрешенных;
  - разрешить пакеты на UDP-порт номер 500;
  - разрешить прохождение протокола с идентификатором 50;
  - разрешить пакеты на UDP-порт номер 1701.

Не забывайте, что для обоих фильтров необходимо разрешить прохождение как *входных* пакетов, так и соответствующих симметричных *выходных*.

Настройка создания VPN в случае использования Microsoft Internet Security Acceleration Server в качестве брандмауэра организации осуществляется с помощью мастера операций. Реально этот мастер выполняет две операции: активизирует RRAS и добавляет VPN-порты, а также создает фильтры, разрешающие прохождение PPTP- и L2TP-пакетов на интерфейс RRAS.

Настройки клиентов для подключения по VPN

Настроить VPN-подключение к сети предприятия можно в любых операционных системах клиента. Но, например, каждая версия Windows имеет неко-

[1] Drop all packets except those that meet the criteria below.

торые отличия по созданию VPN-канала. Так, в Windows 95/98 первоначально необходимо программно добавить в систему такое устройство, как *VPN-адаптер*[1]. Поэтому конкретные особенности реализации такого подключения следует уточнить по справочной документации. В последних версиях (Windows XP, Windows 2000) данная операция выполняется с помощью мастера подключений.

Чтобы создать VPN-подключение к удаленной сети организации, достаточно (для систем Windows 2000/XP/Vista) вызвать задачу создания нового подключения и в мастере установок отметить вариант подключения к корпоративной сети, после чего просто ответить на запросы мастера.

Примечание

Если параллельно с работой в корпоративной сети необходимо организовать использование Интернета (или доступ в иные сети) *не* через сеть организации, то в дополнительных настройках параметров подключения по VPN следует *отключить* применение *шлюза по умолчанию* из сети организации.

Действующий канал VPN будет отображаться пиктограммой еще одного сетевого соединения.

Политики подключений

Администраторы имеют возможность регулировать параметры доступа удаленных клиентов в локальную сеть.

Примечание

Описываемые политики доступа определяют одновременно как возможность подключения по модему, так и создание VPN-подключения.

При использовании RRAS настройки доступа выполняются путем задания расписания входящих соединений (когда можно и когда нельзя устанавливать подключение) и путем *политики подключений*. На каждом сервере RRAS применяются свои политики доступа. При этом в домене не существует возможности централизации этих настроек[2]. То есть если в организации имеется несколько точек доступа, то настраивать каждую из них следует индивидуально.

---

[1] Установка Microsoft VPN-адаптера выполняется через задачу установки/удаления программ на вкладке компонентов Windows (сетевые компоненты). Следующим шагом в настройке VPN будет создание нового dial-up-подключения, в котором вместо модема следует указать адаптер, установленный на предыдущей операции.

[2] Точнее, администратор не может централизованно управлять политиками доступа RRAS. Но он может создать на каждом сервере RRAS одинаковые политики, определяющие права доступа к локальной сети в зависимости от членства в доменных группах, после чего централизованно настраивать доступ путем изменения состава этих групп.

Возможный выход — это установка службы IAS (Internet Authentication Service)[1]. После установки IAS достаточно в настройках каждого сервера RRAS указать использование этой службы[2]. Таким образом, *все серверы* удаленного доступа при попытках подключения пользователей будут обращаться к одному серверу IAS, а настраивать одну политику доступа гораздо удобнее, чем постоянно заботиться об идентичности параметров различных серверов.

Варианты аутентификации пользователей

Существуют различные варианты проверки данных пользователей, пытающихся осуществить подключение к локальной сети. По умолчанию используются безопасные методы, предполагающие как шифрование пароля пользователя, так и шифрование передаваемых данных. Вряд ли администратору придется разрешать менее безопасные варианты, предусмотренные в целях совместимости с предыдущими версиями клиентов.

Самым безопасным способом аутентификации пользователя является использование *смарт-карт* (или их аналогов). Если имеется техническая возможность, следует использовать только этот вариант подключения, для чего в политике RRAS (или IAS) указать среди вариантов аутентификации пользователей *только протокол расширенной проверки подлинности* (*Extensible Authentication Protocol, EAP*).

Разрешения на подключения

По умолчанию политика RRAS не разрешает подключения к сети предприятия ни одному пользователю. В этом случае используются права доступа, прописанные в настройках каждого пользователя, а по умолчанию пользователи создаются *без наличия права* создания подключения.

Если администратор сохраняет политику подключения по умолчанию, то он должен *индивидуально* выдать разрешения пользователям на подключение к локальной сети. Для этого необходимо установить параметр разрешения доступа на вкладке настройки входных звонков профиля пользователя.

Другой способ разрешения состоит в создании собственных политик доступа, в которых право подключения предоставляется либо определенным пользователям, либо их группам. Создание и редактирование новой политики подключения не представляет никакой сложности и легко может быть выполнено любым специалистом.

---

[1] IAS — это реализация сервера RADIUS (Remote Authentication Dial-In User Service) на платформе Microsoft. RADIUS традиционно используется многими интернет-провайдерами для аутентификации подключаемых к сети пользователей.

[2] В целях резервирования обычно настраиваются основной и резервный серверы IAS.

Настройка безопасного подключения одного филиала к другому

Многие организации имеют несколько территориально разделенных площадок, которые должны работать в составе единой компьютерной сети. Безопасное соединение таких локальных сетей можно выполнить с помощью VPN-канала, создание которого в этом случае имеет некоторые особенности.

Во-первых, такое подключение должно устанавливаться автоматически и автоматически же восстанавливаться в случае разрыва. Во-вторых, через такое соединение должны передаваться пакеты не только на компьютер, осуществивший подключение, но и для всей удаленной сети. Подобный вариант подключения носит название *интерфейса по требованию* (dial-in-интерфейса).

Создание интерфейса по требованию осуществляется мастером. Достаточно выбрать в меню RRAS опцию создания нового интерфейса по требованию, дать ему имя, указать параметры учетной записи, с помощью которых будет осуществляться подключение к другому серверу, и ввести параметры удаленной сети для создания статической маршрутизации.

Система отличает подключение удаленного пользователя от подключения интерфейса по требованию *только по имени пользователя,* выполняющего эту попытку. Поэтому при настройке подключений двух сетей *имя* подключающегося *пользователя должно совпадать с названием интерфейса*. То есть на сервере с интерфейсом по требованию с именем `Int1` должен быть указан пользователь `Int2` для подключения к удаленному интерфейсу по требованию с именем `Int2`. А на другом сервере — `Int1`.

В Windows 2000 после создания интерфейса по требованию необходимо вручную задать в RRAS статические маршруты, которые будут включаться при подсоединении этого интерфейса[1]. Для этого выделите заголовок **Static Route**, вызовите команду создания статических маршрутов, выберите интерфейс по требованию и введите параметры удаленной сети. Эту операцию следует выполнить с обеих сторон канала связи офисов.

Другие настройки подключений интерфейсов по требованию (должно ли соединение инициироваться сервером или ему следует только ожидать попытки подключения, время "простоя", после которого можно разъединять связь, или необходимость постоянного соединения и т. п.) достаточно очевидны и легко настраиваются через консоль управления сервером RRAS.

Примечание

На рынке представлено много оборудования, специализированного на создании и поддержании VPN как подключений для удаленных пользователей, так и

[1] В Windows 2003 Server параметры статической маршрутизации интерфейса по требованию вводятся в процессе работы мастера создания интерфейса.

соединений филиалов между собой. Аппаратное решение более производительно и требует меньше внимания от администратора. Стоимость использования VPN Router обычно соответствует цене операционной системы вместе с программой межсетевого экрана (в случае официального приобретения). Учитывая стабильную работу канала, создаваемого таким оборудованием, данные варианты VPN-подключений можно рекомендовать для организации безопасных связей между центральным и удаленными офисами.

В случае разрыва канала...

Удаленные офисы небольших предприятий обычно укомплектованы всего лишь несколькими компьютерами. В этом случае размещение в удаленном офисе контроллера домена не оправдано как экономически, так и по соображениям безопасности (поскольку в филиале обычно невозможно установить особый порядок доступа к серверу).

При этом перед администраторами стоит задача обеспечить совместную работу филиала с центральным офисом. Достаточно часто качество канала связи с центральным офисом (Интернетом) оставляет желать лучшего; в результате при обрыве связи удаленные пользователи теряют возможность доступа к ресурсам не только головного офиса, но и к локальным (документы, хранимые в папках совместного доступа на компьютерах других сотрудников филиала, локальный принтер и т. п.), если для доступа к ресурсам применяются *доменные учетные записи*.

Существуют два возможных пути решения данной проблемы. Первый — это создание на удаленных компьютерах локальных учетных записей, совпадающих по имени с доменными и имеющими тот же пароль, что в домене. В этом случае при обрыве связи и недоступности контроллера домена доступ к ресурсам на других компьютерах будет осуществляться по *локальным учетным записям*. Недостаток этого варианта состоит в том, что необходимо постоянно синхронизовать учетные записи домена и локальных компьютеров в случае смены паролей пользователей.

Второй путь — размещение таких ресурсов филиала (общие папки, принтер) на *терминальном сервере*. Поскольку в новых версиях Windows существует кэширование параметров последних входов пользователя, то при обрыве связи пользователь сможет войти на терминальный сервер *без наличия подключения к контроллеру домена*, используя параметры последнего входа, хранимые в кэше. Однако подключиться к совместно используемым папкам на других компьютерах будет невозможно.

Карантин RRAS

Если компьютеры локальной сети находятся "под присмотром" администратора, то о состоянии систем, подключаемых средствами удаленного доступа, можно только предполагать. В результате, например, спамеры начинают ак-

тивно использовать такие компьютеры: на них существенно проще установить программу-троян и заставить почтовую систему организации пересылать спам. Поскольку удаленный пользователь успешно регистрируется в системе, то почтовый сервер будет принимать от него для рассылки любую корреспонденцию. Поэтому естественно желание администраторов каким-то образом проконтролировать удаленную систему перед подключением.

В RRAS Windows 2003 добавлена возможность такой проверки. Происходит это следующим образом: при подключении удаленного клиента сервер проверяет политику доступа, и если установлены требования проверки клиента, то подключает систему и временно помещает ее *в карантин*. На клиенте в это время запускается программа, проверяющая выполнение определенных администратором условий. Результат проверки сообщается серверу удаленного доступа, который принимает решение отключить клиента или предоставить ему полный доступ в сеть.

Для выполнения таких действий необходимо установить службу карантина, которая входит в состав пакета Resource Kit Tools для Windows Server 2003 (бесплатно загружается с сервера Microsoft). Установка производится запуском файла rqs_setup.bat, который создает на компьютере службу **Remote Access Quarantine Service**. После установки службы необходимо добавить в реестр параметр **AllowedSet** (тип `REG_MULTI_SZ`) со значением в виде версий сценариев, которые будут запускаться на клиентах.

Далее следует создать сценарий *(профиль)* удаленного входа клиента. Удобно использовать компонент Connection Manager Administration Kit (CMAK), входящий в состав сервера (установка через компоненты Windows в составе Management and Monitoring Tools). После запуска CMAK следует выбрать опцию создания нового профиля, дать ему имя[1] и создать **New Custom Action**. Именно эта настройка будет описывать параметры карантина.

В окне настройки **New Custom Action** следует указать программу (сценарий), который будет запускаться на клиенте. Эта программа может использовать ряд переменных, которые будут ей переданы системой[2]. Минимально в строке **Parameters** нужно указать:

- %DialRasEntry% (имя удаленного подключения/службы);
- %TunnelRasEntry% (имя туннельного подключения);
- %Domain% (название домена, к которому осуществляется подключение);
- %UserName% (имя пользователя);
- %ServiceDir% (путь к папке профиля).

---

[1] Имя следует давать по требованиям названий файлов 8.3, поскольку это название станет именем исполняемого файла на клиенте (к нему автоматически будет добавлено расширение exe).

[2] Полный список доступен в онлайновой справке CMAK.

Параметр **Action Type** следует установить в значение **Post-connect**, а **Run this custom action for:** — в значение **All connections**. Далее проверить, что установлены (отмечены флажками) параметры **Include the custom action program with this service profile** и **Program interacts with the user**, и сохранить изменения. Затем на вкладке **Additional Files** следует указать те файлы, которые необходимо иметь пользователю. Это, во-первых, программа карантина для клиента (rqc.exe), во-вторых — та программа (сценарий), которая будет запускаться на стороне пользователя.

После завершения работы мастер настроит профиль CMAK. Полученные в результате файлы будут сохранены в папке %SYSTEMDRIVE%\Program Files\CMAK\Profiles\<*имя профиля, данное при его создании*>. Файл с именем, указанным вами при настройке CMAK, и с расширением exe необходимо передать пользователям, которые должны будут запустить его у себя для создания профиля подключения.

После настройки параметров подключения для клиента администратору системы необходимо создать политику удаленного доступа, которая определит параметры карантина, а именно: назначить время карантина (период ожидания сервером ответа от клиента перед его отключением) и IP-фильтры, которые должны ограничить доступ клиента к ресурсам сети во время карантина.

Настройка времени ожидания производится в меню редактирования профиля политики в разделе **Advanced**. В этом окне следует добавить атрибут с вендором Microsoft и названием **MS-Quarantine-Session-Timeout**. Значение этого параметра следует установить равным максимально допустимому периоду ожидания в секундах.

Второй возможный атрибут — это **MS-Quarantine-IPFilter**. После его добавления в свойствах следует выбрать те фильтры, которые должны быть активизированы на время карантина. Минимально необходимо разрешить входящий и исходящий трафик по порту 7252 (TCP). Этот порт по умолчанию используют программы карантина rqc/rqs. Необходимость открытия других портов определяется администратором (например, если нужно разрешить в это время использование DNS, то следует разрешить UDP 53 и т. п.).

Примечание

Network Access Quarantine Control (NAQC) может использоваться при подключении операционных систем Windows 98 SE/ME/2000/XP/Server 2003.

Терминальный доступ

При удаленном подключении к офису пользователи хотят воспользоваться всеми сервисами, которые реализованы в локальной сети. Однако недостаточное качество каналов связи зачастую не позволяет эффективно работать

во многих приложениях. Одним из вариантов решения данной проблемы является использование *терминальных служб*.

Принцип действия терминальных служб состоит в том, что все вычисления производятся на мощном удаленном компьютере (его называют *терминальным сервером*), а пользовательский компьютер является "удаленной консолью". Данные и команды, которые пользователь вводит (с клавиатуры, мышью), передаются на терминальный сервер, где они обрабатываются, а пользователю возвращаются лишь графические изменения в интерфейсе. Иными словами, пользовательский компьютер практически использует только монитор, клавиатуру, мышь.

В результате при работе в типовой офисной программе терминальный клиент в среднем передает по сети около 500 байт данных в секунду, что позволяет полноценно работать с удаленным компьютером, используя модемные соединения или медленные каналы связи.

Терминальные серверы от Microsoft

В 1995 г. компания Citrix выпустила продукт под названием Winframe, который стал первым терминальным сервером на базе Windows NT. После договора между Microsoft и Citrix о кросс-лицензировании в 1998 г. вышли версии Windows NT Server Terminal Server Edition и Citrix MetaFrame (продукт Citrix расширял возможности терминального сервера Windows NT TSE). В "поколении W2K" терминальные службы включены в поставку всей линейки серверов Windows 200*x* Server.

Терминальные клиенты

В качестве клиентов терминала могут служить практически любые компьютеры, в том числе и классов 386/486/Pentium, причем сами терминалы *не нуждаются в модернизации*. Поскольку все вычисления производятся на сервере, то при необходимости нужно наращивать или обновлять *только* его мощности.

Одновременно использование терминалов снижает административные затраты на сопровождение. У пользователя становится меньше возможностей повлиять на стабильность работы системы, а администраторы начинают управлять "всем в одном месте". Терминальные системы более безопасны, поскольку устранение уязвимости на сервере ведет к аналогичному результату для всех его клиентов, и практически не оставляют никаких "вольностей" пользователю — ведь контролю администратора поддается практически все.

Кроме того, стоимость терминальных устройств существенно ниже полнофункциональных компьютеров. Терминалы могут быть выполнены на бездисковой основе (Linux-терминалы, которые можно загрузить по сети с сер-

вера), так и на основе загрузки с тех или иных аналогов жесткого диска (например, DiskOnModule и т. п. — объем ядра Linux вместе с программой подключения к RDP-серверу[1] составляет менее 8 Мбайт).

Режимы терминальных служб

Для версий Windows 2000 и Windows Server 2003 используется различная терминология для обозначения терминальных служб.

В Windows 2000 Server существуют два варианта установки терминальных служб: *административный режим* (Remote Administration) и *режим приложений*.

Примечание

Добавление терминальных служб производится через задачу **Установка и удаление программ | Сетевые компоненты**.

Административный режим используется *только* для удаленного управления сервером, потребляет крайне мало ресурсов компьютера, но не предназначен для одновременной работы многих пользователей с установленными на компьютере приложениями. В административном режиме одновременно к серверу могут подключиться не более двух человек, причем обладающих административными правами на данном сервере. Для административного режима не требуется наличия клиентских лицензий.

Режим приложений позволяет организовать одновременную работу *многих пользователей*. Он требует приобретения клиентских лицензий для обеспечения доступа к серверу. Обратите внимание, что прикладное программное обеспечение следует устанавливать *после* включения терминальных служб. В противном случае может возникнуть необходимость переустановки программ.

В Windows 2003 Server терминальными службами называются *только* терминальные службы режима приложений по терминологии Windows 2000. Административный режим стал называться *подключением к удаленному рабочему столу*.

Лицензирование терминальных служб

Для удаленного администрирования серверов (подключения к удаленному рабочему столу в новой терминологии) не требуется никаких лицензий. В то

[1] Тонкие клиенты на базе Linux обычно содержат в себе возможности подключения к различным терминальным службам (по протоколам Citrix ICA, RDP, Tarantella, X, telnet, tn5250 и т. д.). Пользователи могут бесплатно загрузить как исходные коды, так и готовые образы программ для любого варианта загрузки — с диска или дискеты, CD, по сети и т. п. (см., например, **http://thinstation.sourceforge.net/**).

же время для использования *терминальных служб* необходимы специальные лицензии, которые приобретаются отдельно от сервера. Существуют различные схемы лицензирования, на которых мы не будем останавливаться. Лицензии достаточно дороги для того, чтобы обеспечить благожелательное отношение к вам продавца при обращении за консультациями.

Примечание

Одна неприятная особенность перехода с Windows 2000 на Windows 2003 Server состоит в том, что сервер лицензий от Windows 2000 не может "раздавать" лицензии для подключения к терминальной сессии новой версии операционной системы.

"Технически" необходимость выдачи лицензий предполагает установку в локальной сети (и активацию) специального *сервера лицензий*. При работе в составе домена Windows сервер лицензий необходимо устанавливать на контроллере домена. Если использовать вариант установки **Enterprise**, то сервер терминальных лицензий будет обнаруживаться клиентами автоматически (используя службу каталогов) в любом домене леса, но только в пределах данного сайта.

Установка сервера лицензий производится через задачу **Установка и удаление программ** выбором соответствующей позиции. Сервер лицензий обязательно должен быть активирован через сайт изготовителя. Также активируются[1] клиентские лицензии. Без активации лицензий сервер создает временные лицензии, которые можно использовать в течение 90 дней. Но и постоянные лицензии также не выдаются клиентам на неограниченный срок: они периодически обновляются[2], чтобы восстановить лицензии, "отданные" компьютерам, которые уже больше не работают в сети (например, вышли из строя).

Примечание

После установки лицензий имеет смысл выполнить резервное копирование сервера, чтобы можно было восстановить лицензии. У автора был печальный опыт выхода из строя сервера с последующим обращением к представителям изготовителя по поводу восстановления лицензий. Увы, просьбы пользователей, видимо, игнорируются соответствующими службами поддержки.

Еще одно "приятное" нововведение при переходе к Windows 2003 Server — это необходимость приобретения клиентских лицензий для *всех* типов опера-

[1] В случае необходимости администраторы легко найдут в Сети любые рекомендации по выполнению данной операции.

[2] Эта возможность присутствует, начиная с Windows 2000 SP3.

ционных систем. Хотя при работе с терминальными службами Windows 2000 Server клиенты с операционными системами Windows 2000 или Windows XP Professional не требовали приобретения лицензий, то для работы с терминальным сервером Windows 2003 Server лицензия необходима для любых клиентов.

Особенности установки ПО при работе в режиме приложений

Режим терминального сервера не предназначен для использования программ, вызывающих интенсивную нагрузку на процессор. Не рекомендуется использовать этот режим для мультимедийных и аналогичных приложений. Такие задачи целесообразнее решать на локальных системах. Терминальный сервер предназначен прежде всего для "обычных" офисных программ.

Установка прикладных программ в режиме приложений должна использовать специальные условия. Эти условия реализуются автоматически при запуске установки через утилиту установки и удаления программ, расположенную в Панели управления. В режим установки можно также перейти, если набрать в командной строке `change user /install`. По завершении установки следует восстановить нормальный режим командной строки `change user /execute`.

После установки приложения имеет смысл проанализировать дополнения, внесенные им в раздел `Run` реестра. Например, многие программы, инсталлируемые на терминал, выводят в системной области панели задач некие индикаторы. Так, антивирусная программа показывает наличие и состояние защиты на компьютере. В большинстве случаев такие индикаторы только отнимают лишние ресурсы системы и могут быть отключены в целях повышения производительности.

Некоторым программам могут понадобиться специальные конфигурации установки для режима терминальных служб[1]. Например, пакет MS Office XP невозможно установить без специального файла настроек, который следует загрузить с информационного сервера Microsoft.

Для корректной работы приложений в режиме терминального сервера должен выполняться ряд условий, прежде всего, отсутствие записи данных в каталоги самой программы или в четко прописанные папки жесткого диска. Понятно, что на практике можно встретить программу, которая будет некорректно работать в режиме терминала. Исправить подобную ситуацию призваны специальные сценарии, исполняемые при входе пользователя в систему.

---

[1] Разработчики не гарантируют работоспособности всех прикладных программ на терминальном сервере в режиме приложений. Но за все время работы с терминальным сервером автору не приходилось встречаться с ситуацией, когда прикладная программа не работала в этих условиях.

По умолчанию при каждом входе в терминальную сессию исполняется сценарий USRLOGON.CMD[1], вызывающий, в свою очередь, несколько других командных файлов. Если администратор не настраивал сценарии совместимости, то запуск этого сценария с настройками по умолчанию не производит каких-либо операций. Чтобы добавить настройки для некоторых программ (в Windows 2003 Server присутствуют настройки для программ Eudora 4, Visual Studio 6 и Outlook 98[2]; которые хранятся в папке Windows\Application Compatibility Scripts), следует запустить соответствующий файл из папки Install, для удаления[3] — из папки Uninstall. В папке Logon находятся те сценарии, выполнение которых добавляется после включения совместимости.

Примечание

Сценарии совместимости достаточно сложны, а администратору редко приходится создавать собственные варианты. Поэтому для подробного разбора этих сценариев мы просто отошлем читателя на сайт изготовителя.

Установка ПО на клиентских компьютерах

Необходимое программное обеспечение для работы с терминальным сервером входит в состав Windows XP/Vista и Windows 2003 Server. Это программа Подключение к удаленному рабочему столу (вызов из меню **Пуск | Стандартные | Связь**). Для других операционных систем программу подключения к серверу терминалов нужно установить отдельно. Целесообразно воспользоваться последней версией из состава Windows Vista (доступна к свободной загрузке с сайта Microsoft), хотя можно работать и с версиями ПО от Windows 2000/2003 Server. Сами установочные файлы находятся в папке %systemroot%\system32\clients\tsclient. В случае необходимости сервер позволяет сформировать установочные дискеты с помощью программы, которая находится в группе **Административные задачи**.

Примечание

Если на терминальном сервере установлено специальное расширение терминальных сервисов (соответствующая программа доступна для загрузки из Интернета бесплатно), то осуществить подключение к такому серверу можно с использованием обычной программы просмотра Интернета. Для этого достаточно ввести в строке адреса следующий URL: **http://адрес_сервера/tsweb** и согласиться на установку соответствующего органа управления ActiveX.

---

[1] Администратор может добавить свои файлы сценариев, выполняемых при входе в систему, откорректировав значение параметра `AppSetup` ключа `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon`.

[2] Сценарии для некоторых программ можно взять также из поставки Windows 2000.

[3] Сценарии входа замедляют процесс начала работы пользователя в терминале. Поэтому при отсутствии необходимости дальнейшего использования программы желательно деинсталлировать сценарий совместимости.

Разрешения на подключения к терминалу

В Windows 2003 Server по умолчанию подключение к терминалу разрешено только администраторам и членам группы **Пользователи удаленного рабочего стола**. Поскольку эта группа первоначально пуста, то в нее нужно добавить соответствующих пользователей.

Второе место, где контролируется право работы в терминале, — это параметр учетной записи пользователя, разрешающий такое подключение. По умолчанию это право *включено* для каждой учетной записи. Но администраторы могут задействовать этот параметр для индивидуальных запретов или разрешений.

Для подключения к удаленному рабочему столу в целях управления сервером (режим удаленного администрирования), строго говоря, не обязательно быть администратором данного компьютера. Достаточно состоять в локальной группе **Пользователи удаленного рабочего стола**. Однако следует учесть, что в этом случае могут возникнуть проблемы с запуском программ, настройкой приложений и т. п., поскольку вошедший в систему пользователь не будет обладать полным комплектом необходимых прав.

Работа в режиме терминального доступа

Работа в режиме терминального доступа внешне ничем не отличается от работы пользователя, сидящего за экраном и клавиатурой удаленного сервера, особенно если при подключении использован вариант вывода на полный экран.

При подключении клиента к терминальному серверу на последний автоматически устанавливаются принтеры клиента. Это позволяет вывести печать результатов работы, выполняемой на удаленном компьютере, на локальный принтер клиента. Иными словами, пользователь, реально выполняя работу на компьютере в офисе, имеет возможность выполнить печать результатов на принтере, находящемся у него дома.

Кроме того, возможно копировать текст и графику между приложениями, запущенными в терминальной сессии, и задачами, работающими локально.

Начиная с версии RDP 5.0 (Windows 2003 Server), клиентам доступно подключение к терминальной сессии своих локальных дисков, а также использование смарт-карт для аутентификации доступа к серверу.

Примечание

Одной из проблем администрирования терминального сервера являются зависшие задания печати пользователей в различных сессиях. Для того чтобы удалить их, достаточно периодически выполнять следующий сценарий: `net stop spooler del %systemroot%\system32\spool\printers\*.* /q net start spooler`.

Подключение к консоли

Если вы работали за консолью сервера, войдя в систему локально с клавиатуры, а потом попытались подключиться для удаленного управления, то по умолчанию будет создана новая сессия, а локальный экран терминального сервера окажется недоступен. Это не всегда удобно для администраторов: иногда необходимо увидеть сообщения, которые отображаются после старта системы (например, сообщения от системы контроля серверной платформой или предупреждения о неудачном запуске службы), или использовать задачи управления, доступ к которым сохранен на локальном столе, или просто продолжить работу с документом, который остался открыт, когда вам неожиданно пришлось уйти с рабочего места.

Такая возможность появилась с версии Windows 2003 Server. Для работы с экраном консоли нужно запустить клиента подключения к удаленному рабочему столу с ключом `/console`:

```
MSTSC /console
```

Кроме того, есть возможность переключиться в консольную сессию, уже работая в терминале. Среди команд терминала есть утилита `SHADOW`, позволяющая подключиться к любой терминальной сессии. Сессия консоли всегда имеет нулевой номер, поэтому достаточно выполнить команду:

```
SHADOW 0
```

В отличие от запуска подключения с ключом (`MSTSC /console`), данная команда не сможет подключить к консоли, если с последней предварительно не был выполнен вход в систему.

Примечание

Лично у автора несколько раз возникали проблемы при подключении к консоли через терминальную сессию с использованием смарт-карты. Есть проблемы аутентификации при удаленном запуске программ в консольной сессии, кроме того, система практически не позволяет использовать два сертификата одного пользователя и т. п.

Командная строка управления терминальными сессиями

Ранее уже упоминались команды `change user`, `SHADOW`. Перечислю еще несколько команд, которые будут полезны администраторам для управления режимом терминальных служб. Подробности использования команд легко уточнить по справочной документации системы.

- `change logon`

  Разрешает или запрещает новые подключения пользователей к терминальному серверу. Программа полезна, если вы хотите временно, на период работ по настройке сервера, запретить пользователям создавать новые сессии.

- `query`

  В числе прочего команда позволяет запросить список терминальных серверов организации, что вряд ли представляет особую ценность. Главное — команда показывает список текущих пользователей на сервере, идентификаторы их сессий. Эта информация полезна, если вы захотите отключить конкретного пользователя (например, в случае зависания его сессии) от терминала.

- `logoff`

  Команда завершает работу пользователя и удаляет его сессию. В параметрах команды нужно указать тот номер, который вы получили при запросе параметров пользователя командой `query`.

- `reset session`

  В отличие от предыдущей команды завершает сеанс пользователя "силовыми методами". Полезно в случае зависших сеансов.

- `MSG`

  Позволяет послать сообщение пользователю терминальной сессии (конкретному или всем). Например, если вы выключаете сервер, то с помощью этой команды можно попросить пользователей завершить работу к заданному сроку.

- `TSPROF`

  Используется для копирования профиля пользователя.

- `TSSHUTDN`

  Выключает (перезагружает) сервер.

Удаленный рабочий стол в Windows XP/Vista

Операционная система Windows XP включает в себя (в ограниченном варианте) поддержку служб терминального сервера. Установленные ограничения позволяют осуществить одновременно только одно терминальное подключение к рабочей станции. Причем если подключение выполняется не от имени текущего пользователя, то для локального пользователя будет осуществлена операция выхода из системы[1].

Чтобы осуществить подключение удаленных пользователей к компьютеру Windows XP, необходимо, во-первых, разрешить данную возможность. Эта

[1] Данное ограничение носит искусственный характер. Благодаря ошибке разработчиков в Интернете можно найти программы, которые позволяют обойти это ограничение (Termiserv_XPSP2_i386_1.0.exe — в системе заменяется dll-библиотека на версию, которая распространялась с неокончательным вариантом сервис-пака, в результате можно установить несколько терминальных подключений).

опция устанавливается через **Панель управления | Система |** вкладка **Удаленное использование**, на которой следует поставить флажок соответствующего разрешения.

Во-вторых, необходимо определить пользователей, которым разрешается подключаться к рабочему столу компьютера. По умолчанию таким правом обладают только администраторы системы. Чтобы изменить состав разрешений, нужно в окне, описанном выше, нажать кнопку **Выбрать удаленных пользователей** и добавить в список необходимые учетные записи.

Примечание

Обычно локальные пользователи не имеют пароля. В то же время в параметрах системы заложено, что сетевое подключение к компьютеру может быть осуществлено *только* с ненулевым паролем. Поэтому для удаленного подключения необходимо использовать учетную запись пользователя компьютера *только с ненулевым паролем*.

Безопасность данных в терминальной сессии

Данные, передаваемые по каналу связи, в режиме терминального доступа шифруются. Существуют три уровня шифрования. На базовом уровне выполняется шифрование потока от клиента к серверу с 40-битным ключом по алгоритму RC4, на среднем и высшем уровнях защиты используется шифрование потоков по тому же алгоритму RC4, но с 56- и 128-битными ключами. Выбор уровня шифрования осуществляет администратор терминального сервера, устанавливая соответствующие параметры соединения (через задачу настройки терминальных подключений в группе **Административные задачи**).

Если пользователь подключается к компьютеру с операционной системой Windows 2003 Server при помощи терминальной сессии, то он имеет возможность использовать вход в удаленную систему с помощью смарт-карты. Это существенно повышает безопасность работы в системе.

Примечание

Целесообразно дополнительно обезопасить терминальный сервер, создав на основе IPSec фильтры, разрешающие прохождение только пакетов, адресованных на порт 3389.

Несмотря на то что работа клиента с терминальным сервером может быть осуществлена с использованием программы просмотра Интернета, этот вариант также использует протокол RDP. Если подключение осуществляется к терминальному серверу, расположенному в защищенной корпоративной сети, то администратору сети необходимо кроме доступа к серверу по протоколу HTTP (80-й порт) разрешить использование и протокола RDP (3389-й порт).

Подключение администратора к терминальной сессии

Администратор[1] терминального сервера имеет возможность подключиться к пользовательской сессии. Данный режим обычно служит для оказания помощи пользователям терминального сервера: администратор получает возможность наблюдать за чужим экраном и демонстрировать выполнение операций.

Операция выполняется через задачу управления терминальными сессиями исполнением соответствующей команды меню свойств. По умолчанию для выполнения данной операции система запрашивает подтверждение пользователя. Однако можно легко установить настройки, позволяющие выполнить операцию и без такого согласия. Эти настройки выполняются через параметры по умолчанию для терминальной сессии.

Дополнительные ограничения терминальных сессий

Терминальный сервер как сервер публичного доступа обычно нуждается в более строгих ограничениях, чем персональный компьютер пользователя.

Примечание

Конечно, как и при всяких настройках, администратору нужно представлять возможные опасности и разумно реализовывать только необходимые ограничения. Если вы включите *все* те ограничения, параметры которых присутствуют в групповых политиках для терминального сервера от Microsoft, то нормально работать в терминальной сессии не сможет ни один пользователь.

В частности, пользователей нужно ограничить использованием только заданного перечня программ. Следует запретить им доступ к локальным ресурсам сервера, ограничить в выполнении ресурсоемких операций, лишить права устанавливать новые программы и т. п. Приведу небольшой список возможных ограничений[2].

Примечание

Желательно создать специальное OU, в которое переместить терминальный сервер. Для этого OU следует назначить собственную групповую политику, в которой и определить необходимые ограничения.

- В разделе **Конфигурация компьютера | Конфигурация Windows | Параметры безопасности | Параметры ограниченного использования**

[1] Точнее, тот пользователь, которому такое право дано протоколом RDP. По умолчанию это только администраторы терминального сервера. Но при необходимости данное значение можно изменить, воспользовавшись оснасткой управления параметрами RDP-протокола.

[2] Подробное объяснение целей установки каждого ограничения можно найти в специальных статьях на сайте Microsoft, например в статье "Locking Down Windows 2003 Server Terminal Server Sessions".

программ следует определить те программы, которые разрешено запускать пользователям терминала.

- В разделе **Конфигурация компьютера | Конфигурация Windows | Параметры безопасности | Локальные политики | Параметры безопасности** необходимо максимально ограничить параметры **Devices** (ввести доступ к CD-ROM и дискете только для локальных пользователей, т. е. тех, кто работает с консоли сервера).
- Параметры раздела **Конфигурация компьютера | Административные шаблоны | Terminal Services** позволяют настроить параметры сессий пользователя. Рекомендуется запрещать пользователю подключать как диски своего компьютера, так и любых других систем (для исключения запуска программ с этих носителей).
- В разделе **Конфигурация компьютера | Административные шаблоны | Windows Installer** желательно отключить возможность установки программ с использованием Windows Installer.
- В других разделах рекомендуется запретить просмотр и поиск *любых* ресурсов (например, просмотр сети, поиск принтеров, поиск файлов и т. п.). Оцените также целесообразность включения ограничивающих параметров разделов **Конфигурация пользователя | Административные шаблоны**: Windows Explorer, Start Menu & TaskBar, System, Control Panel.

Примечание

Операцию поиска в Проводнике можно вызвать быстрыми клавишами <Ctrl>+<E>. Чтобы заблокировать эту возможность, создайте файл с некоторым поясняющим текстом (например, текстовый или в формате HTML) и установите следующие значения реестра системы: `HKLM\SOFTWARE\Microsoft\Internet Explorer\Search` параметры `SearchAssistant=REG_SZ: <путь к файлу>` и `CustomizeSearch=REG_SZ: <путь к файлу>`. Теперь при попытке выполнить операцию поиска пользователь увидит только содержание данного файла.

В общем случае следует руководствоваться принципом: чем более публичным является терминальный сервер, тем большие ограничения должны налагаться на его использование в целях предупреждения не всегда разумных инициатив пользователей.

Создание локальных копий данных на мобильных устройствах

Пользователю, удаленно работающему с ресурсами организации, хочется выполнять работу так же быстро, как если бы он находился в офисе, и иметь возможность завершения работы независимо от наличия удаленного доступа к офису. Выходом в такой ситуации является создание копий данных на мо-

бильном устройстве с последующей их синхронизацией с сервером. Такое решение позволяет пользователю продолжать работу полностью в автономном режиме.

Примечание

Первой программой Windows, предназначенной для синхронизации данных двух источников, был Портфель. Данная программа сохранена и в текущих версиях ОС, однако она является *индивидуальным* решением. Пользователь должен вручную помещать в Портфель файлы, с которыми он предполагает работать в другом месте, а потом также вручную проводить синхронизацию изменений. С основами работы в данной программе легко разобраться, воспользовавшись интерактивной справочной системой.

Автономные файлы

В Windows 200*x*/XP/Vista предусмотрена возможность кэшировать сетевые ресурсы на локальный компьютер. В результате можно продолжить работу с файлами и после отключения от компьютерной сети (например, на ноутбуке в автономном режиме), а затем автоматически синхронизовать все изменения.

Примечание

В первых версиях операционных систем при кэшировании зашифрованных файлов локальные копии данных во временной папке *не шифровались*. Впоследствии этот недостаток был устранен. Но при разрешении автономной работы с такими данными в целях предотвращения утечки данных администратору следует убедиться, что у пользователей установлены последние версии операционных систем.

Сделать файлы сетевой папки доступными в автономном режиме можно, разрешив ее кэширование (рис. 8.10). Обратите внимание, что по умолчанию не кэшируются файлы следующих типов: *.slm; *.mdb; *.ldb; *.mdw; *.mde; *.pst; *.db*, но эта установка может быть изменена с помощью групповой политики.

Работа с файлом при наличии подключения к сетевому ресурсу будет производиться именно с сетевой копией. Операции синхронизации (с учетом их настроек) сделают обе копии файлов идентичными.

Существует несколько вариантов кэширования файлов. При *ручном способе* на локальный диск копируются только файлы, явно отмеченные пользователем. Если выбрать вариант *автоматического кэширования документов*, то на локальном диске будут создаваться автономные копии тех документов, которые открывались пользователем. Вариант *автоматического кэширования программ и документов* отличается "односторонностью": на локальный диск

всегда копируются более новые версии файлов с сервера, но не наоборот. Считается, что версии на сетевом ресурсе имеют большее предпочтение.

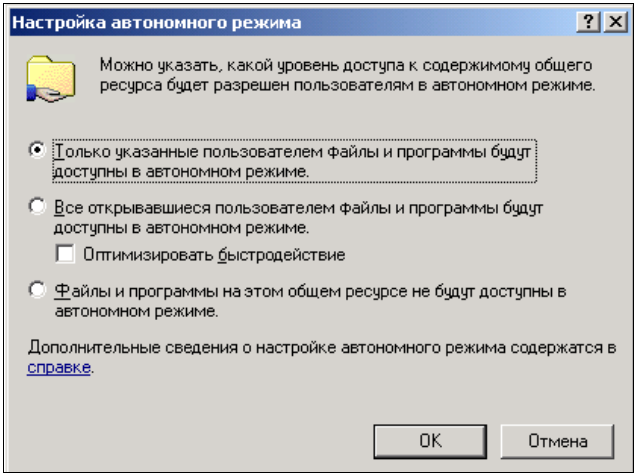


Рис. 8.10. Включение и настройка автономных файлов

Опция **Создать ярлык папки автономных файлов на рабочем столе** позволяет вывести на рабочий стол ярлык к папке, в которой хранятся автономные копии файлов. Эта опция удобна, если вы предполагаете продолжить работу с файлами в автономном режиме.

Для автоматического кэширования файлов выделяется по умолчанию 10% объема жесткого диска. Эта величина может быть изменена в настройках опций автономных файлов. Если объем автономных файлов превышает заданный лимит, то система автоматически удаляет самые старые версии. Таким образом, в автоматических режимах нет гарантии, что все необходимые файлы будут доступны автономно. Система может удалить часть из них, если будет достигнут порог допустимого использования жесткого диска. Обратите внимание, что объем автономных файлов, которые были кэшированы в ручном режиме, не учитывается в данном лимите. То есть выбранные *вручную* файлы *всегда будут доступны автономно*.

Варианты синхронизация автономных файлов

Существуют различные варианты синхронизации автономных файлов с сетевыми ресурсами. Вы можете установить синхронизацию при входе и/или выходе из системы, по заданному времени или в период нахождения компьютера в ждущем режиме (рис. 8.11).

Настройки синхронизации устанавливаются в программе Синхронизовать, которая расположена в меню **Пуск | Стандартные**. Заметьте, что синхрони-

зация может быть проведена только в то время, когда пользователь совершил вход в компьютерную сеть (`log on`).

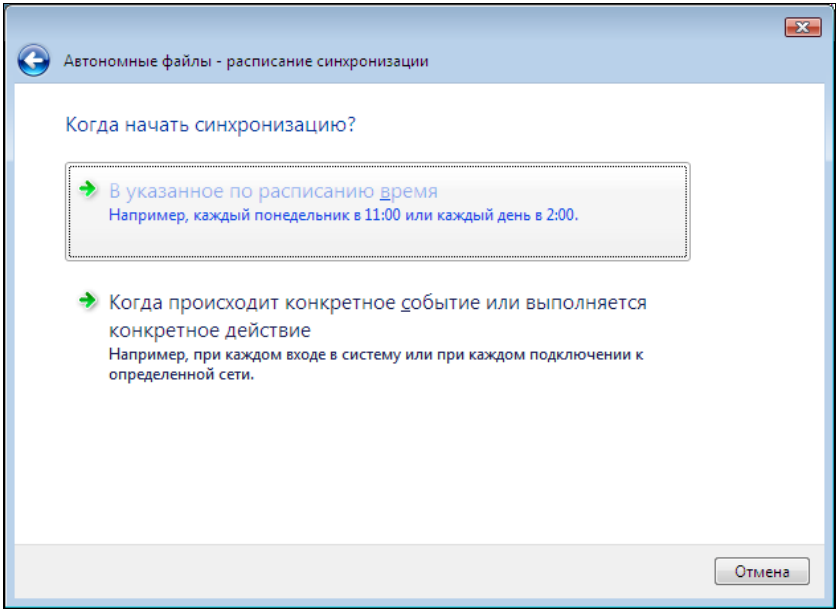


Рис. 8.11. Настройка вариантов синхронизации автономных файлов в Windows Vista

Разрешение конфликтов

В случае работы с автономными копиями файлов возможно возникновение ситуаций, когда документ редактировался как автономно, так и был изменен другим пользователем на сетевом ресурсе. В этом случае программа предложит вам выбрать один из трех вариантов разрешения данного конфликта: либо сохранить обе версии файлов, либо использовать версию на сетевом ресурсе, либо локальную копию.

Удаление автономных файлов

Удалить автономные копии файлов можно двумя способами. Первый способ — это удалить файлы из папки, в которой они хранятся для автономной работы (ярлык к этой папке часто выводят на рабочий стол для возможности работы с файлами в автономном режиме). Второй способ — это выбрать операцию удаления автономных файлов в окне настройки соответствующих опций папок компьютера.

Но обратите внимание, что такое удаление не отключает само кэширование файлов. При следующем соединении с сетевыми ресурсами кэширование бу-

дет проведено снова и на локальном диске опять будут созданы автономные копии файлов. Чтобы отключить кэширование, необходимо изменить опции настройки папок системы.

Настройка автономных почтовых папок

Если политика организации предусматривает хранение почты сотрудников только на почтовом сервере, то для ускорения удаленной работы с почтой следует создать локальные копии почтовых сообщений. Покажем, как настроить почту для работы в автономном режиме в случае использования в качестве почтового сервера MS Exchange Server, а в качестве клиента — MS Office.

Настройка автономных папок в Outlook 200*x* производится через меню **Сервис | Параметры |** вкладка **Настройка почты**. На этой вкладке нужно нажать кнопку **Отправить и получить**, чтобы открылось окно настройки параметров отправки и получения корреспонденции, в котором и следует произвести необходимые действия.

При использовании Outlook 97 автономные папки создаются в тот момент настройки профиля, когда система задает вопрос: "Путешествуете ли Вы со своим компьютером?". При положительном ответе создаются автономные папки. Поэтому самым простым способом создания автономных папок в этом случае будет удаление конфигурации почтового клиента (через задачу **Почта** в Панели управления) и повторном прохождении всех шагов мастера создания почтового профиля.

После настройки автономных папок сообщения (для выбранных папок) будут скопированы на локальный компьютер. В дальнейшем по выбранному графику содержимое папок будет синхронизироваться с почтовым сервером. Причем пользователь сможет продолжать работу с почтой и при отсутствии связи: сообщения будут отосланы или приняты сразу после восстановления соединения.

Кэширование сервера Exchange 2003

При использовании программы Outlook 2003 совместно с сервером Exchange 2003 появляется возможность кэширования почтовых папок. Эта опция позволяет снизить нагрузку на почтовый сервер и продолжать работу при отсутствии подключения.

Однако режим кэширования следует отключать при большом объеме папок пользователя (рекомендуется отключение при суммарном объеме сообщений более 1 Гбайт), поскольку в этом случае операции синхронизации папок после включения ноутбука в локальной сети будут занимать существенное время.

Перенаправление папок хранения документов

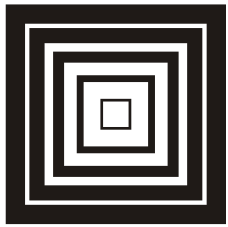
Для систем Windows 2000/XP/Vista администратор может с помощью групповой политики осуществить перенаправление целого ряда специальных папок на сетевые ресурсы. Так можно перенаправить Рабочий стол, Мои документы, Мои рисунки, меню **Пуск**, папку Application Data[1].

Такое решение может быть рекомендовано, поскольку позволяет хранить на сервере актуальные копии всех документов, с которыми работают пользователи. Это облегчает операции резервного копирования данных и снижает риск утери информации в случае выхода из строя клиентского компьютера. Однако сохранение файлов на сервере неизбежно выполняется медленнее, чем локально, что может вызывать некоторые недовольства пользователей. Одновременно повышается нагрузка на сервер и увеличивается объем необходимого для него дискового пространства.

Примечание

Не забудьте отключить эти установки для профилей, применяемых при удаленном подключении.

[1] Это выполняется в разделе **Конфигурация пользователя | Конфигурация Windows | Перенаправление папок**.



ГЛАВА 9

Безопасность

После подключений Windows XP SP1 к Интернету система была заражена через 18 минут[1].

Безопасность информации компьютерной сети привлекает особое внимание специалистов, впечатляющими темпами растут расходы на ее обеспечение. Но при этом часто забывают, зачем вообще нужно обеспечивать информационную безопасность, и ставят перед собой невыполнимую задачу достижения абсолютной надежности.

Зачем нужно заниматься обеспечением безопасности и какой ее уровень оптимален для системы?

Попытаемся оценить последствия выхода из строя какого-либо компьютера, перехвата управления над ним злоумышленником, копирования находящейся на нем информации и т. п.

Если это наш домашний компьютер, то нам, скорее всего, было бы жаль потерять хранимые на нем данные, хотя их копирование вряд ли нанесет какой-либо ущерб. Нам бы не хотелось переустанавливать операционную систему чаще, чем того требует практика работы с Windows. При подключении к Интернету, особенно если это происходит через выделенную сеть, мы не хотим, чтобы кто-то посторонний воспользовался нашими учетными данными и использовал их для оплаты своего трафика. При этом трудно представить ситуацию, что кто-то захочет заблокировать работу нашего компьютера в Интернете путем организации атак отказа в обслуживании. Не будет критичным для домашнего компьютера и выход из строя, например, блока питания, хотя ремонт и доставит нам некоторые неудобства. В результате меры безопасности, реализуемые на персональном компьютере, обычно ограничиваются только установкой антивирусной программы и межсетевого экрана.

Если аналогичным образом оценить какую-либо производственную систему, то последствия будут существенно иными. Сервер, на котором собираются

---

[1] См. отчет по эксперименту на **http://www.interface.ru/home.asp?artId=6980**.

данные о соблюдении технологических параметров, нельзя остановить на время большее, чем первичные данные могут храниться в буфере оборудования, а кража документации по изделиям может принести немалый ущерб предприятию, если такое действие было осуществлено в интересах конкурента.

На основании приведенных примеров можно заключить, что в каждом конкретном случае затраты, выделяемые на обеспечение безопасности, должны коррелировать с потенциальной опасностью. Если злоумышленник задастся целью "сломать" систему, он обязательно это сделает и нам не поможет никакая защита. Важно снизить вероятность такого вторжения до экономически оправданных значений и минимизировать возможный ущерб.

Удобство в работе и безопасность. Человеческий фактор

Как руководители, так и системные администраторы должны четко понимать, что удобство в работе пользователей и безопасность предъявляют к системе совершенно противоположные требования. Чем безопаснее система, тем больше ограничений накладывается на текущую работу и тем более неудобной она становится, и наоборот. Проще всего использовать систему, в которой отсутствуют какие-либо ограничения по безопасности данных. Любая реальная система содержит разумные компромиссы, определяемые в каждом конкретном случае индивидуально.

При реализации тех или иных организационных и технических мероприятий всегда следует учитывать человеческий фактор. Если вы потребуете от сотрудников частой смены пароля, то, чтобы не забыть, они начнут записывать пароли на различные памятки. Контроль сложности паролей не заставит пользователей формировать их при помощи генераторов случайных чисел. Скорее всего, большинство будет постоянно использовать один и тот же пароль, составленный на основе некоторой осмысленной последовательности символов, изменяя в нем (когда настанет срок очередной смены пароля) по одному символу.

Любая идеально спроектированная система защиты окажется неработоспособной, если она не будет учитывать практические аспекты эксплуатации информационной системы.

Интернет-ресурсы, посвященные безопасности

Системному администратору необходимо быть достаточно информированным о текущем состоянии компьютерной безопасности. Это предполагает

периодическое ознакомление с данными специализированных сайтов, посвященных этой тематике, по возможности подписку на оповещения об обнаруженных критических уязвимостях.

Примечание

Существует мнение, что крупные ресурсы, посвященные вопросам безопасности, имеют соглашения с software-гигантами по замалчиванию некоторых данных, способных повлиять на имидж разработчика. Так, Cnews (**http://www.cnews.ru/newtop/index.shtml?2005/02/01/173840**) сообщил, что российские специалисты сразу после выхода SP2 для Windows XP обнаружили, что "в этом обновлении не работают механизмы предотвращения выполнения данных — то, ради чего SP2, собственно, и выпускался. Самое парадоксальное в этой ситуации то, что ни Microsoft, ни крупнейшие порталы по информационной безопасности не стали публиковать эту информацию". "Возникает мысль о том, что компания во главу угла ставит свои маркетинговые интересы, а лишь затем заботится о безопасности своих продуктов", — приводит CNews слова одного из экспертов.

Отмечу следующие источники.

- SecurityFocus (**http://www.securityfocus.com**).

  Сайт позволяет подписаться на многочисленные рассылки по проблемам безопасности. Честно говоря, автору больше нравится читать приходящие сообщения электронной почты, чем периодически посещать страницы Интернета, выясняя новости сайтов.

- Packet Storm (**http://www.packetstormsecurity.org**).

  Сайт включает в себя перечни эксплойтов, сценариев, кодов, которые применяются при атаках на компьютерные системы. Эти коды собираются с андеграунд-сайтов, правда, не всегда оперативно. Но информация сайта, а также приведенные на нем ссылки на ресурсы Интернета заслуживают внимания администратора.

- CERT vulnerability notes (**http://www.kb.cert.org/vuls/**).

  Сайт, на котором публикуется информация об уязвимостях от группы United States Computer Emergency Readiness Team. Эта группа существует с 2003 года и занимается анализом и предупреждением кибер-преступлений в США.

  На сайте также можно осуществить подписку на рассылку об обнаруженных уязвимостях.

- Common Vulnerabilities and Exposures (MITRE CVE, **http://cve.mitre.org**).

  Сайт посвящен вопросам стандартизации уязвимостей.

- ISS X-Force (**http://xforce.iss.net**).

  Сайт Internet Security Systems — организации, являющейся одним из лидеров изучения безопасности и осуществляющей круглосуточный монито-

ринг Интернета. Администраторы могут загрузить различные патчи, устраняющие те или иные уязвимости.

- Еженедельная рассылка @RISK (**http://www.sans.org/newsletters/risk/**).

  Институт SANS (SysAdmin, Audit, Network, Security) занимается изучением уязвимостей и обучением специалистов безопасности. Данные об обнаруженных уязвимостях публикуются институтом в нескольких периодических рассылках, на одну из которых можно подписаться по указанному выше адресу.

- Русскоязычный сайт с исследованиями уязвимостей (**http://securityvulns.ru/**).

- Группа реагирования на компьютерные инциденты (**http://www.ciac.org/ciac/index.html**).

В заключение приведем еще несколько ссылок на ресурсы, посвященные проблемам безопасности, в том числе списки рассылки и несколько андеграунд-ресурсов:

- **http://www.osvdb.org**
- **http://www.securitylab.ru**
- **http://www.secunia.com**
- **http://www.ntbugtraq.com**
- **http://www.thc.org**
- **http://astalavista.com**
- **http://www.insecure.org**
- **http://www.zone-h.org**

Анализ рисков

Причины, способные вызвать нарушение функционирования информационной системы, можно разделить на следующие группы:

- умышленные действия пользователей, имеющих доступ к информации и/или настройкам системы;
- не умышленные, ошибочные действия пользователей, имеющих доступ к информации и системе;
- умышленные действия лиц, не имеющих доступа к информации;
- отказ оборудования, порывы кабелей и т. д.

Задачу защиты информационной системы целесообразно рассматривать по уровням:

- уровень сети (уязвимости протоколов TCP/IP, канального уровня);
- уровень операционных систем (особенности реализации и уязвимости различных ОС);

- уровень управления базами данных (выделен особо, поскольку практически все информационные системы используют те или иные базы данных);
- уровень прикладных приложений.

Для каждого уровня защиты системному администратору необходимо определить риски и выявить их возможные причины, исходя из чего предусмотреть соответствующие меры противодействия.

Наиболее трудоемки в определении риски, связанные с конкретной реализацией информационной системы и используемым в ней программным обеспечением. Чтобы правильно предусмотреть возможные опасности при использовании на одном компьютере программного продукта А, на другом — В и при наличии, например, конкретного типа хранения данных на сервере, нужно обладать высокой квалификацией практически по всем используемым продуктам.

Хорошо, если такие специалисты в организации есть и они могут выработать какие-либо *предупреждающие* мероприятия. В подавляющем же большинстве случаев используется информация только о типовых уязвимостях, которые известны техническому персоналу.

Примечание

В силу особой важности этого положения, хочу еще раз акцентировать внимание на том, что ни одна программа, сканирующая сеть на наличие уязвимостей, ни одна аудиторская организация, приглашенная для анализа безопасности, не смогут предложить вам исчерпывающий перечень мероприятий. В большинстве случаев вы получите анализ типовых уязвимостей в типовой структуре. Так, сканеры безопасности проверяют, прежде всего, реализацию всех мер, предлагаемых изготовителем в инструкции по повышению безопасности *(см. разд. "Индивидуальная настройка серверов" далее в этой главе)*, и установку обновлений *(см. разд. "Обновления" далее в этой главе)*. При сертификации системы особое внимание уделяется наличию комплекта организационно-распорядительной документации (приказов, инструкций, матриц доступа и т. п.). "Закрытие" всех этих уязвимостей не даст шанса "покоиться на лаврах".

После того как будет определен перечень возможных рисков, необходимо рассмотреть стоимость "блокирующих" мероприятий.

Как правило, существует несколько возможных путей решения, и вам необходимо, исходя из специфики организации, выбрать оптимальный. Например, риску кражи сервера с важной информацией можно противопоставить введение круглосуточной охраны, а можно предусмотреть какое-либо аппаратное шифрование данных на жестком диске. Если стоимость сервера меньше стоимости мер его защиты от пожара, то выгоднее пожертвовать конкретным компьютером, ограничившись резервным копированием данных.

В итоге такого анализа вы получите достаточно большой перечень возможных рисков. Понятно, что реализовать все мероприятия будет практически невозможно. Поэтому следует руководствоваться достаточно общим правилом "30/70": 70% всех уязвимостей могут быть закрыты реализацией лишь 30% мероприятий, надо только правильно ранжировать их по значимости.

К сожалению, практика оперативного появления в продаже практически любых баз данных, имеющих коммерческое значение, свидетельствует, что многие меры защиты существуют больше "для отчетности", чем реально обеспечивают конфиденциальность информации. Без *постоянного* внимания к вопросам информационной безопасности говорить о безопасности бессмысленно.

Три "кита" безопасности

Объем работ по обеспечению безопасности информационной системы составляет основную часть рабочего времени системного администратора, поэтому важно правильно организовать свою работу. На какие принципиальные моменты я бы советовал обратить внимание.

- Обеспечьте документальное оформление безопасности информационной системы организации.

  Все действия, которые предпринимает системный администратор в части тех или иных технических настроек системы, являются только реализацией требований, которые должны быть заложены в концепции информационной безопасности предприятия и реализующих ее конкретных положениях и инструкциях.

- Реализовывайте эшелонированную систему обороны.

  При организации мер защиты информационной системы возьмите курс на создание нескольких рубежей защиты. Взломать два уровня защиты гораздо сложнее, чем один.

  Так, антивирусную защиту можно настроить на сервере (анализ сообщений на почтовом сервере, проверка трафика Интернета на прокси-сервере и т. п.) и на компьютере пользователя. Проверку пользователя можно выполнять как при физическом подключении (настройкой безопасности портов активного оборудования), при входе в сеть, при запуске прикладной программы (используя аутентификацию при входе в задачу) и т. д.

- Постоянно контролируйте систему.

  Ни одни правила не выполняются, пока нет реального контроля. Не доверяйте радужным отчетам. Проводите независимый контроль, организуя

специальные проверки. Анализируйте данные статистики: отклонения[1] от "нормального" поведения могут свидетельствовать о готовящейся атаке.

И последний совет. Сколько бы усилий вы не прилагали, защищая систему, всегда может обнаружиться уязвимость, которая может позволить злоумышленнику провести успешную атаку. Ваша задача заключается в реализации таких мер, которые позволят уменьшить эффект от вторжения и с минимальными затратами для предприятия восстановить работу информационной системы.

Основные направления работ по защите информационной системы

В каждой организации "лидеры" по эффективности мер обеспечения безопасности будут свои. Тем не менее существует несколько мероприятий, необходимость реализации которых никем не ставится под сомнение:

- выработка организационных мероприятий обеспечения безопасности;
- поддержание актуальной защиты от вирусов и вторжений;
- установка обновлений безопасности программного обеспечения;
- индивидуальная настройка серверов (hardening);
- использование брандмауэров при подключении к Интернету.

Организационное обеспечение информационной безопасности

Практика показывает, что организационные мероприятия по эффективности в несколько раз превосходят технические меры защиты.

Прежде всего, на уровне руководства предприятия необходимо сформировать четкое представление об основных положениях информационной безопасности. Предпочтительно создать концепцию информационной безопасности, в которой определены категории обрабатываемой информации, перечислены предполагаемые риски, установлены направления и объем защиты данных для каждой категории.

Каждая автоматизированная система предприятия должна иметь официально присвоенную ей категорию по конфиденциальности, любое рабочее место —

[1] Например, на одном из предприятий кража данных была обнаружена анализом статистики сетевого трафика: пользователь копировал информацию в ночное время, и эти действия проявились повышением сетевого трафика в часы, когда подобной активности не предполагалось.

паспорт, в котором должны быть перечислены конфигурация системы, установленное программное обеспечение, категории информации, с которой предполагается работать на данном компьютере. После того как такой укрупненный анализ будет выполнен, станет проще планировать и реализовывать защиту данных.

В организационно-распорядительных документах организации необходимо зафиксировать правила взаимодействия пользователя с информационной системой. Пользователь должен знать, с чем он работает, какие программы он может использовать, а какие утилиты запрещены в организации (например, сканирования сети) и т. п. В инструкциях необходимо оговорить правила работы с электронной почтой организации, поведение пользователя в случае возникновения предположения о наличии вируса, требования к взаимодействию с Интернетом и т. д.

Чем точнее определены права пользователя и ответственность за нарушение обязанностей, тем с большей вероятностью вы можете ожидать исполнения инструкций.

Естественно, что выполнение требований инструкций должно сопровождаться периодическими проверками, например, путем анализа журнала посещенных сайтов Интернета *(технический контроль)* или проверкой отсутствия записей паролей на стикерах *(организационные меры)*.

Индивидуальная настройка серверов

Типовая конфигурация операционной системы после стандартной установки "из коробки" позволяет использовать систему в производственной деятельности сразу после ее установки. При этом в подавляющем большинстве случаев система содержит *излишние функции*, которые целесообразно отключить в целях повышения безопасности[1]. Как правило, следует отключить запуск служб системы, не используемых в конкретной конфигурации, и настроить параметры безопасности (протоколы аутентификации, уровень предоставления информации анонимному пользователю и т. п.) по максимально возможному уровню с учетом специфики информационной системы. Такие настройки индивидуальны для каждого случая применения компьютера, поэтому привести универсальные рекомендации в данной книге не представляется возможным.

Отмечу только, что администратору системы следует оптимизировать *каждый* сервер под те задачи, которые он решает. Необходимые рекомендации

[1] Каждая избыточная функция — это дополнительный код, который может содержать потенциальные ошибки, может использоваться для проникновения в систему и т. п.

можно легко найти на сайтах разработчиков программного обеспечения по ключевым словам "hardening" или "security guide". Приведу несколько названий соответствующих документов: "Windows 2000 Security Hardening Guide", "Exchange Server 2003 Security Hardening Guide", "Windows XP Security Guide", "Hardening the Windows Infrastructure on the ISA Server 2004 Computer", "Red Hat Linux Security Guide", "Apache Security Configuration Guide" и т. д. В подобных документах обычно достаточно подробно описываются параметры, влияющие на уровень безопасности системы, и возможные последствия в функционировании информационной структуры при их изменении. Администратору следует внимательно проанализировать каждый параметр и оценить целесообразность предполагаемых изменений.

Security Configuration Manager

В составе Windows 2003 Server после установки SP1 присутствует программа Security Configuration Manager (SCM). Как видно по названию, SCM предназначена для настройки параметров безопасности сервера. Практически программа предлагает применить к системе один из шаблонов безопасности, выбрав ту или иную роль данного сервера.

SCM привлекательна тем, что предлагает применить *комплексно* все те рекомендации, которые содержатся в объемных руководствах по безопасности. Однако в реальных системах малых и средних предприятий редко можно найти серверы с "чистой" ролью: обычно присутствуют те или иные модификации, заставляющие администратора тщательно ревизовать предлагаемые к назначению настройки. По крайней мере, во всех случаях, когда данная программа использовалась автором, предлагаемый комплект настроек приходилось дополнительно модифицировать вручную.

Обеспечение сетевой безопасности информационной системы

Сеть передачи данных может объединять несколько десятков портов и более, при этом администратор не может быть уверен, что к системе подключены только рабочие места пользователей. Существует много уязвимостей, которые позволяют злоумышленнику перехватывать сетевой трафик или нарушать работу систем передачи данных.

Если кто-то принесет мобильное устройство и, например, начнет прослушивать сеть, пытаясь перехватить пароли, то такой факт негативно скажется на общем уровне безопасности всей информационной системы. Поэтому в организациях с повышенными требованиями к защите информации обычно ис-

пользуют технологии, позволяющие контролировать подключение сетевых устройств.

Фильтрация по MAC-адресам

Самый простой способ контроля подключенного к сети устройства заключается в проверке его адреса. Этот контроль поддерживается практически всеми управляемыми коммутаторами. При включении режима контроля MAC-адреса коммутатор запоминает MAC-адрес из первого пришедшего пакета и в дальнейшем пропускает данные только с этого устройства.

Включение данного режима позволит защититься от такой уязвимости, как ARP-spoofing[1], при реализации которой злоумышленник может "встать" между двумя компьютерами, обменивающимися данными, и перехватывать весь трафик.

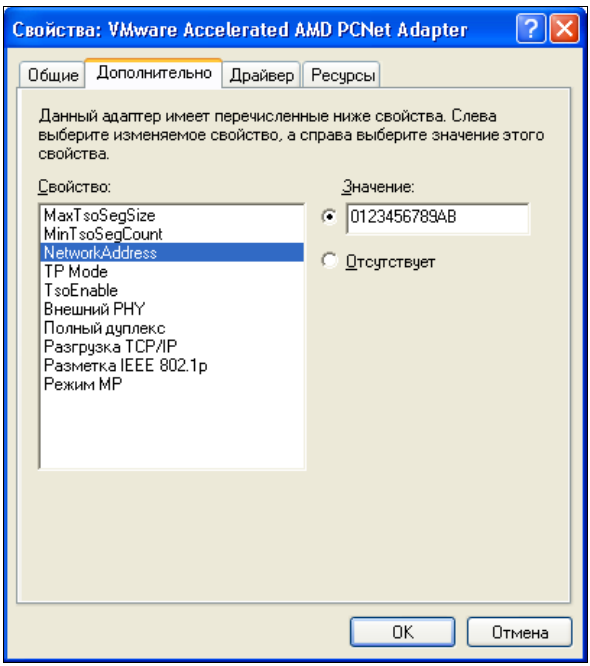


Рис. 9.1. Изменение MAC-адреса путем редактирования свойств адаптера. Если настройки сетевого адаптера не содержат возможности смены MAC-адреса, можно его изменить через реестр системы — параметр `NetworkAddress` ключа `HKLM\SYSTEM\CurrentControlSet\Control\Class\<GUID` сетевого адаптера>. После изменения MAC-адреса желательно перезапустить сетевой интерфейс (отключить и снова включить)

[1] Данная атака использует особенности реализации протокола разрешения имен (ARP) и не зависит от реализации программного обеспечения.

Но поскольку при обнаружении пакета с другим адресом коммутатор блокирует порт до явного вмешательства, администраторы не любят включать такую возможность по собственной инициативе.

Примечание

Использование фильтрации по MAC-адресам в тех или иных списках доступа не имеет смысла. Существует много способов заменить реальный MAC-адрес на произвольное значение. Это легко сделать даже средствами Windows (рис. 9.1), не говоря уже о различных специализированных утилитах, таких как SMAC (**http://www.klcconsulting.net/smac**) и др.

Протокол 802.1*x*

Наиболее безопасным средством контроля подключения к сети в настоящее время является использование протокола 802.1*x*. Протокол 802.1*x* предназначен для аутентификации устройства, подключаемого к локальной сети. Первоначально он был разработан для беспроводных сетей, но впоследствии стал применяться и для контроля устройств, подключаемых к проводным сегментам.

Принципы подключения, описываемые в стандарте, достаточно просты. Первоначально порт, к которому подключается устройство, находится в отключенном состоянии и может пропускать *только* пакеты процесса аутентификации (эти пакеты передаются между подключаемым устройством и службой аутентификации). Подключаемое устройство можно идентифицировать как по его параметрам (например, по заранее известному MAC-адресу или сохраненному сертификату), так и по данным пользователя (в этом случае порт будет открыт после входа пользователя в операционную систему). В качестве службы аутентификации используется RADIUS. После получения подтверждения от RADIUS порт открывается для передачи информации в обоих направлениях.

В процессе аутентификации могут быть использованы различные технологии подтверждения устройства. Наиболее безопасным считаются идентификации на основе сертификатов. Именно настройки данного варианта мы и опишем в настоящем разделе.

Особенности применения протокола 802.1*x*

Поскольку протокол 801.1*x* изначально предназначался для беспроводных сетей, администраторам необходимо учитывать некоторые особенности его реализации в ЛВС.

Область применения

Протокол 802.1*x* следует использовать только на портах подключения *конечных* устройств. Применить его на уровне распределения и выше невозможно.

Количество устройств на одном порту

Стандарт предусматривает открытие порта после получения подтверждения идентификации устройства. В результате к порту коммутатора можно подключить небольшой сетевой концентратор с несколькими устройствами. После открытия порта аутентифицированным устройством другие компьютеры смогут беспрепятственно работать в локальной сети.

Для предупреждения такой опасности можно применить несколько решений. Во-первых, включить на портах контроль по MAC-адресам; такую возможность поддерживает большинство коммутаторов. Обнаружение на порту второго устройства с другим MAC-адресом заблокирует порт. Вторая возможность предусматривает контроль за подключенными устройствами; данный режим реализован не для всех моделей коммутаторов. Например, для коммутаторов Cisco режим, когда через порт может работать только одно устройство, называется single-host, а описанный в стандарте — multiple-hosts.

Применение для IP-телефонии

Если предприятие использует IP-телефонию, то подключение телефонных аппаратов и компьютера обычно производится к *одному* порту коммутатора (используется коммутатор на два порта в телефоне). Как правило, настраивать аутентификацию для IP-телефонов не имеет смысла, поскольку, во-первых, при правильном администрировании подключение аппарата сопровождается вводом соответствующего пароля с консоли телефона, во-вторых, данные аудиопотока выделяются в отдельную VLAN. Поэтому многие модели коммутаторов имеют настройки, позволяющие включить необходимость аутентификации по протоколу 802.1*x* для всего трафика, *кроме* IP-телефонии.

Отсутствие возможности поддержки протокола 802.1*x*

Есть ряд устройств, которые не поддерживают данный протокол: во-первых, это компьютеры, на которых установлены старые версии операционных систем, во-вторых, — сетевые принтеры и аналогичные устройства.

В этом случае на соответствующих портах следует использовать иные методы контроля подключенных устройств (например, по MAC-адресам).

Настройка протокола 802.1*x*

Как уже говорилось, мы опишем самый безопасный вариант настройки — на основе сертификатов.

В этом случае администратор должен обеспечить:

- ❒ настройку Центра Сертификации;
- ❒ настройку службы каталогов;
- ❒ настройку службы RADIUS;
- ❒ настройку клиентского компьютера;
- ❒ настройку коммутатора.

Рассмотрим особенности упомянутых настроек.

Настройка Центра Сертификации

Для аутентификации по протоколу 802.1*x* вам необходимо, чтобы, во-первых, клиенты имели соответствующие сертификаты, во-вторых, сертификат должен получить RADIUS-сервер.

Автоматическая выдача сертификатов компьютерам

Часто для компьютеров, входящих в домен, удобно настроить автоматическую выдачу сертификатов. Это делается с помощью групповой политики путем настройки **Конфигурация компьютера | Конфигурация Windows | Параметры безопасности | Политики открытого ключа | Параметры автоматического запроса сертификатов | Создать необходимый автоматический запрос**.

Получение сертификата RADIUS

RADIUS-серверу необходим специальный сертификат, который можно использовать при аутентификации по протоколу 802.1*x*. По умолчанию шаблон данного сертификата не опубликован в Центре Сертификации. Чтобы получить данный сертификат, следует:

- ❒ открыть оснастку Центр Сертификации;
- ❒ отметить папку Шаблоны сертификатов и в ее динамическом меню выбрать операцию **Создать | Выдаваемый шаблон сертификата** (рис. 9.2);
- ❒ выбрать шаблон RAS и IAS-сервер[1].

По умолчанию получение данного сертификата доступно только администраторам домена. Для этого необходимо на сервере, на котором запущена служ-

[1] Этот шаблон доступен *только* в Центре Сертификации, созданном на Windows 2003 Server Enterprise Edition.

ба IAS, открыть оснастку управления сертификатами *локального компьютера* с правами соответствующей учетной записи и запросить сертификат данного типа. После выполнения операции следует проверить наличие сертификата в соответствующем контейнере.

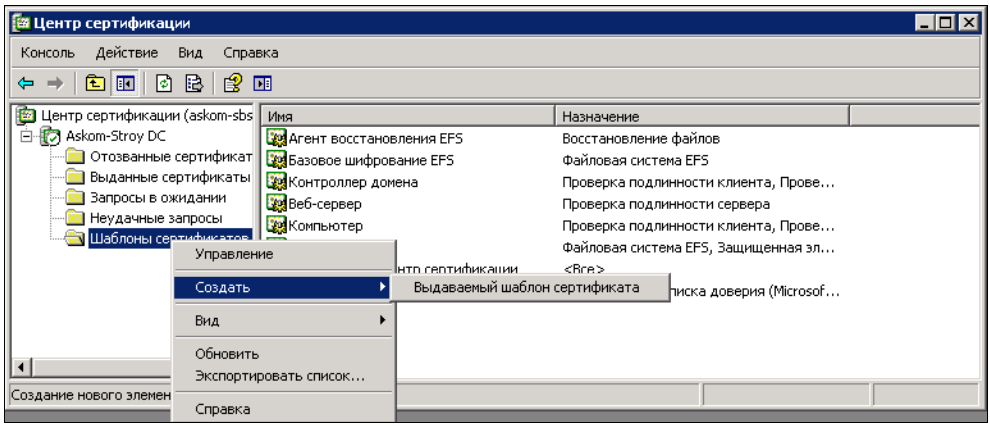


Рис. 9.2. Публикация шаблона сертификата RADIUS-сервера. Для использования в протоколе 802.1*x* аутентификации на основе сертификатов сервер IAS должен получить специальный сертификат, который по умолчанию не опубликован в Центре сертификации

Настройка службы каталогов

При настройке сети организации права доступа обычно предоставляются на основании членства в той или иной группе безопасности, а не путем индивидуального назначения. Для предоставления права доступа создайте в службе каталогов соответствующие группы безопасности и включите в них требуемые объекты. Если вы предполагаете аутентифицировать компьютеры, то в группу надо включить учетные записи компьютеров (по умолчанию они не отображаются среди объектов выбора; для отображения учетных записей компьютеров следует изменить тип выбираемых объектов).

Кроме того, не забудьте включить опцию разрешения входящих звонков для соответствующих учетных записей (в том числе и компьютеров).

Настройка службы RADIUS

Компьютер со службой IAS (реализация службы RADIUS в Windows) должен входить в специальную группу безопасности домена, чтобы иметь доступ к параметрам учетных записей. Эта операция выполняется путем авторизации службы в ее меню.

Настройка компьютера с IAS предполагает настройку *клиентов* и создание *политик удаленного доступа.*

Настройка клиентов IAS

IAS сможет предоставлять данные о результатах аутентификации после регистрации в нем всех устройств, которые могут обращаться с соответствующими запросами. Делается это созданием *клиента* для *каждого* такого устройства (в нашем случае — коммутатора).

При создании клиента указывается его IP-адрес и ключ. Ключ — это пароль, который должен быть одинаковым в настройках IAS и клиента. Рекомендуется для каждого клиента выбирать его уникальным и достаточно сложным — длиной более 20 символов; ключ вводится всего в двух конфигурациях и практически не меняется в процессе работы.

Настройка политик удаленного доступа

Возможность получения клиентом аутентификации от службы IAS всецело определяется *политиками удаленного доступа*. Обычно таких политик достаточно много; они просматриваются по очереди, пока запрос клиента не совпадет с какой-либо из них.

Политику удаленного доступа следует создавать при помощи мастера создания политик, указывая вариант Ethernet и вводя на запрос о группах Windows названия групп, которым предоставлено право доступа.

В результате служба IAS будет проверять членство компьютера или пользователя в соответствующей группе. Если проверка выполнится успешно, то коммутатор получит соответствующее разрешение на открытие порта.

Настройка автоматического назначения VLAN для порта коммутатора

Многие коммутаторы имеют возможность назначить порт в тот или иной VLAN в соответствии с данными аутентификации. Для этого данные от службы IAS должны возвращать соответствующие параметры. Покажем, как это сделать.

После создания политики удаленного доступа откройте ее свойства и нажмите клавишу редактирования профиля. Выберите вкладку **Дополнительно** (рис. 9.3) и добавьте следующие три атрибута:

- Tunnel-Medium-Type со значением 802 (includes all 802 media plus Ethernet canonical format);

- Tunnel-Pvt-Group-ID со значением номера VLAN, в которую должен быть помещен порт в случае удачной аутентификации (на рисунке выбрана VLAN с номером 20);
- Tunnel-Type со значением Virtual LANs.

При получении запроса служба последовательно проверит соответствие его данных имеющимся политикам удаленного доступа и возвратит первое удачное совпадение или отказ.

Совет

Журналы IAS сложно интерпретировать без специализированных программ просмотра. Они бесплатны, их несложно найти в Интернете. Экран одной из таких программ показан на рис. 9.4.

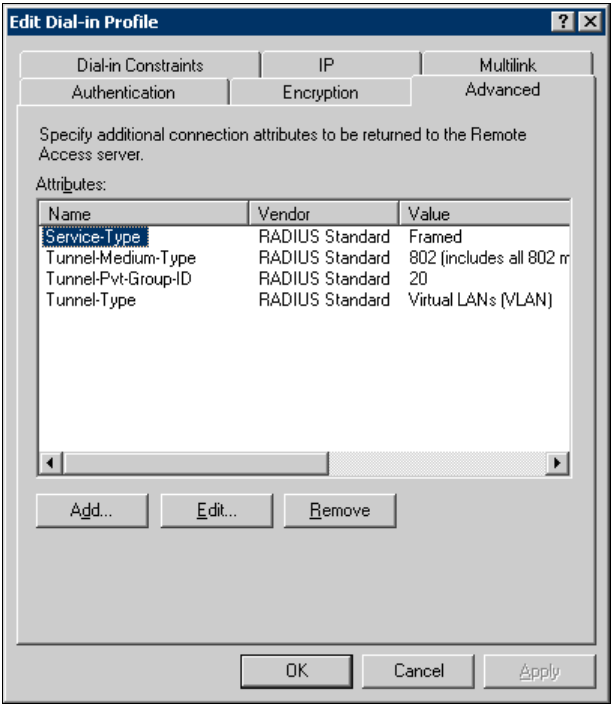


Рис. 9.3. Настройка атрибутов, используемых для автоматического назначения порта коммутатора в VLAN

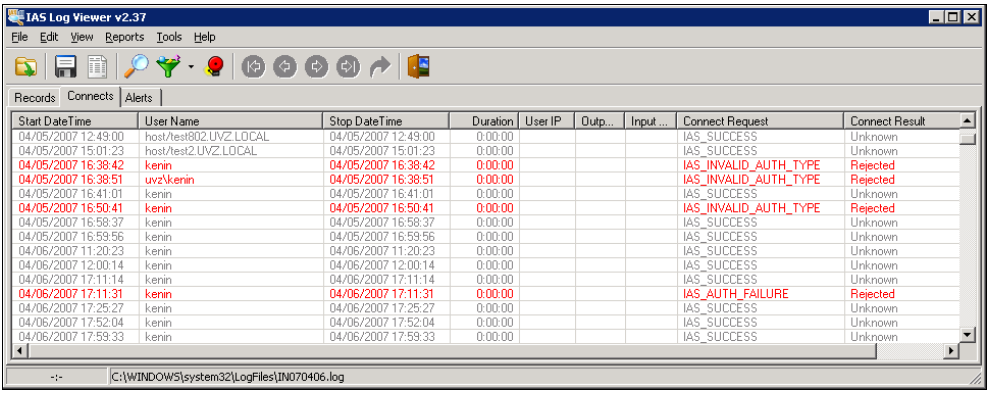


Рис. 9.4. Журнал подключений с использованием протокола 802.1*x*

Настройка клиентского компьютера

Для использования протокола 802.1*x* при подключении к локальной сети на компьютере должна быть запущена служба **Беспроводная настройка**. Только в этом случае в свойствах сетевого подключения появится третья вкладка, определяющая настройки протокола 802.1*x* (рис. 9.5). По умолчанию настройки предполагают использование для аутентификации именно сертификатов, так что никаких изменений данных параметров не требуется.

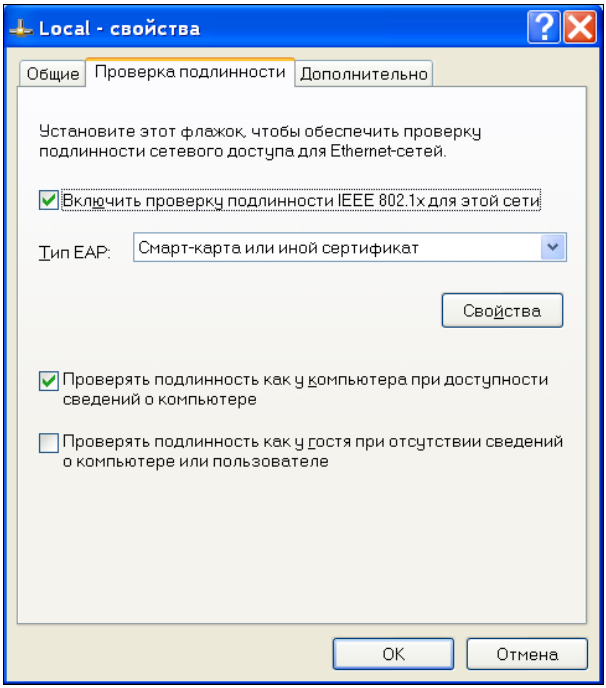


Рис. 9.5. Окно настройки протокола 802.1*x* на клиенте

Совет

Проще всего настроить данную службу на режим автоматического запуска с использованием групповой политики. Для этого следует открыть **Конфигурация компьютера | Конфигурация Windows | Параметры безопасности | Системные службы** и указать для службы **Беспроводная настройка** вариант автоматического запуска.

Следующим шагом необходимо проверить наличие сертификата, на основании которого предполагается осуществить открытие порта коммутатора. Для этого нужно открыть консоль управления сертификатами, обратив внимание на выбор правильного контейнера для просмотра. Так, если предполагается аутентифицировать компьютер, следует просматривать контейнер **Локальный компьютер**.

По умолчанию Windows настроен на использование сертификата пользователя, входящего в систему. Если вы предполагаете аутентифицировать *компьютер*, то нужно создать в ветви реестра `HKLM\Software\Microsoft\EAPOL\Parameters\General\Global` параметр `AuthMode` (тип `DWORD`) и установить его значение равным 2.

Совет

Этот параметр можно настроить централизованно в групповой политике, если воспользоваться советами, изложенными в *разд. "Редактирование параметров безопасности" главы 6*.

Настройка коммутатора

Настройки коммутаторов отличаются для различных вендоров. Приведем в качестве примера вариант настройки коммутатора Cisco.

В данном примере использованы настройки по умолчанию для портов службы RADIUS, не включены параметры повторной аутентификации и некоторые другие. Кроме того, в качестве гостевой VLAN (в нее будет помещен порт, если устройство не поддерживает протокол 802.1*x*) определена VLAN с номером 200, а в случае неудачной аутентификации устройство будет работать в VLAN с номером 201.

Сначала в конфигурации коммутатора создается новая модель аутентификации, указывающая на использование службы RADIUS:

```
aaa new-model
aaa authentication login default group radius
aaa authentication dot1x default group radius
aaa authorization network default group radius
```

Далее включается режим использования протокола 802.1*x* и определяются параметры RADIUS-сервера:

```
dot1x system-auth-control
radius-server host <IP-адрес> key xxxxxxxxxxxx
```

После чего для каждого интерфейса настраивается использование протокола 802.1*x*. В качестве примера выбран порт номер 11:

```
interface GigabitEthernet0/11
 switchport mode access
dot1x port-control auto
dot1x guest-vlan 200
 dot1x auth-fail vlan 201
```

Этих настроек достаточно, чтобы использовать на коммутаторе аутентификацию по протоколу 802.1*x*.

Безопасность приложений

Эту тему обычно "обходят" при обсуждении вопросов безопасности. Между тем, сколь бы хорошо ни защищалась операционная система, сколь бы пра-

вильно ни были написаны фильтры и политики брандмауэров, но если уязвимости прикладного программного обеспечения позволят получить доступ к защищенным данным, то все предпринятые усилия окажутся напрасными. В большинстве случаев мы можем только надеяться на то, что вопросам безопасности уделяется внимание на каждом этапе проектирования, что разработка контролируется профессионалами своего дела и т. д.

Прикладное ПО может явиться причиной утечки конфиденциальных данных не только из-за ошибок его разработки, но и просто благодаря недостаточному вниманию к документированным функциям. Так, файлы документов, подготовленные в программе Microsoft Word, кроме самого текста могут содержать и конфиденциальные данные[1], не предназначаемые для посторонних глаз: имена компьютера и пользователя, путь к сетевому принтеру, список редактировавших документ лиц, возможно, адреса их электронной почты и т. п. А если документ будет сохранен со включенными версиями или режимом исправлений, то партнер сможет проследить, например, позиции различных сотрудников по ценам, предлагаемым в документе, что отнюдь не будет способствовать принятию варианта, наиболее благоприятного для вашей организации.

Задача контроля прикладного ПО кажется практически неразрешимой. По мнению автора, наиболее рациональный выход — это использование ПО с открытым кодом, поскольку залогом его безопасности является независимая экспертиза.

Следует взять за правило не устанавливать на рабочие станции программы для изучения или тестирования и применять только минимально необходимый состав ПО. На предприятии должен быть организован единый фонд дистрибутивов, чтобы обеспечить установку программ на рабочие станции только из проверенного источника.

[1] Эти данные можно удалить вручную, если очистить соответствующие поля документа и выбрать нужный режим сохранения, однако удобнее использовать утилиту для удаления скрытых данных, доступную по адресу **http://www.microsoft.com/downloads/ details.aspx?familyid=144e54ed-d43e-42ca-bc7b-5446d34e5360&displaylang=en**.

План обеспечения непрерывности функционирования информационной системы

Вам очень поможет в работе, особенно при построении взаимоотношений с руководителями, наличие плана обеспечения непрерывности функционирования информационной системы.

Подобный план представляет собой перечень мероприятий, которые необходимо осуществить в случае отказа оборудования или в иной нештатной ситуации. В нем должно быть определено, например, можно ли перенести функции сервера в случае его отказа на другое оборудование? Допустимо ли заменить его другим сервером, службы которого не критичны и от них можно отказаться на время ремонта основного компьютера? Где должны храниться дистрибутивы, чтобы операция могла быть проведена дежурным оператором? Какова должна быть процедура восстановления данных? Описав все аварийные ситуации и пути их устранения, вы сможете рассчитать ожидаемое время восстановления системы в каждом случае отказа.

Если такой план будет утвержден руководством, то, с одной стороны, вы получите защиту от неоправданных требований немедленного восстановления работы, поскольку для каждой ситуации период восстановления будет четко оговорен. С другой стороны, этот план станет инструкцией, что нужно делать в аварийной ситуации.

Любой план обеспечения непрерывного функционирования предполагает наличие резервной копии данных. Создание резервной копии — это единственный способ, гарантирующий возможность полного восстановления данных. Получить такую копию можно различными операциями. Администраторы иногда используют свои сценарии, например, реализующие необходимые параметры копирования данных в архив с помощью опций архиваторов. Но при разветвленной структуре данных правильно настроить подобное копирование становится затруднительно. Приходится анализировать большое количество файлов на предмет наличия изменений, останавливать на время создания резервных копий работающие с этими данными программы (поскольку иначе невозможно получить доступ к открытому файлу) и т. п. Поэтому в условиях офисов применяются специальные программы резервного копирования, чаще всего основанные на технологии теневого копирования.

Volume Shadow Copy

Начиная с Windows 2003 Server, в системе присутствует возможность создания "снимков" файлов в определенный момент времени, даже если файл от-

крыт каким-либо процессом. Данная служба позволяет корректно сохранять в том числе и копии файлов баз данных (например, MS Access, MS SQL), базы почтовых серверов и т. п.

Примечание

Возможность теневого копирования добавлена и в персональную операционную систему Vista. Если при использовании технологии на сервере опция включалась только для папок, предоставленных для совместного использования, то Vista позволяет настраивать создание теневых копий на локальном диске.

Кроме отсутствия пропуска файлов при проведении операции, Volume Shadow Copy (VSC, теневое копирование) позволяет администраторам настроить сетевые папки на хранение *нескольких версий файлов*. Для сетевой папки может быть включено расписание, по которому система будет создавать мгновенные снимки имеющихся в папке файлов. При необходимости возврата к предыдущей версии файла пользователи смогут восстановить

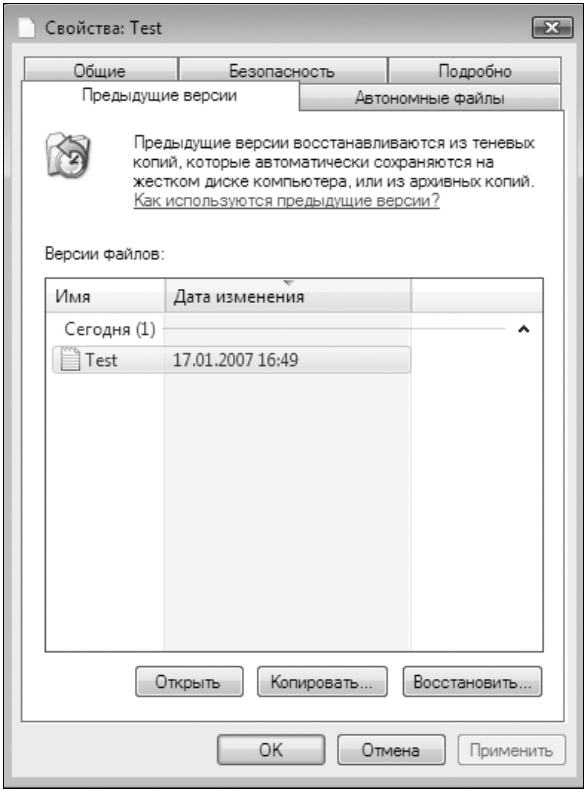


Рис. 9.6. Список существующих теневых копий файла

копию, сохраненную в требуемый период, причем на создание таких "снимков" затрачивается крайне незначительный объем дискового пространства.

Для включения данной возможности достаточно установить эту опцию в свойствах сетевой папки и настроить желаемое расписание.

Самостоятельно восстановить предыдущую версию файла пользователи могут при помощи клиентской части VSC, файл установки которой находится в папке сервера System32\Clients\twclient\<*платформа_клиента*>. VSC добавляет к свойствам файла дополнительную вкладку, отображающую наличие версий файла и позволяющую выполнить восстановление данных (рис. 9.6).

Примечание

Восстановить удаленный файл с помощью VSC можно, если создать одноименный файл в исходной папке и выбрать в меню его свойств восстановление предыдущей версии.

Устройства хранения данных

Постоянное совершенствование жестких дисков привело к тому, что на сегодня они стали самым оптимальным устройством для хранения данных резервного копирования. По сравнению с другими вариантами (стримерами, различными библиотеками и т. п.) жесткие диски обеспечивают низкую удельную стоимость хранения единицы данных, имеют высокую скорость записи и чтения данных, позволяют производить произвольный доступ к информации[1].

В малых и средних организациях объем данных, для которых необходимо создавать резервные копии, редко превышает несколько сотен гигабайт, что не превышает емкости одного или нескольких жестких дисков, объединенных для повышения скорости записи/чтения в программный RAID. Поэтому оптимальным способом хранения резервных копий для небольших организаций является использование обычной дисковой подсистемы компьютера. Конечно, необходимо разместить соответствующий системный блок в специальном месте, чтобы исключить одновременное повреждение как серверов, так и устройства резервного копирования (например, в случае пожара в помещении).

Типы операций резервного копирования

При периодическом резервном копировании информации не имеет смысла каждый раз сохранять ту часть данных, которая не подвергалась изменению.

[1] В отличие, например, от стримеров, для прочтения конкретного участка данных, с которых может потребоваться перемотка магнитной ленты.

Поэтому было разработано несколько методов записи данных, отличающихся длительностью операций резервного копирования и восстановления.

- **Normal backup.**

  При этом копировании сохраняются все данные, определенные настройками программы. Преимущество способа состоит в том, что вся информация может быть восстановлена за одну операцию. Недостаток заключается в значительном объеме постоянно записываемой информации и, следовательно, увеличенной длительности самой операции резервного копирования и повышенном износе жестких дисков (магнитных лент стримера).

- **Copy backup.**

  Этот способ создает резервную копию всей информации, но не меняет в исходных файлах архивные биты. Используется для создания — при необходимости — промежуточной полной резервной копии данных без внесения каких-либо изменений в схемы резервного копирования.

- **Differential backup.**

  При данном способе каждая операция резервного копирования сохраняет только те данные, которые были изменены с момента последней операции Normal backup. То есть при ежедневном копировании на устройство хранения будут переноситься в первый день данные, измененные за прошедшие сутки, во второй день — все данные, измененные за последние два дня, в третий — за три дня и т. д. Преимущество способа — удобство (оперативность) восстановления данных. Нужны только данные от операции полного резервного копирования и последней операции Differential backup. Недостаток — больший объем ежедневного копирования (по сравнению с методом Incremental backup).

- **Incremental backup.**

  Этот вариант предполагает копирование при каждой операции всех данных, которые изменились с момента последней операции Incremental backup. То есть если вы используете ежедневное копирование, то будут записываться только данные, которые изменены за последний день. Преимущество способа — самый низкий объем копируемых данных и самое быстрое завершение операции. Недостаток — после аварии необходимо сначала восстановить информацию из полной резервной копии, а потом — *последовательно из каждой копии*, созданной методом Incremental backup.

На практике резервное копирование предполагает регулярное выполнение операций полного резервного копирования, а в промежутках — проведение резервного копирования вариантом Differential backup или Incremental backup. Конкретная стратегия (периодичность копирования, типы операций) выбирается индивидуально для каждой организации. При этом в расчет принимают-

ся такие параметры, как общий объем информации, объем ежедневно изменяемых данных, емкость устройств для хранения резервных копий, необходимость хранения определенного числа копий данных на различные моменты времени, максимально допустимый объем потери информации и т. п.

Примечание

Главное правило при планировании резервного копирования — не смешивать различные способы резервного хранения, иначе существует опасность запутаться в последовательности операций восстановления.

Объекты резервного копирования

В целях обеспечения сохранности данных желательно иметь минимум две копии информации, иначе выход системы из строя во время резервного копирования приведет к потере как основной информации, так и единственной ее копии, с которой в этот момент будет проводиться работа.

При запуске встроенной программы резервного копирования мастер операций позволяет выполнить пошаговые настройки. При работе в ручном режиме в настройках программы архивации данных необходимо указать папки, для которых следует выполнить резервное копирование: это может быть как весь диск, так и только определенные каталоги. При этом администратору следует учесть, что многие серверные программы (такие как почтовый сервер MS Exchange, сервер баз данных MS SQL Server и т. д.) имеют собственные опции резервного копирования, часто позволяющие настроить его более оптимально, чем резервное копирование всех данных диска. Так, указанные выше программы имеют возможности выборочного резервного копирования (сохранения только выбранных администратором баз данных), настройки Differential backup и Incremental backup для отдельных баз. В свою очередь резервная копия программы "1С", выполненная встроенными средствами, занимает на порядок меньше места на диске, чем копирование настроек пользователей и баз данных системными средствами.

Следует также учитывать, что до Windows 2003 Server программа резервного копирования не могла сохранять *открытые файлы*, т. е. если файл был открыт другой программой, то он не сохранялся в резервной копии. Поэтому почтовые базы, базы данных SQL и т. п. могли быть сохранены только при помощи встроенной функциональности резервного копирования.

Кроме папок жесткого диска, в настройках операции присутствует возможность резервного копирования *состояния системы* (system state).

Примечание

Для получения возможности восстановления работоспособности операционной системы следует включать данную опцию при резервном копировании.

При копировании состояния системы сохраняются[1]:

- реестр системы;
- база регистрации классов COM+;
- системные и загрузочные файлы;
- файлы, подпадающие под защиту File Protection System;
- база данных службы каталогов (AD database, если компьютер является контроллером домена);
- папка SYSVOL (на контроллере домена);
- база данных сервера сертификатов[2] (если компьютер является центром сертификации);
- конфигурационная информация кластера (если сервер входит в состав кластера);
- метабаза IIS[3] (если на компьютере работает Web-служба).

Automated System Recovery

Программа резервного копирования содержит специальную возможность — Automated System Recovery (ASR), предназначенную для автоматического восстановления операционных систем. Чтобы воспользоваться ASR, необходимо запустить мастер программы архивирования данных, который выполнит резервное копирование системы[4] (в том числе всего содержимого системного и загрузочного дисков) и сформирует дискету, содержащую настройки для восстановления.

После этого в случае выхода системы из строя достаточно начать загрузку с установочного компакт-диска и нажать клавишу <F2> при появлении соответствующего запроса. Далее, считав с этой дискеты параметры резервного копирования, система установит минимально работоспособную версию Windows и произведет восстановление файлов и данных, созданных во время резервного копирования.

---

[1] Администратор не имеет возможности выбрать для резервного копирования только часть этих параметров. Посмотреть состояние системы можно, если выполнить восстановление данных в другую папку.

[2] Может быть выполнено резервное копирование (восстановление) только сервера сертификатов с помощью его оснастки управления *(см. главу 12, разд. "Резервное копирование центра сертификации")*.

[3] Может быть выполнено резервное копирование только метабазы сервера IIS с помощью его оснастки управления.

[4] Мастер производит полное резервное копирование (Normal backup).

ASR является самым быстрым штатным способом восстановления работоспособности операционной системы при минимальном количестве ручных операций. Основное неудобство связано с необходимостью ручного создания дискеты с записью состояния. В результате на практике дискета создается или один раз, или с очень большими промежутками от одной операции до другой, и администратору приходится восстанавливать актуальное состояние системы, используя данные "обычных" операций резервного копирования.

Копирование образов диска

Недостатком "классических" средств резервного копирования является восстановление данных на *работающую* систему: в случае отказа критичных служб задержки на выполнение установки самой операционной системы часто бывают недопустимы. В таких ситуациях может помочь создание *копий жестких дисков* системы.

Программы копирования дисков позволяют создать образ диска и восстановить систему за одну операцию. В зависимости от объема диска восстановление может занять разное время; для "средней" рабочей станции оно составляет около 20 минут.

На рынке представлено несколько продуктов данного класса.

Paragon Drive Backup позволяет создать копию диска непосредственно во время работы компьютера. Кроме того, можно планировать создание резервных копий (в том числе и дифференциальных), просматривать образ диска и восстанавливать только отдельные файлы. Поскольку в составе программы практически не представлены средства работы с образом диска, программу целесообразно использовать для восстановления с "родного" образа.

Продукты Symantec (Norton) давно популярны у администраторов. Программа Symantec Ghost Solution Suite позволяет не только создавать образы дисков, но и редактировать их. В результате можно обновлять в файлах образов отдельные компоненты, менять конфигурацию системы и т. д. В качестве дополнительных возможностей программы следует отметить функции инвентаризации программного обеспечения и аппаратных средств, встроенные средства переноса настроек пользователей, улучшенные настройки планирования операций.

Symantec Ghost Solution Suite может осуществлять одновременное развертывание нескольких систем с использованием многоадресной рассылки. В целях уменьшения влияния данного приложения на работу остальных систем для операций можно задавать максимально допустимый процент использования полосы пропускания сети. Недостатком является необходимость перезагрузки компьютеров при создании образов диска. Система автоматически перегружается в специальную DOS, автоматически запускается режим копирова-

ния, после завершения которого происходит повторная перегрузка в рабочую среду. Для большинства сетевых адаптеров настройка DOS для копирования происходит автоматически с использованием встроенного списка драйверов, но в отдельных случаях могут потребоваться ручные операции.

Примечание

Решение от Symantec позволяет создать образ диска и компьютера, работающего в среде Linux.

Acronis True Image (рис. 9.7) позволяет создать образ работающей системы без загрузки специальной среды. Для этого используется функционал теневых копий.

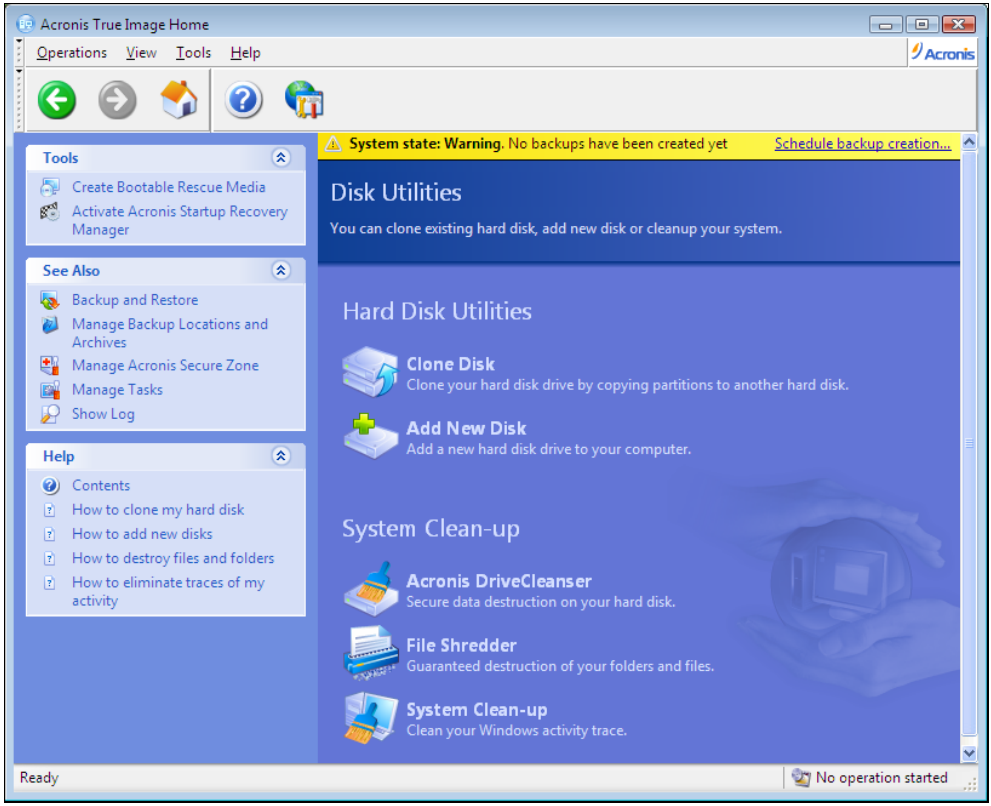


Рис. 9.7. Программа Acronis True Image

Продукт интуитивно прост, легко позволяет централизованно установить приложение, скопировать диск, отредактировать полученный файл образа и выполнить восстановление в случае необходимости. Следует отметить, что

средства редактирования образа позволяют заменить драйверы системы, в результате чего образ диска можно восстанавливать на систему *отличающейся конфигурации*. Имеются возможности восстановления и отдельных файлов из образа диска.

Среди особенностей программы отметим также возможность копирования диска локально в скрытый раздел. Это позволит пользователю самостоятельно восстанавливать отдельные файлы (естественно, сам жесткий диск не должен полностью выйти из строя).

В отличие от комплекта Symantec в данном программном обеспечении практически отсутствуют средства, облегчающие групповые операции копирования и восстановления при значительном количестве компьютеров в организации. С другой стороны, восстановление системы при помощи Acronis происходит существенно быстрее. Эти два продукта составляют друг другу конкуренцию.

Необходимые права для операции backup

При выполнении операции резервного копирования в копию данных должна быть включена вся имеющаяся в системе информация, в том числе те данные, для которых средствами операционной системы наложены ограничения доступа. Поэтому при выполнении операции резервного копирования используются учетные записи пользователей, обладающих *возможностью обхода разрешений файловой системы для данной операции*[1].

По умолчанию такими правами обладают учетные записи операторов резервного копирования системы. При необходимости администратор может предоставить данные права любой учетной записи, включив ее в группу операторов резервного копирования.

Примечание

В целях обеспечения должного уровня безопасности желательно включить протоколирование использования прав резервного копирования, иначе операторы резервного копирования смогут практически бесконтрольно получать доступ к любым данным. Например, обладая такими правами, с помощью утилиты из состава Resource Kit можно скопировать информацию, доступ к которой ограничен по соображениям безопасности и на которую отсутствует даже право чтения.

Данные резервного копирования содержат защищенную информацию системы, поэтому хранение резервных копий должно обеспечиваться теми же мерами безопасности, которые предусмотрены для эксплуатации самих контроллеров домена. Кроме того, при выполнении операции резервного копи-

[1] А для восстановления — правами перезаписи соответствующих объектов.

рования рекомендуется предоставлять допуск к данным для их восстановления только администраторам системы.

Восстановление данных

При проведении резервного копирования программа сохраняет в протоколе параметры созданных копий, поэтому для восстановления достаточно выбрать в окне программы необходимый файл. Если такая информация не сохранилась, то следует сначала провести *каталогизацию* файла резервной копии, для чего в меню **Сервис** выбрать команду **Каталогизировать архивный файл** и указать соответствующий файл, после чего можно выполнить восстановление обычным способом.

В общем случае, сначала необходимо провести восстановление системы из полной резервной копии (вариант Normal backup), после чего восстановить последние изменения. В зависимости от выбранной стратегии резервного копирования следует восстановить либо последовательно все Incremental-копии, либо только последнюю Differential-версию.

Примечание

Поскольку операции резервного копирования данных различных программ имеют некоторые индивидуальные особенности, крайне желательно хотя бы раз провести тестовое восстановление системы из резервной копии. Это позволит приобрести опыт и существенно сэкономит время при восстановлении серверов в реальных условиях производства.

Операция восстановления данных может быть использована при замене оборудования компьютера. В этом случае следует установить на новом компьютере операционную систему и восстановить на нее имеющиеся резервные копии. Программа корректно сохранит необходимые драйверы, отвечающие за взаимодействие с аппаратной частью новой системы, и восстановит все прикладные данные.

Резервное копирование и восстановление зашифрованных данных

Зашифрованные данные можно включать в операции резервного копирования обычным образом. При этом создавать резервные копии можно на любых носителях, в том числе и на логических дисках с файловой системой FAT, которая не поддерживает возможность шифрования данных.

В виде файла резервной копии зашифрованные данные могут быть перенесены с одного компьютера на другой, однако восстановить их можно только на диски с файловой системой NTFS, иначе их данные невозможно будет прочесть.

Таким образом, использование операции резервного копирования является способом, с помощью которого зашифрованные данные могут быть без повреждений перенесены на другой компьютер, если их нельзя расшифровать "на месте". Такой перенос может оказаться необходим, например, для получения доступа к зашифрованным данным уволившегося сотрудника и наличия только централизованного сертификата восстановления.

Восстановление контроллера домена

Восстановление контроллера домена из резервной копии имеет несколько особенностей. Во-первых, такое восстановление можно провести только в специальном режиме — Directory Services Restore Mode, который выбирается при старте системы[1].

Вторая особенность связана с тем, что база службы каталогов использует *multimaster replication*. Поскольку изменения могут вноситься на любом контроллере домена, то система по специальному алгоритму[2] определяет контроллер с наиболее "актуальными" данными и восстанавливает с него информацию на текущий контроллер. Иными словами, данные службы каталогов восстановленного контроллера будут автоматически заменены на последнюю версию, если таковая присутствует в домене.

Бывают ситуации, когда администратор желает восстановить службу каталогов или ее часть в том состоянии, как *она была сохранена в резервной копии*, что может потребоваться, например, при случайном удалении каких-либо объектов AD. Эти операции выполняются в специальном режиме — **Authoritative Active Directory Restores**, который доступен только при загрузке в варианте восстановления службы каталогов. Загрузив утилиту NTDSUTIL, необходимо перейти в режим восстановления, выполнив команду `authoritative restore`. Далее можно восстановить данные командой `restore database`. При необходимости сохранения только части базы данных службы каталогов следует использовать команду с указанием восстанавливаемых объектов:

```
restore subtree ou ouname,dc=dcname,dc=dcname
```

Затем необходимо перезагрузить контроллер в нормальном режиме.

---

[1] Для входа в этот режим используется специальный пароль, задаваемый при установке контроллера домена. До начала операции следует убедиться, что вы знаете этот пароль. В Windows 2000 для установки данного пароля можно использовать утилиту Setpwd.exe (из папки system32), в Windows Server 2003 пароль можно сменить с помощью утилиты `ntdsutil` (команда `Set DSRM Password`).

[2] Служба каталогов использует для всех объектов AD специальные счетчики (update sequence numbers, USN), которые увеличиваются при внесении каждого изменения. Более актуальными считаются данные с наибольшим значением USN. При равных значениях счетчика сравнивается время внесения изменений и сохраняются самые последние данные.

Создание копий информации отдельных служб

Часто администратору необходимо восстановить данные настройки только отдельных служб системы. Например, для переноса на новый компьютер. Часть таких операций (создание копии центра сертификации, копии метабазы IIS) мы уже упоминали. Но этим имеющиеся возможности не ограничиваются.

Сохранение настроек DHCP

Резервное копирование данных DHCP-сервера система производит автоматически. По умолчанию база DHCP-сервера сохраняется по пути, указанному в параметре `BackupDatabasePath` ветви реестра `HKLM\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters`. Обычно это папка %SystemRoot%\System32\DHCP\Backup. Резервное сохранение производится с интервалом в час, и при обнаружении проблем с базой система восстанавливает ее также автоматически.

Для ручного восстановления базы на этот же сервер достаточно остановить службу DHCP и переписать файлы базы[1].

Сохранение настроек DNS

Если зона Интернета обслуживается сервером DNS и ее настройки хранятся в виде файла, то, во-первых, можно скопировать сам файл зоны (его содержимое идентично для MS и не-MS DNS-серверов); во-вторых, оснастка DNS позволяет скопировать эти настройки в текстовый файл, который может быть использован для создания зоны на другом сервере DNS.

Сохранение настроек DFS

Хотя для управления структурой DFS используется графическая оснастка, в системе присутствует команда, позволяющая из командной строки добавлять и удалять ссылки на сетевые ресурсы структуры DFS. С помощью этой команды можно создать пакетный файл, который автоматически воссоздаст структуру DFS:

```
dfscmd /view \\dfsname\dfsshare /batch > filename.bat
```

Сохранение данным способом структуры DFS имеет особое значение для корней, созданных на рядовых серверах, поскольку такие корни DFS (в отличие от доменных корней DFS) не сохраняются в структуре службы каталогов и их настройка может быть утеряна после сбоя компьютера.

---

[1] Система также автоматически сохраняет параметры реестра, относящиеся к DHCP-серверу. Эти файлы резервных копий находятся в той же папке, что и резервные копии базы DHCP.

Сохранение реестра системы

Отдельные ветви реестра системы можно сохранять в программе regedit, используя операцию экспорта (и импорта — в случае восстановления данных). Для этого нужно выделить соответствующую ветвь и выбрать желаемую команду меню.

Примечание

В сценариях можно использовать чтение/запись реестра с помощью команд Visual Basic или WMI. В пакетных операциях для импорта/экспорта значений реестра из командной строки предназначена команда `reg` (справка `reg /?`).

Сохранить раздел таким способом невозможно. С этой целью рекомендуется использовать штатную программу резервного копирования и проводить операцию сохранения состояния системы.

Примечание

В Windows 98/ME реестр системы мог быть сохранен и восстановлен с помощью специальной утилиты Scanreg.exe (DOS-версия) или Scanregw.exe (Windows-версия).

Системы непрерывного копирования данных

Традиционно резервное копирование данных выполняется по предустановленному графику. Очевидно, что в случае возникновения аварийной ситуации может быть произведено восстановление только до последнего момента сохранения. Все изменения, внесенные после этого события, будут потеряны. Для некоторых информационных систем объем потери должен быть минимизирован.

В этом случае необходимо внедрить одну из систем *непрерывной защиты данных* (Continuos Data Protection, CDP).

В настоящее время на рынке представлены продукты как гигантов ИТ-индустрии: Backup Exec от Symantec (**www.symantec.com**), System Center Data Protection Manager от Microsoft (**www.microsoft.com**), Tivoli Continuous Data Protection от IBM (**www.ibm.com**), так и системы менее крупных компаний: WANSynchHA Enterprise Rewinder от XOsoft (**www.xosoft.com**), InControl от FilesX (**www.filesx.com**), Availl CDP от Availl (**www.availl.com**) и др. Стоимость решений варьируется от тысячи долларов (System Center Data Protection Manager, Backup Exec) до нескольких десятков тысяч (InControl).

На что следует обратить внимание при выборе решения. В первую очередь, уточните, в каком режиме сохраняются данные. Многие продукты, отнесенные производителями к классу CDP, сохраняют данные в фиксированные

моменты времени, причем промежуток между сохранениями может достигать от минут до часа. Проверьте, какую детализацию допускает тот или иной продукт.

Второе. Большинство продуктов CDP ориентировано на файловые серверы, тогда как в реальной системе непрерывная защита должна быть реализована для данных почтового сервера, баз данных и т. д. Перед приобретением продукта следует убедиться в наличии такой опциональности.

Не все системы поддерживают работу с кластером, позволяют восстановить систему с "голого" железа или удобно просмотреть сохраненные данные. Различная функциональность реализована и при копировании данных удаленного филиала (например, регулирование занимаемой для операции полосы пропускания канала Интернета).

Таким образом, выбор системы CDP следует осуществлять после тщательного анализа и сравнения различных вариантов.

Защита от вредоносных программ и вторжений

В обязанности администратора входит защита системы от самораспространяющегося кода при помощи антивирусных средств, выявление и предупреждение внедрения сторонних кодов (троянов и руткитов), предупреждение использования ошибок в операционной системе и прикладных программах, позволяющих злоумышленнику выполнять на системе некоторые операции.

Современные программы защиты компьютера приобретают комплексный характер. На рис. 9.8 представлена программа Symantec Endpoint Protection, которая помимо функций антивирусной защиты включает современный межсетевой экран и средства обнаружения атак и вторжений. Программа способна обнаруживать клавиатурные шпионы; блокировать хосты, осуществляющие атаки; маскировать операционную систему (подменять типовые ответы на контрольные пакеты IP). В ней содержатся опции, включавшиеся ранее только в специализированные программы, например, защита от подмены MAC-адреса, интеллектуальный контроль протоколов DHCP, DNS, обнаружение руткитов и т. д.

Антивирусные программы

Наличие мер *актуальной* антивирусной защиты обязательно сегодня для каждого компьютера. По различным оценкам, вред, приносимый вирусами, исчисляется десятками миллионов долларов. Несмотря на все профилакти-

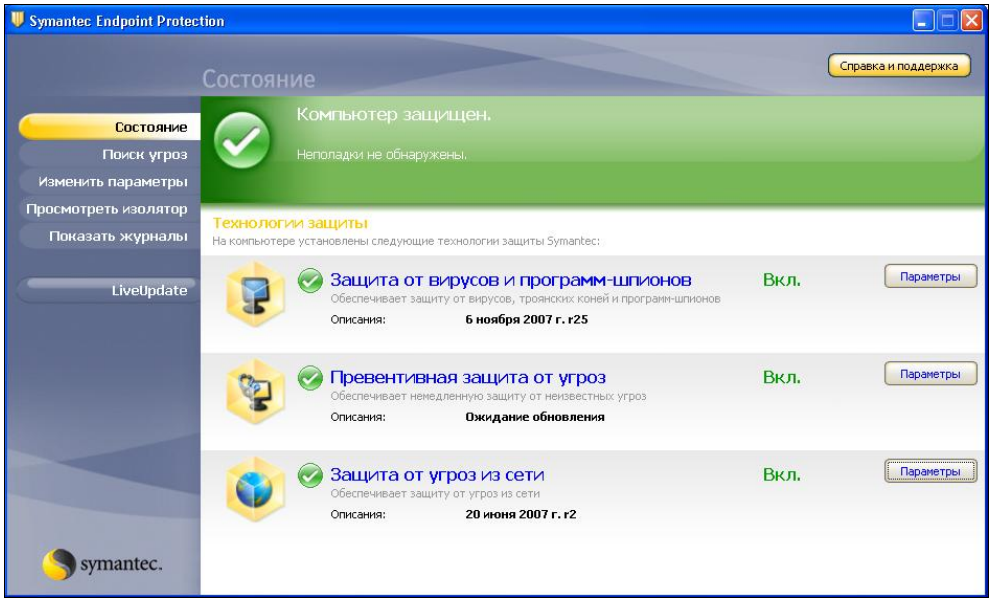


Рис. 9.8. Интерфейс программы Symantec Endpoint Protection

ческие меры, ежегодно заражению подвергается в среднем около 9% компьютерного парка, а количество постоянно функционирующих сетей, объединяющих зараженные компьютеры, управляемые злоумышленниками, превышает 10,5 тысяч.

Примечание

Я не случайно акцентировал внимание на *актуальности* защиты. Типовой ошибкой является установка антивирусной программы с последующим необновлением вирусных баз. Такая ситуация не только бессмысленна, т. к. не защищает от вторжения вирусов, но и вредна, поскольку создает иллюзию защищенности системы.

Индивидуальные версии антивирусных программ целесообразно использовать только в очень малых сетях. Корпоративные решения позволяют администратору снизить объем загружаемых обновлений (обновления будут получены из Интернета только один раз, а потом просто распространены по локальной сети), централизованно настроить опции антивирусной защиты (например, установить частоту загрузки обновлений, исключить из проверки некоторые типы файлов и т. п.), получать статистические данные по пользовательским системам и т. п.

Следует особо тщательно подходить к выбору программ, предназначенных для антивирусной защиты контроллеров домена, почтовых серверов и т. п. — часть файлов в таких системах должна быть исключена из проверки. При

этом некорректная настройка антивирусной защиты может не только снизить производительность системы, но даже и нарушить ее функционирование.

Во избежание излишних проблем желательно использовать программы, сертифицированные для соответствующих применений. Список таких продуктов можно получить, например, по адресу **http://cert.veritest.com/CfWreports /server/.**

Примечание

Сравнение антивирусных программ по проценту обнаружения вирусов во многом имеет рекламный характер. Продукты известных фирм практически идентичны по своим функциональным возможностям.

Установка антивирусной защиты

Установка корпоративной антивирусной системы обычно не представляет сложности. Первоначально устанавливается сервер, производится настройка основных опций (частоты обновления, действий при обнаружении вируса, исключений и т. п.), после чего инсталлируются клиентские части системы, которые автоматически конфигурируются в соответствии с параметрами защиты предприятия.

В условиях предприятия редко используют установку клиентской программы путем ее запуска из определенной папки. Обычно установка проводится централизованно, из консоли управления с правами доменного администратора. Другой вариант — установка клиентских компонентов через групповые политики.

В текущей работе администратору необходимо только периодически следить за функционированием системы и за тем, чтобы на вводимые в эксплуатацию компьютеры обязательно были установлены клиентские компоненты. Последнее обычно вызывает наибольшие затруднения, поскольку в средних сетях администратору не всегда удается отследить наличие компьютера без антивирусной защиты[1].

К организации антивирусной защиты следует подходить творчески. Например, поскольку наличие антивирусных программ негативно сказывается на производительности систем, то специализированные серверные системы, к которым нет доступа пользователей для записи файлов, часто можно исключить из числа защищаемых. Или, учитывая, что основной объем вирусов на

[1] Такая ситуация может возникнуть если, например, пользователь, имеющий административные права, отключил службу антивирусной защиты или подключил к системе личный ноутбук, а также после переустановки операционной системы. В этих случаях можно использовать распространение антивирусных программ через групповую политику и централизованно фиксировать параметры запуска режима проверки *(см. главу 6, разд. "Политики по установке программного обеспечения")*.

сегодня распространяется через электронную почту, имеет смысл установить антивирусную программу, которая осуществляет проверку всей приходящей в организацию почты непосредственно на почтовом сервере — *дополнительно* к проверкам на пользовательских системах.

График обновлений антивирусных баз

Опыт последних вирусных пандемий свидетельствует о том, что они достигают своего пика уже на второй, максимум третий день после начала распространения вирусов. Обновления антивирусных баз обычно появляются уже через несколько часов после обнаружения вируса, поэтому в условиях сети организации имеет смысл настроить график обновлений *не реже одного раза в сутки*.

Внимательность пользователя

Уровень безопасности системы может быть существенно повышен, если пользователь в своих действиях будет учитывать потенциальную возможность заражения вирусом.

Прежде всего, необходимо приучить пользователей к мысли, что работать без антивирусной программы и с устаревшими данными о вирусах — означает постоянно рисковать здоровьем своего компьютера и результатами работы.

Как показывает практика последних компьютерных пандемий, электронная почта является самым быстрым и эффективным способом распространения вирусов. Поэтому следует постоянно проводить профилактическую работу с пользователями, обучая их особым мерам предосторожности:

- использовать оформление письма в виде "только текст", не применяя оформление по стандарту HTML: неформатированное послание принципиально не может содержать никакого опасного кода;
- приучать пользователей не открывать любые вложенные в письмо файлы. Во-первых, вложенные файлы могут содержать исполняемые коды или определенные последовательности, использующие ошибки программ и позволяющие организовать атаку на компьютер: например, одна из критических уязвимостей систем на основе Windows связана с возможностью исполнения кода при открытии графических файлов в формате JPEG. Во-вторых, при обычной пересылке корреспонденции система не проверяет параметры отправителя и сохранность письма по пути следования, что позволяет легко подделать письмо и представить его содержимое якобы вполне безопасным. Если возникает необходимость отправки вложения, то следует предварительно письмом в формате "только текст" предупредить адресата о предстоящей отправке.

Чем меньше лазеек для создания вирусов оставляют разработчики программного обеспечения, тем больше эти вирусы используют особенности психологии. Например, в последний месяц мой почтовый ящик буквально был атакован сообщениями о якобы полученной онлайновой открытке, которую можно прочесть по приведенной ссылке. Естественно, что указывала она совсем не на систему электронных поздравлений.

На чисто человеческих слабостях основывается еще один тип вирусов — *вирусы-мистификации*. Обычно это письма электронной почты, не содержащие никакого вируса, но составленные так, что мы сами отправляем их копии в несколько новых адресов. А способность к размножению — это основной признак вируса. Такое письмо может содержать, например, сведения о новом вредоносном вирусе, о котором следует срочно предупредить своих знакомых. Другой классический пример — приглашение поучаствовать в рекламной акции за какое-либо вознаграждение и т. п.

Такие мистификации появляются достаточно часто. Администратору следует оперативно пресекать попытки распространения подобных писем пользователями своей сети, добиваясь сообщения о таком инциденте *только* на адрес администратора. Проверить, является ли это письмо мистификацией или нет, можно на любом из официальных сайтов, например на **www.ciac.com**, **www.sarc.com**.

Лечение вирусов

Невозможно полностью исключить вероятность заражения компьютера вирусом. Если компьютер поразил вирус, то следует сначала обновить базу данных антивирусной программы, если она установлена. В большинстве случаев после этого она сама сможет обезвредить вирус.

Некоторые вирусы блокируют запуск антивирусных программ (если вирус уже внедрился в систему с устаревшей базой данных о вирусах). В этом случае нужно постараться выяснить название вируса, загрузить утилиту, которая позволит устранить внесенные им в систему изменения, после чего можно будет загрузить обновления и выполнить полную проверку системы. Для установления имени вируса следует воспользоваться сканированием системы, например, с дискеты или посредством онлайнового антивирусного сервиса[1]. При работе в составе локальной компьютерной сети можно воспользоваться

[1] Практически все крупные производители антивирусных продуктов создали подобные службы. Например, Symantec Security Check (**http://security.symantec.com/sscv6/default.asp?langid=ie&venid=sym**), Trend Micro (**http://housecall.trendmicro.com/housecall/start_corp.asp**), Panda (**http://www.pandasoftware.com/activescan/com/activescan_principal.htm**), RAV Antivirus (**http://www.ravantivirus.com/scan/**) и т. д.

также возможностью антивирусных программ осуществлять проверку сетевых ресурсов.

Если антивирусная программа не установлена, то следует первоначально провести проверку на вирусы, используя заведомо "чистое" программное обеспечение. Как правило, все антивирусные пакеты имеют версии программ для сканирования и лечения системы, которые можно запустить в режиме командной строки. Эти версии можно бесплатно загрузить с соответствующего сайта изготовителя. При проверке необходимо быть уверенным, что в памяти компьютера отсутствуют вирусы. Для этого система должна быть загружена, например, с заведомо чистой дискеты или с компакт-диска.

После ликвидации вирусов нужно установить антивирусную программу и обновить ее данные о вирусах.

Защита от вторжений

В настоящее время только антивирусной программы недостаточно для защиты компьютера. Антивирусные программы проверяют файлы, сохраняемые на носителях, и контролируют почтовые отправления. Но они не могут предотвратить эпидемии, вызываемые нарушениями в работе служб компьютера. Черви, распространяющиеся в виде пакетов данных, не обнаруживаются классическими системами контроля.

Яркий пример такой пандемии — интернет-червь "Slammer" (январь 2003 года). Небольшой пакет, всего 376 байт, принятый системой с MS SQL Server, приводил к тому, что компьютер начинал рассылать аналогичные пакеты с огромной скоростью по случайным адресам. В результате через некоторое время каналы связи оказались просто не в состоянии пропустить такой объем данных, и функционирование Интернета во многих сегментах практически было парализовано. Этот червь поразил более 90% узлов, которые имели соответствующую уязвимость, менее чем за 10 минут. При этом число зараженных хостов Интернета удваивалось каждые 8,5 секунды.

В настоящее время последние версии комплексных программ защиты[1] стали включать модули, контролирующие передаваемые по сети данные. Если такой модуль обнаруживает сигнатуру, которая применяется для атак с использованием ошибок операционной системы или прикладных программ, то он блокирует соответствующую передачу данных.

Так же, как и антивирусные базы данных, состав данных сигнатур нуждается в постоянном обновлении с центрального сервера. Обычно такое обновление осуществляется единой операцией.

---

[1] Как правило, такие программы соединяют в себе возможности антивирусной защиты и межсетевого экрана.

Защита от постороннего кода

Программы-шпионы. "Троянские кони"

В Интернете широко распространена практика установки на компьютер пользователя определенных программ без его ведома. Иногда их действия просто надоедливы (например, перенаправление стартовой страницы обозревателя на определенные ресурсы Сети в целях рекламы последних), иногда такие программы собирают информацию с локального компьютера и отсылают ее в Сеть (например, о предпочтениях пользователя при посещениях сайтов или передача злоумышленнику данных, вводимых пользователем при работе с сайтами интернет-банков и т. п.). В последнее время такие программы стали использоваться для подготовки вирусных пандемий, для пересылки спама, для внедрения средств удаленного контроля компьютером и т. п.

Обнаружить данную программу весьма сложно, поскольку ее действия внешне никак не отражаются на обычной работе пользователя. В то же время можно предотвратить внедрение таких программ, правда, путем существенного увеличения административных операций, например, введением в групповых политиках организации запретов на запуск неизвестных программ. В этом случае неблагонадежные программы будут блокированы, но существенно возрастет трудоемкость разработки политик и резко увеличится количество обращений рядовых пользователей, предполагающих использовать компьютеры для игр, обучения и т. п.

Хотя функции блокирования троянских кодов включены во многие современные антивирусные программы, администратор может легко найти в Интернете утилиты, специализированные только на решении данной проблемы. В качестве примера можно привести Ad-aware от компании LavaSoft, которую можно найти на сайте **http://www.lavasoftusa.com/.** Такие программы ориентированы на поиск следов троянов (ключей в реестре, записей на жестком диске и т. п.) и особенно полезны при выезде администратора в другую организацию для осуществления технической поддержки. Объем файлов установки позволяет быстро загрузить их из Сети и оперативно очистить компьютеры клиентов от вредоносных кодов в случае обнаружения непредвиденных действий и т. п.

В качестве превентивных мер можно рекомендовать чаще осуществлять проверку электронных подписей защищенных файлов системы, с помощью групповой политики повысить до максимума уровень безопасности офисных программ и обозревателя, разрешить выполнение только подписанных электронной подписью сценариев и т. п.

Поскольку администраторам достаточно часто приходится заниматься поиском троянских программ, опишем основные способы их автоматического запуска.

Автоматически загружаемые программы

В операционной системе существует большое количество способов автоматического запуска программ[1]. Обычно "зловредная" программа для обеспечения своей работы использует тот или иной вариант, поэтому во многих случаях избавиться от вредоносного кода может помочь обычный контроль за списком автоматически загружаемых программ.

Итак, вредоносный код может быть запущен, используя:

- файлы autoexec.bat, config.sys: вариант используется нечасто, поскольку новые операционные системы обычно не учитывают параметры этих файлов;
- файл win.ini: хотя этот файл сохраняется в целях обратной совместимости, но включение программ в строки `run` и `load` позволяет обеспечить их запуск системой;
- папку Автозагрузка для всех пользователей и профиля данного пользователя: достаточно просто проверить содержимое данной папки, чтобы обнаружить такую программу;
- ключи реестра, описывающие автоматически загружаемые программы[2]:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnceEx
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServicesOnce
HKCU\Software\Microsoft\Windows\CurrentVersion\RunServices
HKCU\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run
HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Load
```

Порядок загрузки программ из этих ключей следующий:

```
HKLM\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices
<Logon Prompt>
HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
```

---

[1] Практически полный перечень автоматически загружаемых программ на компьютере можно получить с помощью программы **Сведения о системе**.

[2] Параметры `RunServices` и `RunServicesOnce` не используются в новых версиях ОС.

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
StartUp Folder
HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
```

Отличие запуска через описанные параметры состоит только в том, что программы, указанные в `RunOnce` загружаются синхронно, а в `Run` — асинхронно (могут выполняться параллельно). Программы, перечисленные в параметре `RunOnceEx`, загружаются в одном процессе с индикацией хода выполнения в диалоговом окне.

Администратор домена через групповую политику может отключить для Windows NT 4.0/200*x*/XP автоматический запуск программ при старте системы, определенный в параметрах `Run` и `RunOnce`. Для этого используется ветвь **Конфигурация компьютера | Административные шаблоны | System | Logon |** с параметрами **Do not process...** и аналогичная ветвь для пользовательской части политики. Одновременно необходимые программы могут быть назначены для автозагрузки через параметр групповой политики. Эти значения записываются на компьютере в ветвях

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
```

- Browser Helper Object (BHO): в Windows имеется возможность встраивать в Internet Explorer специально разработанные программы, призванные расширить функциональность обозревателя. Поскольку данные программы имеют практически неограниченные права доступа к локальной системе, хакеры часто используют эту технологию для отслеживания действий пользователя, для показа рекламы или перенаправления на порносайты и т. п.

  Эти программы подключаются через ветвь реестра

  ```
  HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper
  Objects
  ```

  по их GUID. Поскольку среди таких программ присутствуют и "полезные" расширения, то при анализе системы необходимо найти в реестре программу, зарегистрировавшую данный GUID. Помочь в быстром поиске BHO могут такие утилиты, как HijackThis (**http://www.spywareinfo.com/~merijn/files/hijackthis.zip**);

- некоторые другие ключи, которые обычно не приводятся при описании возможных вариантов автозапуска программ, однако возможность использования которых также нельзя исключать:

  ```
  HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad
  HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit
  ```

```
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System\Shell
HKCU\Software\Policies\Microsoft\Windows\System\Scripts
HKLM\Software\Policies\Microsoft\Windows\System\Scripts
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs
```

Автору однажды пришлось долго возиться с вирусом, прописавшим запуск своего устанавливающего файла в ключ `Shell`;

Примечание

Автору не раз приходилось сталкиваться с ситуациями, когда запуск вредоносного кода тщательно маскировался: зараженная программа создавала ничем не выделяющийся процесс, который и пытался активизировать собственно вирус. В подобных случаях помогут утилиты, отображающие иерархию процессов системы (рис. 9.9).

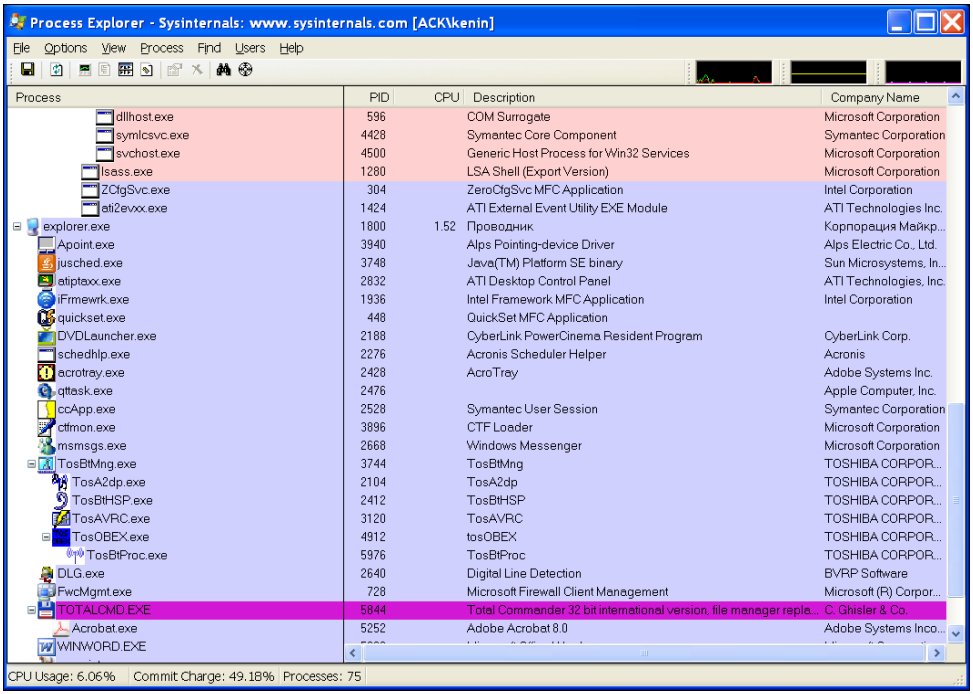


Рис. 9.9. Программа Process Explorer позволяет увидеть иерархию запущенных в системе процессов

- запуск программ, назначенных в расписании: вариант запуска, легко обнаруживаемый простым просмотром назначенных заданий;
- ActiveX: вариант используется не так часто, поскольку в современных ОС для установки ActiveX требуется явное согласие пользователя при нали-

чии у модуля электронной подписи[1]. Кроме того, в любой момент можно просмотреть установленные модули (**Свойства обозревателя** | вкладка **Общие** | **Параметры** | кнопка **Просмотр объектов**) и удалить ненужные;

- службы и драйверы: установленный в виде нового драйвера или службы сторонний код обычно трудно обнаружить, поскольку пользователю системы необходимо точно знать собственную настройку и список драйверов устройств. Например, таким способом устанавливалась одна из версий защиты компакт-диска от копирования. Кроме того, злоумышленники могут скрыть исполняемый код из отображаемых процессов системы, тем самым не давая повода сомневаться в надежности системы.

  Главный способ защиты от таких внедрений — отказ от использования административных учетных записей при текущей работе. В этом случае программа просто не сможет незаметно для пользователя установить новый драйвер или создать дополнительную службу. Правило простое, но обычно редко исполняемое.

Генерация списка автозагружаемых программ

Список автоматически загружаемых программ легко получить при помощи утилиты *msconfig* (рис. 9.10).

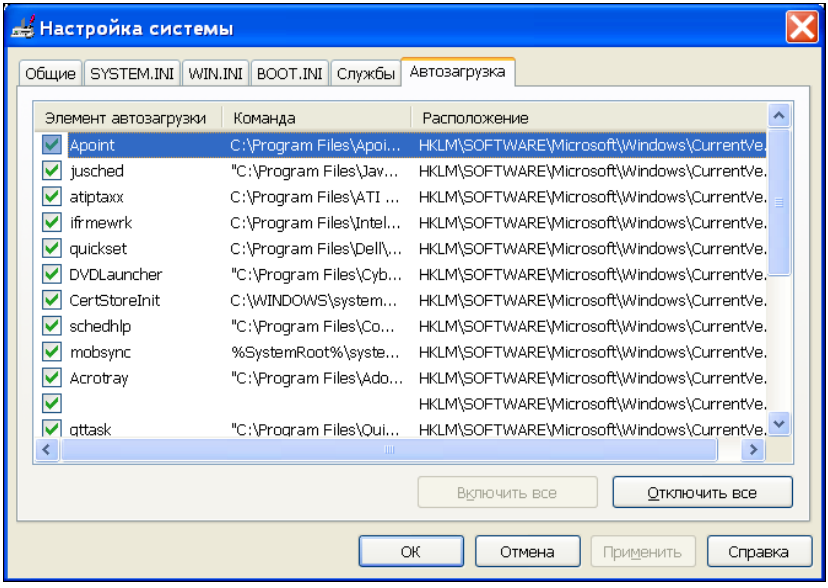


Рис. 9.10. Окно программы msconfig

[1] Это требование используется по умолчанию. Администратор может дополнительно повысить уровень безопасности, задавая параметры групповой политики.

В некоторых случаях удобнее использовать в этих целях следующий сценарий:

```
strComp = "."
Set objService = GetObject("winmgmts: impersonationLevel=impersonate}!\\"
& strComp & "\root\cimv2")
Set colCommands = objService.ExecQuery ("Select * from
Win32_StartupCommand")
For Each objCommand in colCommands
    Wscript.Echo "Command: " & objCommand.Command & vbCR &_
    "Description: " & objCommand.Description & vbCR &_
    "Location: " & objCommand.Location & vbCR & "Name: " &_
    objCommand.Name & vbCR &_
    "User: " & objCommand.User
Next
```

Приведенный код несложно модифицировать для получения данных не только локального компьютера, но и всех систем сети.

Rootkit

Rootkit[1] — это программа, использующая технологии маскировки своих файлов и процессов. Наверняка многие читатели слышали о долгом обсуждении в Интернете системы цифровой защиты прав, которая, будучи установленной на компьютере, использовала эту технологию для скрытия своего присутствия. В качестве еще одного примера можно привести известную антивирусную программу (Kaspersky Antivirus), использующую технологии rootkit для сокрытия своего присутствия при чтении данных NTFS.

Цель такой маскировки достаточно ясная: если программа контроля (антивирусная, антитрояновая и т. п.) не обнаружит присутствия вредоносного кода, то она и не начнет с ним бороться. Сама же возможность маскировки заложена в Windows. Например, вы не видите среди папок диска такие каталоги, как $Mft, $BadClus, а при просмотре совместно используемых ресурсов не обнаруживаете папок C$, ADMIN$, IPC$. Руткиты модифицируют соответствующие фильтры, и их присутствие на компьютере становится незаметным. Кроме того, они используют некоторые специфические особенности: например, наличие нуль-символа в имени службы приводит только к частичному ее отображению, а сохранение двоичных данных в строковом параметре реестра маскирует их от отображения.

---

[1] При общении IT-специалисты обычно не переводят этот термин, используя слово *"руткиты"*. Желающие более подробно ознакомиться с подобными технологиями могут посетить сайт www.rootkit.com.

Для обнаружения руткитов созданы специальные программы. Суть их проверок состоит в сравнении информации, полученной в результате низкоуровневого считывания с диска, с данными, отображаемыми стандартным образом. Кроме этого, производится проверка основных структур операционной системы. Наиболее точный результат можно получить *только* при проверке жесткого диска компьютера из заведомо "чистой" операционной системы, например, при загрузке и запуске программы проверки с CD-ROM.

Одну из возможных утилит для проверки системы на наличие руткитов можно загрузить с сайта Microsoft по ссылке **http://www.microsoft.com/technet/sysinternals/security/rootkitrev**.

Обнаружение нештатной сетевой активности

Вирусная эпидемия или атака на информационную систему не возникают "вдруг". Обычно существует некий период, который характеризуется повышенной нештатной сетевой активностью. Периодический анализ файлов протоколов систем и использование тех или иных *обнаружителей сетевых атак* могут предупредить администратора и дать возможность предпринять встречные шаги.

Хотя профессиональные программы, предназначенные для обнаружения сетевых атак, достаточно дороги, требуют высокого уровня знаний от администратора и обычно не используются в малых и средних предприятиях, администраторы легко могут найти в Сети пакеты, которые позволяют прослушивать активность на TCP/IP-портах системы[1]. Сам факт обнаружения активности на нестандартных портах уже может быть свидетельством нештатного поведения системы, а наличие сетевого трафика в неожидаемые периоды времени может косвенно свидетельствовать о "работе" троянов.

Отмечу несколько бесплатных программ, которые часто применяются для сканирования сети[2]:

- nmap (http://www.insecure.org/nmap/, версии для Windows и Linux);
- Nessus (**http://www.nessus.org**, Linux-версии);
- NSAT (**http://sourceforge.net/projects/nsat/**, Linux-системы).

---

[1] Например, утилита APS (AntiPort Scanner), предназначенная для обнаружения сканирования портов и попыток атак на сервисы, которую можно найти по адресу **http://z-oleg.com/secur/index.htm**.

[2] Преобладание Linux-версий объясняется большими возможностями настройки данной операционной системы на низком уровне по сравнению с Windows-вариантами.

Защита от использования ошибок программного кода

Ошибки находят во всех операционных системах, они свойственны как самим операционным системам, так и прикладному программному обеспечению. Установка обновлений[1] является одним из наиболее критических элементов системы безопасности, причем администратору необходимо следить не только за обнаружением уязвимостей в операционной системе, но и быть в курсе обновлений *всего установленного* программного обеспечения.

Бесконечный процесс обновлений

В среднем ежедневно обнаруживается около десяти уязвимостей, почти три четверти которых легко могут быть использованы хакерами. Обычно через некоторое время после обнаружения уязвимости появляется специальная программа (ее принято называть *exploit*), которая реализует эту уязвимость на практике. Найти такую программу в эпоху глобальных компьютерных сетей не представляет особого труда. В результате обычный пользователь получает инструмент, позволяющий ему, например, повысить свои права до уровня администратора или "свалить" сервер предприятия (рис. 9.11). Можно рассуждать о причинах такого поведения, но автору неоднократно приходилось сталкиваться с наличием подобного пользовательского интереса.

В связи с постоянно повышающимся риском использования обнаруженных уязвимостей подробная информация о них не только не распространяется, но и тщательно скрывается. Соответствующие бюллетени рассылаются фирмами-изготовителями конечным пользователям только тогда, когда для уязвимостей уже подготовлена заплата. Несмотря на это, срок между опубликованием обновления и появлением программы, реализующей данную уязвимость, постоянно уменьшается. В результате администраторы не имеют лимита времени на обдумывание своих действий, тестирование решений и т. п.

Например, во время подготовки материала книги уязвимость в службе DNS систем на основе Microsoft начала "эксплуатироваться" при помощи эксплойтов еще до того момента, как была выпущена соответствующая заплатка.

---

[1] Исторически существуют различные названия обновлений: *заплатки* (Hot fix), которые обычно выпускаются после обнаружения новой уязвимости, *сервис-паки* (service pack), в которые включается не только большинство реализованных ко времени выпуска сервис-пака заплат, но и некоторые усовершенствования и дополнения основных программ, и т. п. В данном контексте для нас не актуальны эти различия. Отметим только, что если заплаты по тем или иным причинам еще можно игнорировать, то сервис-паки следует устанавливать, если, конечно, нет особых "противопоказаний", как было в случае с Windows XP SP2.

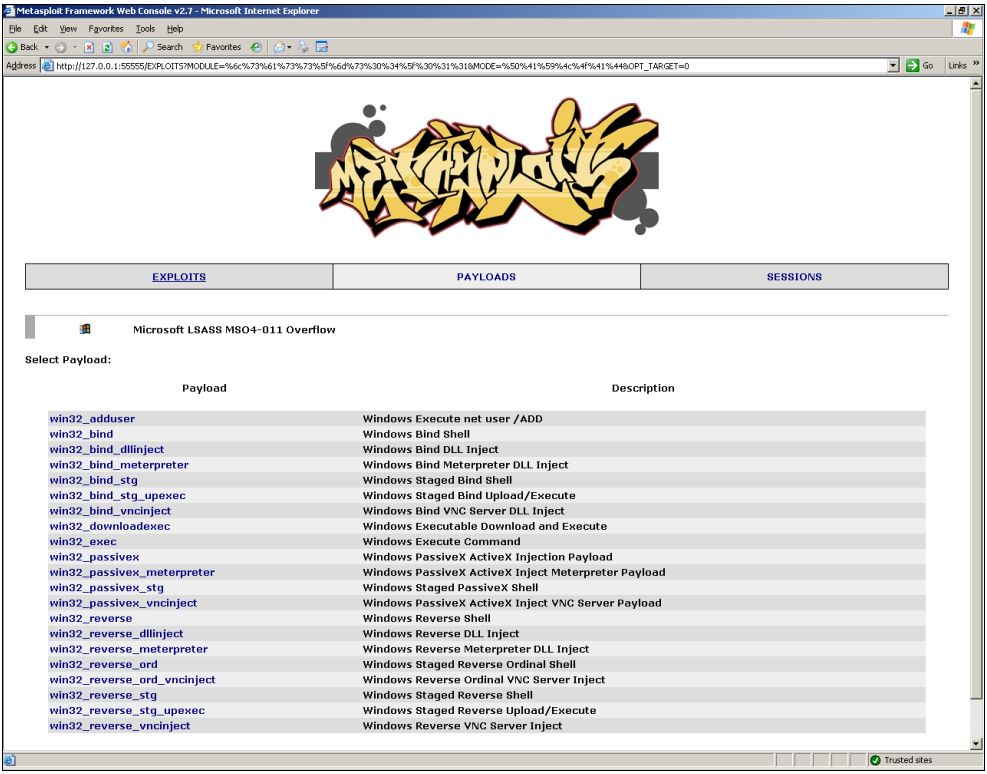


Рис. 9.11. Программа Metasploit предназначена для осуществления атак на компьютеры Воспользоваться уязвимостью пользователь может, найдя в Интернете соответствующий эксплойт. Дальнейшие его действия будут заключаться только в выборе варианта вторжения на чужой компьютер

Где узнать о необходимости установки обновления?

Очевидно, что перед тем, как предпринимать какие-либо меры, необходимо узнать о появившейся опасности.

Информация об обнаруженных уязвимостях публикуется на специализированных сайтах, адреса которых перечислены ранее в *разд. "Интернет-ресурсы, посвященные безопасности"*. Понятно, что просматривать оперативную информацию о событиях безопасности ежедневно практически нереально, поэтому целесообразно подписаться на существующие рассылки.

Ни в коем случае не следует доверять письмам электронной почты, советующим срочно установить то или иное обновление и часто содержащим "файл исправлений". Такие письма обычно являются фальсификацией.

Если у администратора появляется задача проанализировать какой-либо компьютер (или группу) на полноту установки обновлений безопасности, то самый простой способ — это загрузить с сайта Microsoft утилиту Microsoft Baseline Security Analyzer (MBSA). MBSA позволяет выполнить анализ компьютера (локального, удаленной системы или целой подсети) на наличие установленных обновлений безопасности и сформировать некоторые советы по повышению уровня защищенности систем. Для анализа используются актуальные данные, загружаемые с сайта изготовителя.

Примечание

Имейте в виду, что MBSA обнаруживает не все известные на текущий момент уязвимости систем. Кроме нее имеются бюллетени безопасности, совместно с которыми выпускается специальная утилита для тестирования систем. Подробности следует уточнять в соответствующей документации.

Существуют бесплатные средства проверки полноты установки обновлений и от других разработчиков. Например, можно загрузить Windows Vulnerability Scanner (**http://www.pspl.com/download/winvulscan.htm**) — утилиту объемом менее 1 Мбайт, которая проверит состав установленных обновлений Microsoft. По результатам тестирования будет сформирован список отсутствующих обновлений, причем щелчок по номеру бюллетеня безопасности откроет в обозревателе Интернета страницу, с которой можно загрузить соответствующий патч (рис. 9.12).

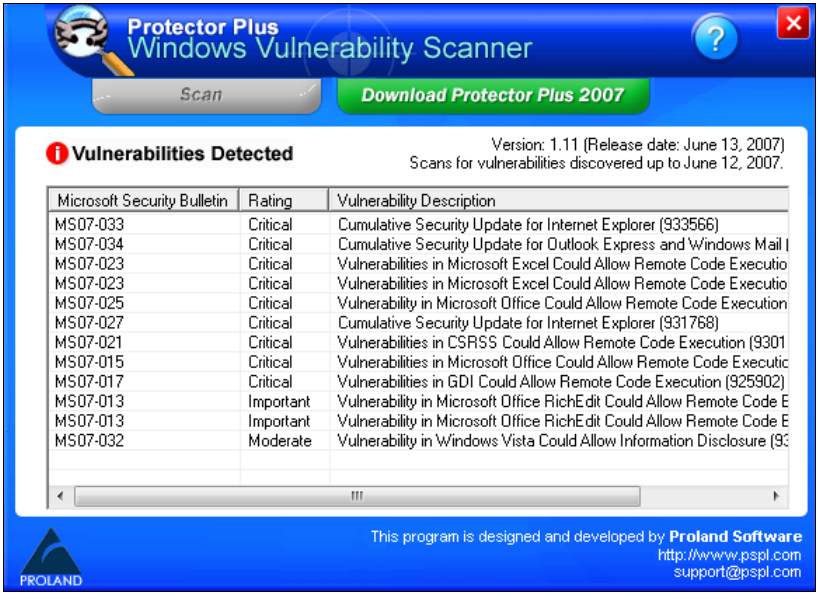


Рис. 9.12. Программа Windows Vulnerability Scanner отображает список обновлений, которые необходимо установить на компьютер

Эта программа удобна для анализа автономных компьютеров, поскольку содержит в себе список выпущенных патчей; очевидно, что она нуждается в периодическом обновлении с сайта изготовителя. Из неудобств работы я бы отметил необходимость самостоятельного контроля номеров бюллетеней безопасности (программа предлагает к установке как текущие патчи, так и те, которые были заменены новыми версиями) и настойчивые предложения установить обновления к продуктам, которые отсутствуют в системе. Так, мне несколько раз предлагалось установить заплатки к MS Office 2003, хотя в операционной системе установки продуктов данного семейства не было — могу предположить только, что отдельные библиотеки были установлены другими программами. Так что остается уповать на корректную работу программ установки обновлений.

Администратор может воспользоваться для сбора информации о системе и любой программой, предназначенной для анализа безопасности компьютерных систем. Сегодня выбор на рынке подобных продуктов довольно разнообразен. Как правило, программы сканирования уязвимостей выполняют типовые операции: проверяют наличие уязвимостей по имеющейся у них базе, сканируют IP-порты, проверяют ответы на типовые HTTP-запросы и т. д. По итогам таких операций формируется отчет, предоставляемый администраторам, и приводятся рекомендации по устранению уязвимостей. На рис. 9.13 представлено окно одной из подобных программ — XSpider (**http://www.xspider.ru/**).

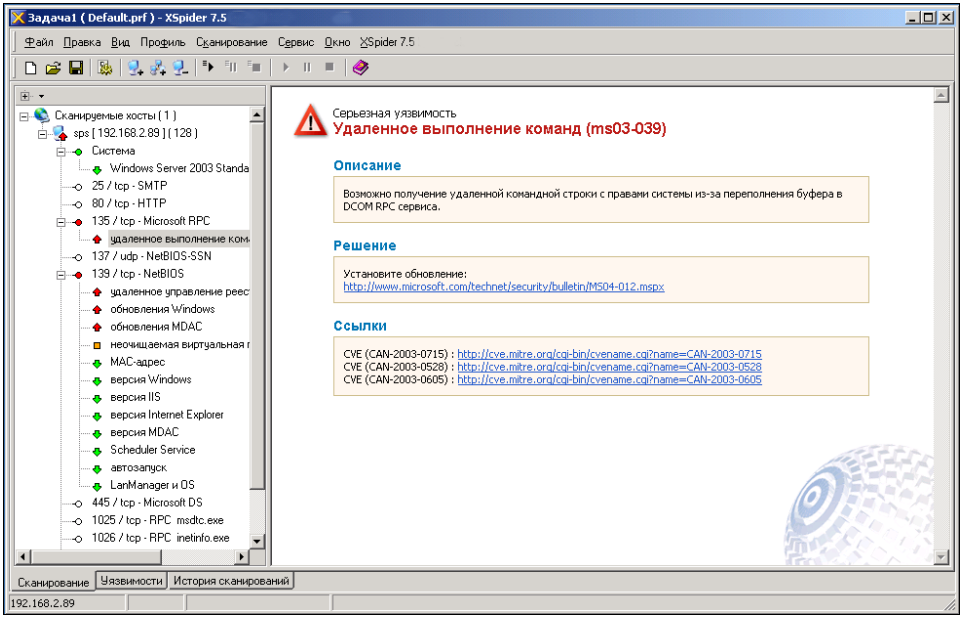


Рис. 9.13. Программа XSpider провела тестирование системы и обнаружила уязвимости

Примечание

При тестировании информационной системы с помощью подобных программ следует проявлять особую осторожность. Во-первых, при тестировании резко повышается нагрузка на сеть. Во-вторых, отдельные тесты могут привести к аварийному завершению работы компьютеров.

Тестирование

К сожалению, сами обновления нередко становятся причиной ошибок в работе компьютерной системы. Те, кто более или менее периодически знакомится с конференциями по программным продуктам, наверняка помнят пики эмоций, когда после установки очередного сервис-пака система просто переставала работать. Можно упомянуть и недавний выпуск второго сервис-пака для Windows 2003, после установки которого в отдельных случаях наблюдались ошибки добавления компьютера в домен, проблемы связи Outlook с сервером Exchange, снижение скорости работы в сети, невозможность подключения к терминальному серверу или установки VPN-соединения и т. п.[1] Автору неоднократно приходилось сталкиваться с ситуациями, когда установка обновлений приводила к сбоям системы, причем часто проблемы возникали не сразу, а уже в процессе эксплуатации, когда сбой в работе системы становился критичным для обеспечения бизнес-процессов организации.

Поэтому администратор поставлен перед дилеммой: применять обновление и рисковать стабильностью работы системы или не ставить и ждать, что атака злоумышленника минует компьютеры небольшой и незаметной организации. В таких случаях можно порекомендовать компромиссный подход: критичные обновления безопасности желательно устанавливать оперативно, а сервис-паки внедрять крайне осмотрительно, обязательно выдерживая тестовые паузы после обновлений каждой службы.

Разработчики программного обеспечения советуют в обязательном порядке тестировать все устанавливаемые на рабочие компьютеры обновления. Тестирование должно проводиться в типовой для данной организации конфигурации для каждой версии операционной системы. Администратору следует самостоятельно определить, выполнение каких функций необходимо проверить после обновления. Понятно, что полностью протестировать систему после установки обновлений в условиях малой или средней организации практически нереально, но проверить хотя бы возможность загрузки компьютера и правильность выполнения основных бизнес-процессов — вполне возможно.

---

[1] См., например, **http://blogs.technet.com/sbs/archive/2007/04/24/common-networking-issues-after-applying-windows-server-2003-sp2-on-sbs.aspx**.

Совет

Ставьте полученные обновления сначала на неосновные компьютеры, в частности, попробуйте произвести эту операцию на своей машине. И, конечно, заранее продумайте, как вы будете восстанавливать систему в случае ее краха. Например, есть ли у вас актуальные файлы резервной копии и насколько будет нарушено функционирование организации, если такое восстановление придется проводить сразу после применения обновления?

Способы обновления операционных систем

Существует большое количество решений, призванных облегчить работу администратора по установке обновлений программного обеспечения.

Примечание

Если в вашей сети уже реализована та или иная технология обновлений программного обеспечения, то не имеет смысла внедрять новый вариант такой службы без особых на то причин.

Для автоматизации обновления операционных систем используется специальная технология, позволяющая проанализировать состав программного продукта, наличие установленных обновлений, сравнить полученные данные с требуемой конфигурацией, сформировать перечень патчей, необходимых для установки, и произвести установку обновлений. Для операционных систем на основе Windows перечисленные операции выполняет специальная программа, запускаемая на сайте **windowsupdate.microsoft.com (www.windowsupdate.com**[1]); аналогичная технология реализована и в решениях, предлагаемых для сетей предприятий — System Update Service и Software Updates для SMS.

На момент подготовки книги Windows Update позволяла устанавливать обновления безопасности для следующих продуктов: MDAC версий 2.5—2.8, Exchange Server 2003, Microsoft Virtual Machine, MSXML версий 2.5, 2.6, 3.0 и 4.0, BizTalk Server версий 2000, 2002, 2004, Commerce Server версий 2000 и 2002, Content Management Server версий 2001 и 2002, Host Integration Server версий 2000 и 2004, SNA Server 4[2].

---

[1] Обновления программ MS Office доступны по **http://officeupdate.microsoft.com/**.

[2] См. KB306460 на сайте Microsoft. Обратите внимание, что каждая из двух версий программы MBSA (Microsoft Baseline Security Analyzer) имеет собственные списки контролируемых на наличие уязвимостей программных продуктов. Поэтому выбор версии должен определиться структурой используемых на вашем предприятии служб.

Обновления с узла Microsoft (Windows Update)

Самый простой способ обеспечить наличие последних обновлений от Microsoft — включить режим автоматической установки обновлений на каждом компьютере информационной системы (рис. 9.14).

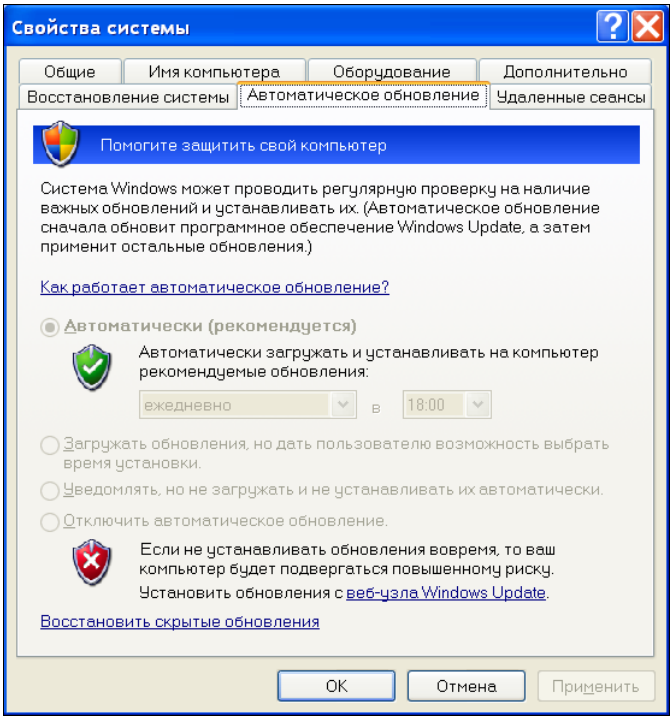


Рис. 9.14. Включение режима автоматических обновлений

Примечание

Часть файлов Windows обновляет, не сообщая об этом пользователю. Например, так обновляются файлы самой службы установки обновлений. При этом следует учитывать, что системными политиками межсетевых экранов разработки Microsoft по умолчанию разрешен неконтролируемый доступ к хостам, с которых производится загрузка обновлений. Поэтому подобные "несанкционированные" обновления могут быть не замечены администраторами, что является серьезной брешью в защите информационной системы.

Windows Update Services

Обновляя систему и пакет MS Office с сайта Microsoft, можно быть уверенным в установке последних версий "заплат". Однако для компьютерной сети предприятия это означает загрузку из Интернета обновлений для каждого

компьютера, что может привести к существенному росту трафика. Поэтому администратору необходимо обратить внимание на централизованную политику опций автоматического обновления[1]. Установку данных настроек не следует отдавать "на откуп" пользователям, чтобы впоследствии не выяснять причины увеличенных сумм счетов за Интернет.

При большом парке компьютеров целесообразно использовать *службу автоматического обновления* Windows Update Services (WUS). Она распространяется бесплатно и предназначена для установки обновлений Windows, критичных для безопасности. Соответствующий дистрибутив может быть загружен с сайта Microsoft и установлен на любой сервер сети.

Примечание

WUS представляет собой Web-сервер. При его установке осуществляются дополнительные настройки, ограничивающие функциональность информационного сервера[2] в целях повышения безопасности. Эту особенность необходимо иметь в виду, если на компьютере, предназначенном для WUS, уже присутствует действующий сайт.

WUS фактически создает сервер Windows Update в локальной сети: на один компьютер загружаются критические обновления, а на локальных компьютерах устанавливаются клиенты Windows Update, настроенные на работу с этим сервером. В результате трафик Интернета может быть существенно снижен.

Настройка WUS крайне проста. После установки необходимо:

1. Открыть страницу управления (расположена по адресу http://<имя_сервера_WUS>/WUSadmin/).
2. Выбрать языки, для которых будут загружаться обновления.
3. Указать параметры учетной записи доступа в Интернет (при работе через прокси-сервер).
4. Назначить расписание, по которому служба будет проверять наличие обновлений на сервере Microsoft.
5. Провести первоначальную загрузку обновлений с последующим подтверждением возможности установки каждого патча.

В дальнейшем необходимо только регулярно проверять работу службы и давать согласие на публикацию (согласие на возможность установки обновлений клиентом) новых обновлений.

---

[1] Эти параметры можно регулировать при помощи групповой политики.

[2] Настройка производится при помощи утилиты LockDown. При этом отключаются различные дополнительные возможности, которые не используются в базовой конфигурации, например, исполнение директив включения внешних данных в HTML-страницы и т. п.

Примечание

Некоторые обновления являются *кумулятивными* (т. е. содержат в себе предыдущие обновления). Например, кумулятивные обновления периодически выпускаются для Internet Explorer. При согласии на установку такого обновления целесообразно отключить публикацию предыдущих версий.

Для настройки клиентов на работу с локальным сервером обновлений необходимо отредактировать групповую политику обновлений. Для этого в политику организации следует импортировать файл настроек (wuau.adm), который устанавливается вместе со службой, и настроить параметры политики. Обычно необходимо указать адрес внутреннего сервера и определить варианты обновлений (выполнять автоматически, показывать сообщения о наличии обновлений и т. п.).

Примечание

Для индивидуальной настройки системы на локальный сервер WUS (если компьютер не использует групповые политики) следует добавить в ветвь `HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate` реестра клиентской системы два ключа: `WUServer` (тип `Reg_SZ`) и `WUStatusServer` (тип `Reg_SZ`). Оба они должны указывать на внутренний WUS-сервер (например, **http://wus**).

Преимущества и недостатки WUS

Хотя служба WUS существенно облегчает обновление компьютерных систем предприятия, она имеет ряд недостатков.

Во-первых, WUS поддерживает версии операционных систем клиентов, только начиная с Windows 2000 SP2[1]. Во-вторых, WUS позволяет устанавливать *только* ограниченный круг обновлений. Вы не сможете использовать эту технологию для обновления прикладного программного обеспечения. В-третьих, регулировать установку отдельного обновления очень сложно: придется либо ставить обновления на все системы, либо создавать специальные настройки. Это создает определенные сложности при тестировании и выдаче разрешений на публикацию обновлений.

Примечание

Возможный вариант решения проблемы состоит в установке в организации двух серверов WUS: основного и ведомого. Основной сервер загружает все обновления, после чего администратор тестирует их на контрольном компьютере, входящем в специально созданную OU со своей групповой политикой. Если при этом обнаружатся проблемы, с данного обновления снимается согласие на публикацию. После тестирования производится загрузка прошедших проверку

[1] Для клиентов Windows 2000 SP2 необходимо вначале установить компонент Automatic Updates, остальные (с версии Windows 2000 SP3, Windows XP) включают в себя эту функцию.

обновлений на второй сервер WUS, на использование которого настроены клиентские компьютеры. Честно говоря, автор совсем не уверен, что этот путь приемлем для небольших организаций.

В то же время при обеспечении безопасности большого парка компьютеров установка WUS позволяет существенно снизить трафик Интернета.

Обновление ПО с использованием специализированных средств

Решения по установке критически важных обновлений представлены разными фирмами. На рис. 9.15 представлено окно программы Quest Central от Quest Software, Inc. (**www.quest.com**). Одной из функций этого пакета является управление критическими обновлениями операционных систем Microsoft, SQL- и Exchange-серверов. Операция осуществляется при помощи программы HFNetChkPro.

На рисунке показано окно проверки системы. Программа обнаружила необходимость установки некоторых обновлений, хотя сами продукты на компьютере отсутствуют (установлены только консоли управления).

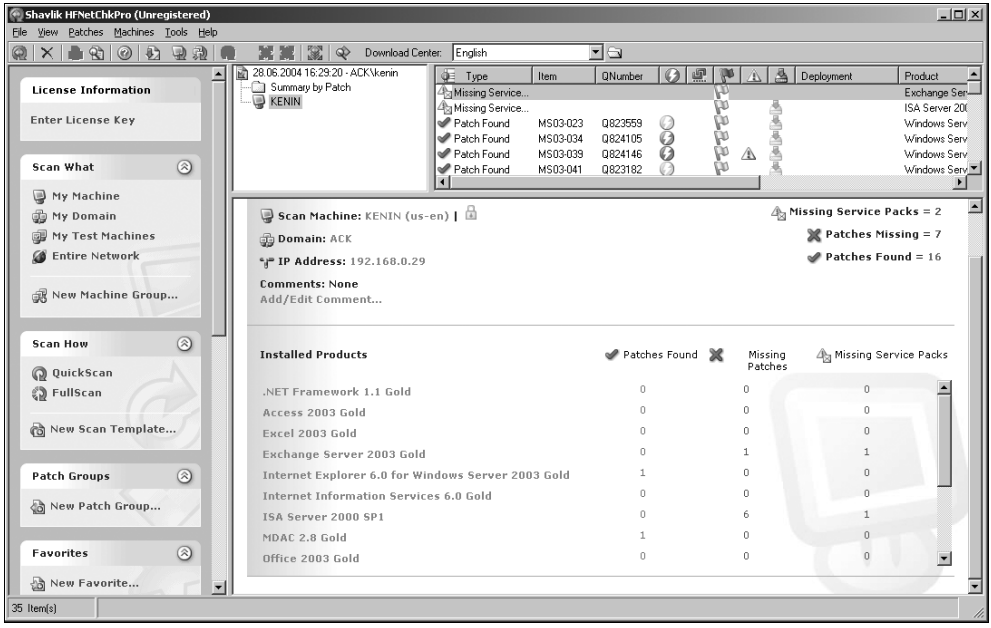


Рис. 9.15. Окно программы Quest Central

Microsoft для управления системами, в том числе для обновления программного обеспечения, разработала System Management Server (SMS) *(см. главу 13,*

разд. "Microsoft System Management Server"). Преимуществом SMS является то, что его можно использовать для установки обновлений *любого ПО*, а не только обновлений системы, критичных для ее безопасности, или MS Office.

Поскольку SMS ведет инвентаризацию аппаратной составляющей и программного обеспечения компьютеров, то администратор получает возможность практически индивидуальной настройки обновлений (например, учитывая версии установленного ПО, наличие свободного места на диске и т. п.) с последующим анализом операций в удобной форме отчетов.

Примечание

Функция обновления программного обеспечения стандартно включена в SMS 2003. Для SMS 2.0 необходимо загрузить пакет расширений (SMS 2.0 SUS Feature Pack), который добавляет эту функциональность.

Опция **Software Updates** позволяет автоматизировать настройку установки критических обновлений Windows и обновлений Office. SMS применяет типовые программы анализа системы, используемые для Windows Update, которые загружаются с сайта Microsoft и средствами SMS устанавливаются на клиентские компьютеры. Данные анализа клиентских систем передаются на сервер SMS, который формирует общий список необходимых обновлений. В результате с сайта Microsoft на локальный сервер загружаются только те обновления, которые соответствуют установленным в организации версиям программных продуктов.

Примечание

Стандартными средствами обнаруживаются не все уязвимости. Для SMS можно использовать утилиту Extended Security Update Inventory Tool, которая также свободно доступна для загрузки и позволяет выявить необходимость установки обновлений в соответствии с положениями бюллетеня безопасности. При этом следует учесть, что утилиты анализа выпускаются совместно с соответствующим бюллетенем безопасности Microsoft. Необходимую дополнительную информацию легко найти на сайте разработчика.

Обновление с использованием SMS можно оптимально настроить под конкретную систему, выбирая загрузку только тех патчей, которые необходимо установить на управляемые компьютеры. На рис. 9.16 в столбце **Request** отображается количество компьютеров, на которые по данным анализа следует установить соответствующее обновление безопасности.

Кроме возможности точной настройки групп обновляемых компьютеров, администратор может задать график обновлений (установить время выполнения операций), отложить операции перезагрузки систем и т. п. Всю текущую работу — пересылку пакетов обновлений в удаленные офисы, установку на вновь появившиеся системы, протоколирование итогов и т. п. — SMS возьмет на себя.

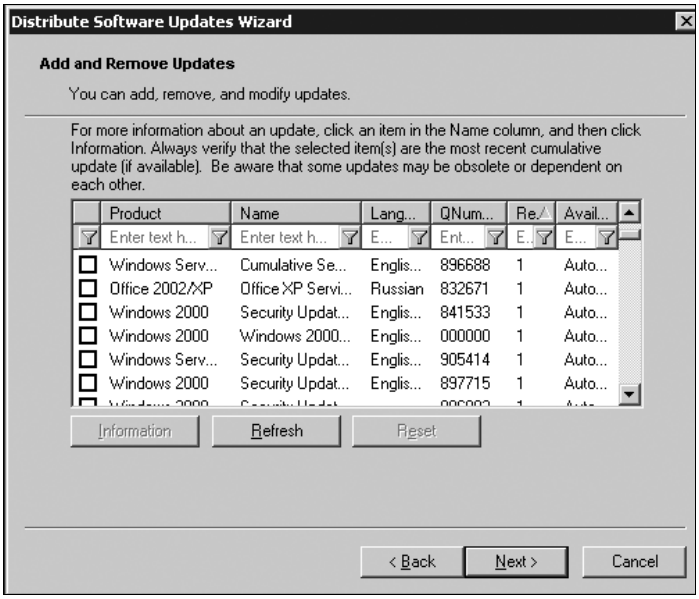


Рис. 9.16. Мастер загрузки обновлений в SMS отображает количество компьютеров, нуждающихся в каждом обновлении

В зависимости от конфигурации сети можно использовать одну задачу обновления для всех систем — это сократит до минимума административные затраты, однако большой размер обновления может оказаться неудобным для разветвленных организаций; можно настроить специализированные задачи обновления для каждого типа операционных систем — это позволит с легкостью ориентироваться в процессах обновлений; кроме того, можно создавать обновления для каждого патча — это даст возможность устанавливать обновления, не терпящие отлагательства. Таким образом, все зависит от специфики информационной системы организации.

Результаты установки обновлений (протоколы выполнения операций собираются стандартными средствами SMS) представляются в виде типовых отчетов SMS, шаблоны которых уже имеются в системе. Администратор может посмотреть, какие обновления необходимо установить на тот или иной компьютер, ознакомиться с текущим отчетом установки обновлений в своей организации (сколько компьютеров нуждается в установке обновления, каков фактический результат операции, какие возникли ошибки и т. п.).

Преимущества и недостатки SMS

SMS — серьезный серверный продукт управления компьютерной системой. Его возможности существенно больше тех, которые реализуются службой

SUS, тем более что установка программных продуктов — это только одна из его функций.

Во-первых, SMS позволяет устанавливать не только обновления, критичные для безопасности системы, но и обновления офиса (стандартно) и других программ (настраивается администратором).

Во-вторых, администратору доступна очень гибкая настройка опций[1]. Так, администратор может настраивать приоритеты установки обновлений. Например, срочно установить обновления, критичные для безопасности систем, и дать возможность пользователю отложить на некоторый срок установку иных обновлений, выбрать время установки обновлений на сервер и т. д.

В-третьих, SMS загружает обновления только для тех программ, которые обнаружены на компьютерах, входящих в сеть предприятия.

В-четвертых, SMS позволяет администратору легко получать наглядные отчеты по результатам операций на отдельном компьютере, по выбранному обновлению, усредненные для всей организации и т. п.

Однако SMS является отдельным коммерческим продуктом, хотя его стоимость и ниже других продуктов управления системами. Кроме того, его эксплуатация требует определенного уровня квалификации администратора системы.

Установка обновлений через групповые политики

Если сеть организации состоит из систем на основе Windows 200*x*/XP, то администратор может устанавливать необходимые обновления через групповые политики. Получив сообщение об обнаружении уязвимости, администратор может вручную загрузить пакет исправлений, протестировать его и распространить на компьютеры организации.

Специально для автоматизации установки обновления выпускаются в формате MSI. Загрузив файл обновления, его следует распаковать в папку на локальном диске, запустив с ключом `-x`. Затем, используя программу редактирования групповой политики, нужно создать пакет установки, импортировав msi-файл из этой папки. Единственное неудобство данного решения — необходимость создания различных политик, учитывающих установленную вер-

[1] Настройка обновлений MS Office более сложна, чем обновлений, критичных для безопасности системы. Так, администратору необходимо учитывать административные установки MS Office (в этом случае обновление клиентов может быть выполнено только из папок административной установки пакета) и обычные. Не могут быть выполнены обновления пакетов, установленных для пользователя (обновляются установки, выполненные только "на компьютер"). Кроме того, часть обновлений требует ручных операций администратора после их загрузки с сайта Microsoft и т. п. С соответствующими описаниями следует ознакомиться в руководстве по SMS.

сию операционной системы и программ MS Office[1]. Поскольку в малых и средних организациях обычно придерживаются однотипности устанавливаемого ПО, то подобные действия не должны вызвать затруднений администратора.

Примечание

При публикации сервис-паков, кумулятивных обновлений и т. п. в групповой политике следует отключить установку предыдущих версий обновлений, которые поглощаются данными пакетами. Для этого нужно выбрать соответствующую программу, дать команду на ее удаление и выбрать вариант продолжения использования теми пользователями, которыми она уже установлена.

Интеграция обновлений ПО

В реальной информационной системе постоянно идет процесс установки новых систем. Естественно, что вводимый в эксплуатацию компьютер сразу должен иметь все последние обновления безопасности. Поэтому целесообразно принять меры для интеграции обновлений в установочные пакеты.

Включение обновлений в образы вновь устанавливаемых систем

Программы установки обновлений, критичных для безопасности, позволяют интегрировать необходимые файлы в соответствующие дистрибутивы[2]. Для этого предназначен ключ запуска `/integrate:`*<путь>*, где *<путь>* — это папка с дистрибутивом, скопированным на жесткий диск.

Если впоследствии операционная система будет установлена с подготовленного таким образом дистрибутива, то она уже будет включать в себя данные обновления.

Примечание

Таким способом можно подготовить и загрузочный CD, если с помощью соответствующих программ сначала сделать образ CD, потом внедрить обновления в дистрибутив, заменить папки в образе и записать новую версию программы установки на CD. Единственным ограничением в этом случае становится объем диска. Уже сейчас, например, после интеграции обновлений, критичных для безопасности Windows XP, вышедших после выпуска второго сервис-пака, составляет 700 Мбайт — предел емкости CD стандартных приводов.

---

[1] Не следует использовать описываемый вариант для ручной установки. Применяйте штатный вариант запуска (программу update или иной запускающий файл).

[2] Мы описываем процесс интегрирования обновления для последней версии программы установки. В случае установки обновлений для предыдущих версий следует уточнить параметры командной строки по справочной документации.

Интеграция патчей msi-файлов

Описанный выше способ предназначен для интегрирования в состав дистрибутива сервис-паков и обновлений безопасности, выпущенных в виде исполняемых файлов (имя обновления аналогично следующему примеру — *WindowsXP-KB935840-x86-RUS.exe*). Но администратор может легко модифицировать и другие дистрибутивы, если они сами и программы обновлений представлены в виде msi-файлов.

Для обновления msi-файлов выпускаются пакеты обновлений *.msp. Чтобы внедрить их в исходные файлы, следует использовать ключ `/update` (`msiexec /update Update.msp`).

Примечание

Если обновление получено в виде исполняемого файла, то его обычно можно достаточно легко извлечь. Так, для пакета MS Office распаковку обновления производят запуском его с ключами `/c /t:`*`<папка для сохранения обновления>`*. В указанной папке будет сохранен файл обновления в формате *.msp.

Совет

Программы, инсталлированные с использованием msi-файлов, хранят параметры исходного установочного файла. Поэтому если в исходный дистрибутив внедрено обновление, то компьютеры, на которых данный продукт был уже установлен, "потеряют" связь с исходным установочным пакетом. В результате станут недоступными некоторые возможности, например, если вы выбрали вариант установки дополнительных опций программы по первому требованию, то этого не произойдет после обновления дистрибутива. Поэтому после такой модификации дистрибутива администратору необходимо связать уже установленный продукт с новым файлом установки[1].

Административная установка

В организациях рекомендуется иметь единый фонд дистрибутивов для установки на рабочие станции. Обычно все установочные пакеты хранятся на совместно используемом сетевом ресурсе. При этом администраторы часто просто копируют файлы установки на такой ресурс, забывая, что существует специальный режим *административной* установки.

Административная установка представляет собой установку программы на сетевой ресурс. При этом установка уже будет включать ряд параметров организации, которые введет администратор в процессе операции (например, название организации, серийный номер и т. п.) и которые будут повторены для каждого пользователя.

---

[1] Значение ключей инсталлятора для режима восстановления уточните, запустив его с ключом показа справки: `msiexec /?`.

В случае использования msi-файлов режим административной установки включается ключом /a — msiexec /a <Product.msi>. В дальнейшем из сетевой папки можно будет выполнить установку продукта на отдельные рабочие станции.

Физическая безопасность

Особая опасность наличия физического доступа к компьютеру состоит в том, что опытный злоумышленник не только получит разовый доступ к информации, но и сможет произвести такую замену служебных файлов системы, что в дальнейшем сможет получать доступ к любым данным в любое время (например, сможет обойти запреты файловой системы NTFS), причем эти действия будут скрыты от текущих пользователей и администратора.

Ограничения доступа к станциям

Если во время работы компьютера операционная система препятствует чтению защищенных данных, то при наличии физического доступа к компьютеру специальных мер для "взлома" применять не нужно. При загрузке с другой операционной системы (например, с дискеты или компакт-диска, при переносе жесткого диска в другой компьютер) никакие установленные в исходной системе ограничения NTFS не будут препятствовать копированию любой информации.

Понятно, что вы не сможете реально ограничить доступ пользователей к рабочим станциям[1]. Поэтому требование ограничения физического доступа относится, прежде всего, к серверам[2] компьютерной сети. При этом следует принять меры к тому, чтобы пользователи не хранили служебную информацию на рабочих станциях.

Уровень физической защиты зависит от конкретных условий. Автор встречал ситуации, когда в небольшой организации сервер просто устанавливался в

---

[1] Даже если вы отключите дисководы гибких дисков, устройства чтения компакт-дисков и опломбируете компьютер, то будет ли у вас уверенность в том, что кто-то не принес внешний CD-ROM? Или не восстановил после своих действий все пломбы? А если вы установили программу, которая блокирует доступ к таким устройствам (например, DeviceLock от SmartLine), то будете ли вы уверены, что опытный пользователь не отключил этот контроль? На большинстве предприятий контроль над рабочими станциями практически не организован.

[2] Во-первых, администраторы должны включить аудит событий включения/выключения серверов; правилами эксплуатации должен быть предусмотрен обязательный разбор причин нештатных выключений серверных станций. Во-вторых, серверы следует устанавливать в специальные помещения (или шкафы с датчиками), оборудованные средствами сигнализации о несанкционированном доступе.

сейф. Более крупные организации размещают серверное оборудование в охраняемом помещении, устанавливая особые правила доступа в него. Существуют возможности оборудования кроссовых шкафов датчиками проникновения, "фирменные" серверы фиксируют каждый случай открытия крышек корпуса и т. п.

Не следует забывать, что данные резервного копирования могут быть использованы для восстановления конфиденциальной информации. Например, можно провести восстановление папок контроллера домена в новое место и получить доступ ко всем защищенным данным. Поэтому меры защиты серверов резервного копирования (устройств, на которые осуществляется копирование данных) должны быть не менее жесткими, чем применяемые к защите контроллеров домена.

Меры защиты от копирования

Серьезной угрозой конфиденциальности компании является легкость, с которой пользователь, имеющий доступ к информации, может скопировать данные: электронная почта, устройства записи компакт-дисков, внешние устройства хранения данных (например, флэш-память, подключаемая к USB-портам системы) — подобный список можно продолжить и дальше.

Существуют различные способы ограничения доступа пользователей к внешним устройствам. Во-первых, есть специальные программы, позволяющие точно настроить возможность работы пользователем с внешними дисководами, CD-RW и USB-портов. В качестве примера сошлюсь на GFI LANguard Portable Storage Control (**http://www.gfi.com/**). Данная программа устанавливает на рабочие станции специальные службы, которые контролируют доступ пользователя к подобным устройствам и разрешают операции только для тех учетных записей, которым подобные действия разрешены администратором. Опция контроля доступа к съемным носителям присутствует также в новом продукте комплексной защиты — Symantec EndPoint Protection.

Второй вариант — это создание групповой политики Windows, позволяющей отключить такие устройства. Подробно данный способ описан в статье KB555324 на сайте Microsoft.

Оба этих варианта "хороши" для неопытных пользователей и легко обходятся специалистами, имеющими доступ к системе (например, посредством возможностей режима загрузки Safe Mode и последующем отключении контролирующих служб). В особых случаях необходимо прибегать к физическому отключению таких устройств и опечатыванию системных блоков.

Существует и программный способ предотвращения утечки информации. Это служба RMS *(см. главу 12, разд. "Служба управления правами (RMS)")*. Хотя

способы "обхода" ее защиты существуют, служба позволяет существенно повысить степень защиты данных.

Шифрование данных на компьютере

В некоторых ситуациях требуется обеспечить повышенную безопасность данных компьютера. При этом администратору приходится учитывать, что:

- невозможно ограничить права доступа к информации владельцу корневого ресурса домена (администратору предприятия): даже при установке явного запрета доступа администратор сможет получить доступ к любой информации. Это свойство доменов Windows;
- штатные системы защиты работают только при включенном компьютере. Если кто-то получит доступ к выключенной системе (например, утерянному ноутбуку или к рабочей станции пользователя), то он сможет при необходимости скопировать желаемые данные.

В подобных ситуациях наиболее действенным способом защиты информации будет *шифрование*. Шифрование файлов присутствует в Windows, начиная с версии 2000. При шифровании используются криптографические технологии, так что получить доступ к защищенным данным постороннему пользователю (в том числе и администратору) практически невозможно[1].

Примечание

Ограничение, которое существует при шифровании файлов, — это невозможность одновременного сжатия файлов и их шифрования. Вы можете либо сжимать данные для экономии места на диске, либо шифровать их в целях обеспечения безопасности данных.

Шифрование папок и файлов

Зашифровать файл (или папку с файлами) можно следующим образом: выделить его в задаче Проводник (или в любом окне просмотра папок диска) и открыть меню **Свойства**. Далее на вкладке **Общие** нажать кнопку **Дополнительно** и в окне **Дополнительные атрибуты** выставить флажок в опции **Шифровать содержимое для защиты данных**. После подтверждения операции данные будут зашифрованы. Если вы сохранили настройку параметров

[1] Обычно все коммерческие криптографические системы имеют специальные инженерные входы для доступа соответствующих служб. Поэтому гарантировать абсолютную защищенность информации невозможно.

интерфейса в значениях по умолчанию, то шифрованные файлы и папки будут отображены светло-зеленым цветом.

После того как файл зашифрован, открыть его может только тот пользователь, который осуществил шифрование. Тот, кто зашифровал файл, может расширить число пользователей, имеющих возможность чтения данных. Для этого нужно опять раскрыть меню свойств файла и дойти до вкладки **Дополнительные атрибуты**. Если файл уже зашифрован, то будет доступна кнопка **Подробно**. При ее нажатии вы увидите окно, в котором перечислены пользователи (рис. 9.17), которые могут расшифровать файл.

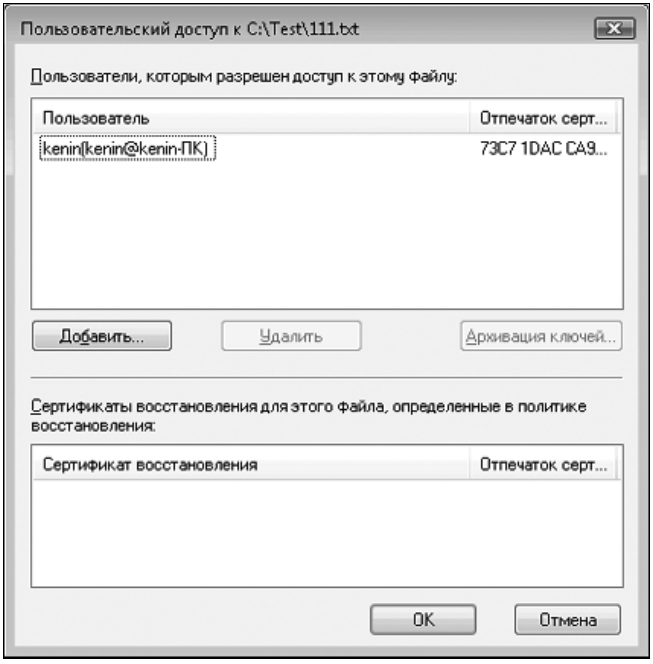


Рис. 9.17. Список пользователей, которым разрешено расшифровать данные файла

Чтобы добавить нового пользователя, достаточно нажать кнопку **Добавить** и выбрать пользователей, которые *имеют на данном компьютере сертификат*.

Совет

Обычно корпоративные политики шифрования предусматривают наличие специального пользователя, которому разрешается расшифровывать все данные. Делается это в целях сохранности производственной информации в непредвиденных ситуациях (несчастный случай с работником и т. п.). Технически такая политика реализуется либо включением по умолчанию дополнительного сертификата в перечень сотрудников, имеющих право на чтение файла, либо пу-

тем сохранения в службе каталогов сертификата пользователя, с помощью которого зашифрованы данные (в последнем случае имеется возможность восстановить ключи шифрования).

При шифровании файлов следует учитывать тот факт, что параметры операции защищены только паролем пользователя. Если этот пароль недостаточно сложен (например, длиной менее 15 символов), то злоумышленник может подобрать его, получить доступ к личному сертификату шифрования и расшифровать данные.

Подводные камни технологии шифрования

При создании наследует свойства своей родительской папки. Таким образом, если папка зашифрована, то файл будет также зашифрован и доступен только для тех пользователей, которые указаны в свойствах данной папки. При перемещении файлов в версиях Windows, предшествовавших Vista, были некоторые особенности, которые могли неприятно удивить пользователя потерей защиты зашифрованных данных: при перемещении файла с одного диска на другой на новом месте фактически *создавался* файл, получая свойства, соответствующие новой папке, иными словами, данные могли перестать быть зашифрованными. Однако если файл перемещался *в пределах одного диска*, то такая операция не приводила к копированию данных, изменялся только указатель на место расположения файла. В результате файл, который не был зашифрован, при перемещении в зашифрованную папку оставался незашифрованным, тогда как зашифрованный файл сохранял защиту при перемещении в незащищенную папку.

Эти же особенности имели место для параметров доступа к файлам при их перемещении из одной папки в другую.

В Windows Vista по умолчанию система следит за уровнем защиты файла. Если зашифрованный файл перемещается в незашифрованную папку, то он остается зашифрованным. А если незашифрованные данные перемещаются в зашифрованную папку, то они автоматически становятся зашифрованными.

Еще одна особенность, которую раньше не всегда на практике помнили пользователи, связана с тем, что зашифрованные файлы могут быть созданы только на дисках с файловой системой NTFS. Иными словами, если вы копировали зашифрованный файл на USB-носитель (а они обычно отформатированы в системе FAT), то данные автоматически становились незащищенными.

Если в Windows Vista пользователю выдается предупреждение о том, что при такой попытке защита будет потеряна, то в предыдущих версиях Windows возможно выполнение операции, после которой данные станут доступны любым пользователям.

Создание временно подключаемых шифрованных дисков

Шифрование папок и файлов просто в использовании, однако оно имеет много неудобств. Во-первых, шифрование фактически индивидуально — невозможно предоставить разрешения на ту или иную группу пользователей, что серьезно осложняет коллективную работу над проектом. Для каждого нового сотрудника в команде придется настраивать параметры шифрования для всех данных. Во-вторых, на практике защищаемая информация не ограничивается только файлами, размещенными в той или иной папке. Часто для хранения и обработки данных используются специализированные программы, запускаемые от имени специальных пользователей (например, сервер баз данных или информационной сервер служб Интернета и т. п.). Использование техники шифрования файлов, которая присутствует в системе, в этом случае становится невозможной.

Существует ряд программ, позволяющих создавать *зашифрованные диски*. Такой диск представляет собой зашифрованный файл, который может быть подключен как новый логический диск. Такое подключение *(монтирование)* осуществляется динамически. Достаточно выбрать соответствующую команду, ввести пароль (или предоставить устройство с ключом шифрования), чтобы в системе появился новый логический диск. Вся информация на таком диске зашифрована и становится доступной после операции монтирования.

Шифрованный логический диск доступен всем программам и пользователям системы. Отключение его может осуществляться либо вручную командой меню, либо автоматически при отсутствии активности (нет обращения к данным с диска в течение определенного периода).

Обычно объем шифрованного диска устанавливается динамически: он меняется в зависимости от числа данных и может расти в пределах свободного пространства исходного диска.

Шифрование диска

Еще один способ защиты заключается в шифровании диска *целиком*. С одной стороны, он более удобен для пользователя. Во-первых, не надо думать, куда сохранять информацию (на защищенный или незащищенный диск): данные всегда зашифрованы. Во-вторых, исключаются такие потенциальные каналы утечки данных, как временные файлы, которые всегда образуются при работе с данными и из которых можно извлечь часть информации. Обычно папки с ними размещаются на незашифрованных дисках (как более быстрых).

С другой стороны, шифрование диска целиком не обеспечивает сохранности данных *в процессе работы*, после загрузки компьютера, особенно в составе

домена организации. После старта операционной системы информация с зашифрованного диска потенциально доступна пользователям сети, особенно лицам, обладающим правами администраторов домена.

В то же время, если работать с динамически подключаемым диском, то шифрованные данные можно подключать *только на время, необходимое для работы с ними*. В отключенном состоянии можно не беспокоиться за сохранность информации.

Существует достаточное количество программ сторонних фирм, позволяющих реализовать возможность шифрования *всего* диска. Например, автор использует программу PGP, которая позволяет не только осуществлять безопасную переписку по электронной почте, но и создавать шифрованные диски (рис. 9.18). Есть как возможность создания любого количества динамически монтируемых дисков, так и наличие операций шифрования целых дисков. Программа позволяет использовать для хранения ключей аппаратные устройства, например, eToken, в которых реализована защита ключей шифрования, которое может быть использовано и для безопасного подключения шифрованного загрузочного диска при старте компьютера.

Можно упомянуть также программы Dekart Private Disk, Utimaco SafeGuard (в том числе версии для мобильных компьютеров, смартфонов), SecurStar DriveCrypt и др. В Windows Vista Ultimate и Windows Vista Enterprise присутствует технология BitLocker, осуществляющая посекторное шифрование данных всего жесткого диска[1]. Данные на диске становятся доступными только при работе операционной системы. При шифровании используется алгоритм AES с длиной[2] ключа 128 или 256 бит.

Самый высокий уровень защиты технология обеспечивает при наличии на материнской плате модуля TPM версии 1.2. В этом случае один из ключей, используемых при шифровании данных, хранится в этом модуле, что обеспечивает самый высокий уровень его сохранности. Однако технология может быть использована и на компьютерах, *не имеющих TPM-модуля*. В зависимости от требуемого уровня защиты компьютера вы можете потребовать использования дополнительного пароля (PIN-кода в случае использования смарт-карт) для дешифрования диска или хранить ключ на сменном носителе.

Совет

Если используется вариант без TMP, то при шифровании учитываются параметры конфигурации компьютера (параметры BIOS, данные загрузочных фай-

[1] Такая методика используется для обеспечения восстановления данных в случае появления сбойных секторов на диске.

[2] Длина ключа устанавливается параметрами групповой политики.

лов). Поэтому в случае необходимости обновления BIOS или обновления версий операционной системы нужно временно отключить шифрование. В противном случае вам придется использовать вариант доступа к диску в режиме восстановления.

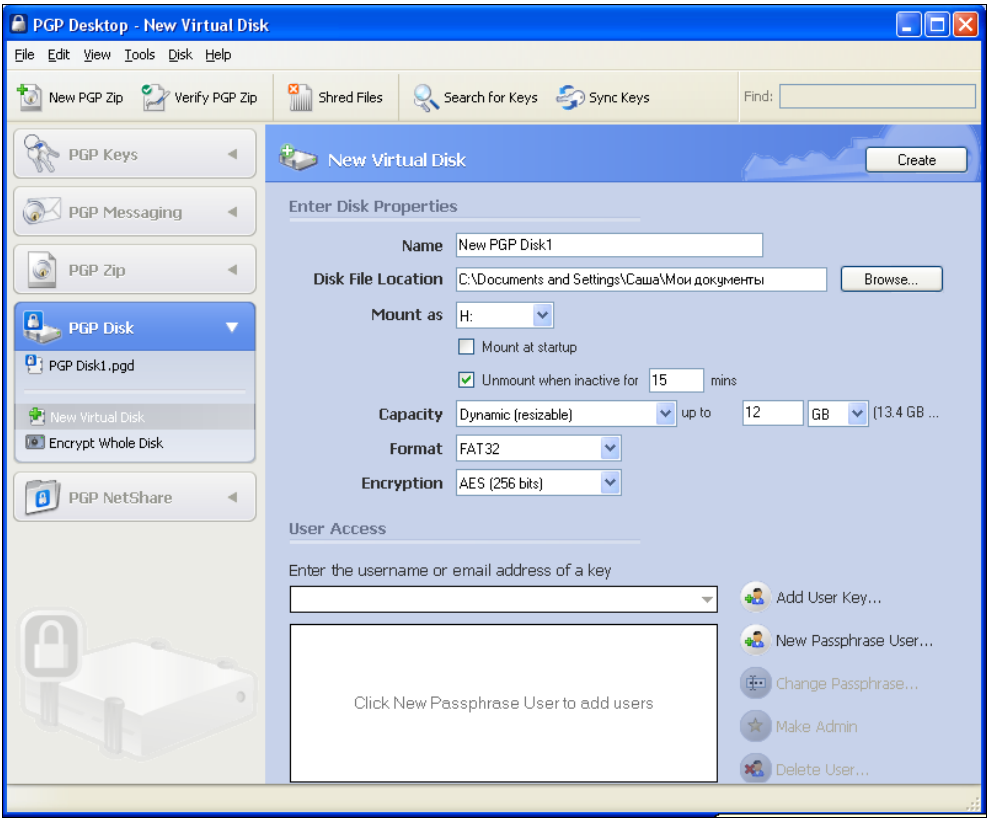


Рис. 9.18. Для создания зашифрованного диска в программе PGP достаточно определить только несколько параметров

Начало загрузки операционной системы Vista обеспечивается *незашифрованными* программами, для включения технологии в системе должны быть как минимум *два* логических диска. Поэтому возможность использования технологии BitLocker должна быть предусмотрена *до* установки операционной системы.

Использование BitLocker на компьютерах без TMP

По умолчанию Windows Vista позволит включить шифрование только при наличии на материнской плате модуля TPM и совместимой версии BIOS.

Если эти требования не выполняются, то можно зашифровать диск, используя сменный USB-носитель для хранения ключа. Такая возможность включается *только* через настройки групповой политики.

Утилита редактирования групповой политики присутствует на компьютере, но она не отображается в системе меню. Чтобы открыть ее, выполните команду `gpedit.msc`.

Параметры, которые необходимо изменить для включения дополнительных возможностей шифрования, находятся по следующему пути: **Политика "Локальный компьютер" | Конфигурация компьютера | Административные шаблоны | Компоненты Windows | Шифрование диска BitLocker** (рис. 9.19). Для параметра **Установка панели управления: включить дополнительные параметры запуска** необходимо установить значение **Включено**. Затем следует закрыть все окна настройки.

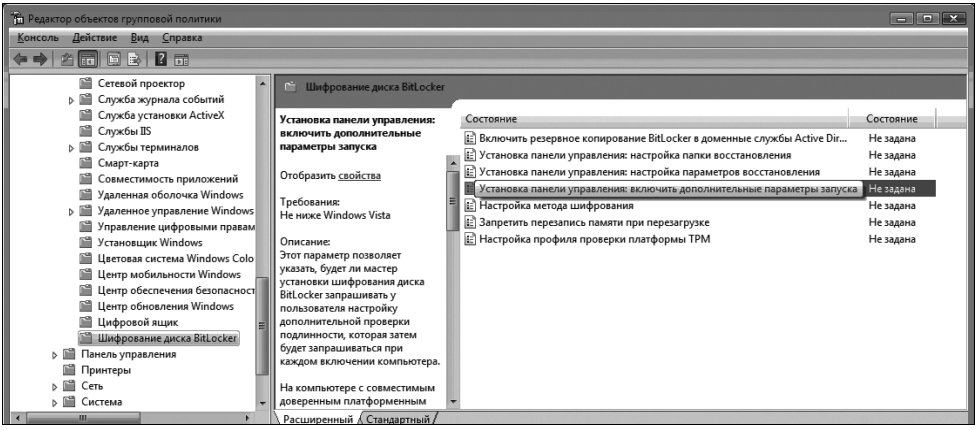


Рис. 9.19. Настройка групповой политики для включения BitLocker на компьютерах без TPM

После того как оснастка **Управление групповой политикой** будет закрыта, нужно дождаться применения политики. Чтобы не ждать, можно перезагрузить операционную систему или, без перезагрузки, выполнить команду `gpupdate /force`.

Совет

Лучше запустить эту операцию из командной строки, чтобы увидеть сообщение о результате.

После применения отредактированной таким образом групповой политики опция шифрования станет доступной.

Включение шифрования

Включение шифрования BitLocker производится через программу **Панель управления | Шифрование диска BitLocker**. Если все необходимые для шифрования условия выполнены, то в окне появляется опция **Включить шифрование**. После ее нажатия запускается мастер операций.

Вам нужно просто следовать указаниям программы. Обратите внимание, что в случае применения USB-носителя для хранения ключа мастер предложит сначала проверить возможность его использования. Не стоит пренебрегать данным этапом, поскольку в практике автора уже был случай, когда пришлось прибегнуть к режиму восстановления после отказа компьютера считать ключ при загрузке системы.

Совет

Технология BitLocker позволяет создавать ключ *восстановления* при любом варианте шифрования, в том числе и при использовании модуля TPM. Не пренебрегайте этой возможностью. Иначе, например, в случае аппаратных проблем вы потеряете все свои данные.

Процесс шифрования диска занимает достаточно длительное время и зависит от объема диска. В этот период можно продолжать работать на компьютере, хотя его производительность несколько снижается.

Шифрование дисков с данными не поддерживается

Шифрование с использованием технологии BitLocker осуществляется *только* для диска с операционной системой. Если на компьютере присутствуют другие диски (диски с данными), то они не могут быть зашифрованы в Windows Vista. Подобную возможность будет поддерживать только серверная версия операционной системы, готовящаяся к выпуску.

Кроме того, на сегодняшний день нет поддержки дисков, используемых в кластерных системах.

Режим восстановления

В случае выхода из строя оборудования (модуля TPM или всей материнской платы), изменения загрузочных файлов (например, перепрошивке BIOS и т. п.) нормальная загрузка компьютера становится невозможной. Вы увидите черный экран с предложением ввести пароль восстановления.

Пароль восстановления создается на одном из этапов подготовки диска к шифрованию с помощью мастера операций. Потом его можно продублировать, воспользовавшись соответствующими опциями задачи шифрования. Пароль представляет собой последовательность цифр. Для того чтобы можно было отличить один пароль от другого (если вы работаете с несколькими

системами), вам сообщается также его название, состоящее из ряда цифр и букв. И название пароля, и его значение сохраняются в один файл, так что легко можно выяснить, подойдет ли данный пароль для восстановления.

Как уже было сказано, пароль состоит только из цифр и вводится при помощи не цифровых, а функциональных клавиш, при этом клавиши <F1>, <F2>, ..., <F10> соответствуют цифрам 1, 2, ..., 0.

После ввода пароля система продолжит загрузку, а затем вы можете отключить режим шифрования.

Обратите внимание, что есть две возможности отключения шифрования. Первая предполагает полное дешифрование диска; это довольно длительная операция. Вторая только временно отключает режим шифрования, если вы собираетесь, например, заменить на компьютере BIOS.

Безопасность паролей

Одним из самых "узких" мест безопасности являются пользовательские пароли. Если вы ни разу не использовали какую-либо утилиту для взлома паролей, то не поленитесь установить любую демо-версию и проверить стойкость реальных паролей. Вы будете приятно удивлены, узнав через несколько часов ее работы существенную часть паролей пользователей.

Мифы и реальности парольной защиты

Для подкрепления рекомендаций по выбору паролей обычно используют простые расчеты: количество всех возможных паролей заданной длины делят на скорость работы программ перебора (обычно это несколько миллионов паролей в секунду). Полученную стойкость пароля считают достаточной, если расчетное время поиска пароля в несколько раз больше периода его плановой смены.

Однако все такие предположения не учитывают обычной пользовательской практики составления паролей. Во-первых, пользователи крайне редко используют в паролях специальные символы, обычно составляя его из букв (русского или латинского алфавита, причем обычно в пароле встречается только один набор), цифр и, иногда, знаков препинания (точка, тире и т. п.). Формальные требования сложности пароля, контролируемые автоматически, достаточно легко обходятся: пароль просто начинают с заглавной буквы, а в конце добавляют цифру или символ. В результате количество вариантов пароля, которые необходимо перебрать для его подбора, резко уменьшается.

Во-вторых, традиционные рекомендации усложнения паролей — замена одних символов на сходные по начертанию (а на @, о на 0 и т. п.), "выбрасыва-

ние" гласных из слова, используемого в качестве пароля, прямой и обратный порядок букв, осмысленные слова и т. п. — давно учтены в программах перебора (рис. 9.20).

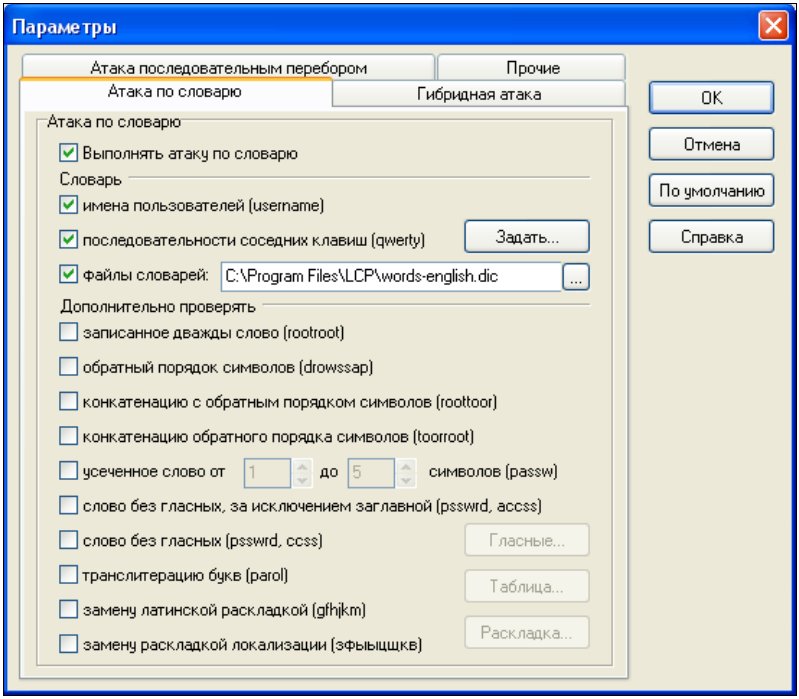


Рис. 9.20. Параметры подбора пароля "учитывают" типовые рекомендации "сложного" пароля

Варианты восстановления забытых паролей

Существуют различные программы, предназначенные для "восстановления" паролей пользователей. Способов получения "первоначальных данных" по паролям много. Это и прослушивание сети (не надо надеяться на использование коммутаторов, поскольку существуют способы "обходить" их фильтрацию пакетов), использование базы безопасности локальной или удаленной машины (при наличии на это устройство административных прав), импорт соответствующих файлов (если есть доступ к данным из другой операционной системы). Программы способны перехватывать и дешифрировать все существующие в настоящий момент протоколы.

На рис. 9.21 представлен результат работы программы LC5 от компании @stake (**www.atstake.com/lc**), которая позволяет узнавать пароли в Windows- и UNIX-сетях. Это данные по реальной сети (имена учетных записей закры-

ты), в которой политикой безопасности включено стандартное требование сложности пароля. Обратите внимание на колонку времени дешифрования каждого пароля — для всех показанных на рисунке учетных записей оно составило менее 50 с. А если просмотреть те пароли, которые были дешифрованы быстрее всех, то основными причинами такого успеха явились действия пользователей, которые составляли пароли на основе своих данных с добавлением цифр (например, пароль `Valentin_1` дешифрирован за 29 с), из простых слов и цифр (например, `Cruel1234` "узнан" за 46 с) или последовательно расположенные клавиши (например, `ASDFGHj1`, 25 с).

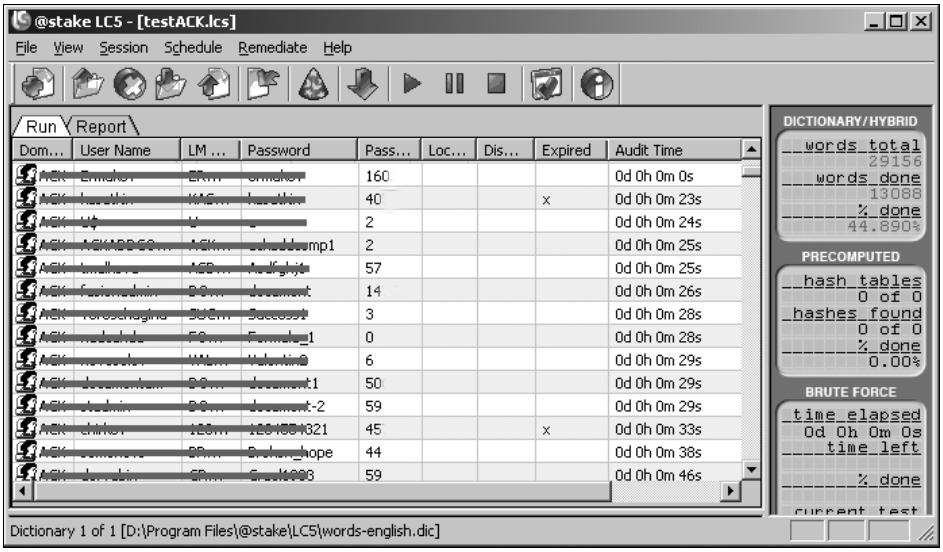


Рис. 9.21. Окно программы восстановления паролей LC5

Rainbow-таблицы

Операционные системы используют не пароли, а их *хэши*, созданные по известным правилам. Параметры вычислительной техники настолько выросли, что у хакеров появилась возможность не перебирать пароли, а составить базу данных хэшей паролей и затем просто выбирать из нее необходимые значения по полученным данным. В результате достаточно узнать (например, перехватить по сети) хэш пароля, выполнить запрос к подобной базе, которую называют Rainbow-таблицей, и получить значение пароля практически сразу.

Программы для использования Rainbow-таблиц доступны в Интернете, единственная проблема их использования заключается в объеме таблиц. В зависимости от набора символов и длины предполагаемого пароля вам придется закачать из Интернета до нескольких десятков гигабайт данных.

Хотя стоит заметить, что с появлением безлимитных тарифов эти объемы стали доступны многим пользователям.

При желании можно создать подобную таблицу и самостоятельно. Так, генератор таблиц Rainbow из состава программы Cain & Abel от Massimiliano Montoro (**www.oxid.it**) позволяет построить таблицу хэшей для паролей, состоящих из всех букв латинского алфавита и цифр, длиной до 8 символов включительно менее чем за полтора дня (рис. 9.22).

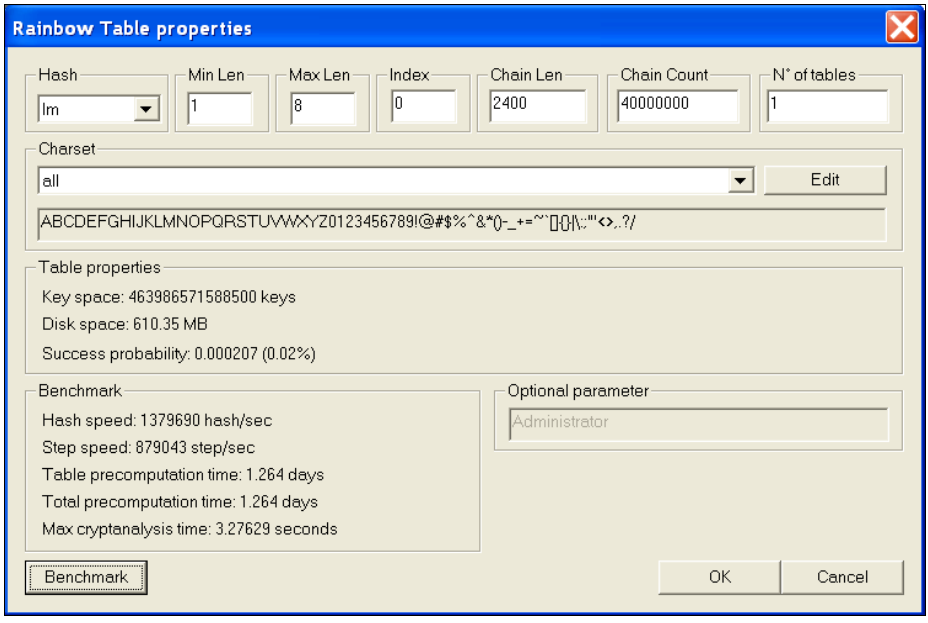


Рис. 9.22. Окно настройки параметров генератора Rainbow-таблицы

Рекомендации по составлению сложного пароля

Все рекомендации, предлагаемые пользователям, должны учитывать их психологию, а не только следовать техническим параметрам. Так, если установить небольшое время жизни пароля (около месяца), то (при одновременном требовании его сложности) это приведет к тому, что пароли начнут записывать, хранить их вблизи компьютера и т. п.

Из описанных ранее примеров атак на пароли следует главный вывод: пароль должен быть *очень* длинным, не менее 15—20 символов. Человеку сложно запомнить произвольную последовательность такой длины, гораздо проще запоминаются *фразы*. Составьте пароль из нескольких слов, разделенных пробелами или знаками препинания. Такой пароль крайне сложно подобрать.

При смене пароля следует перейти к новой фразе, а не модифицировать предыдущую путем добавления нескольких символов в начале или конце.

Ни в коем случае не следует использовать пароль учетной записи для доступа к сайтам Интернета, требующим идентификации. Для упрощения работы с паролями Сети используйте любую программу защищенного хранения паролей.

Технические пути решения проблемы

Организационные меры работы с паролями требуют, насколько это возможно, технического подкрепления. После выполнения рекомендаций по настройке безопасности выполнение ряда параметров будет контролироваться автоматически. Это обеспечит минимальный уровень безопасности.

Для особо ответственных учетных записей (администраторы предприятия и т. п.) необходимо внедрить аппаратные средства аутентификации: смарт-карты, биометрические средства контроля и т. п. Обратите внимание на отсутствие личных послаблений: не отключайте себе те ограничения на пароль (например, необходимость его периодической смены), которые введены для пользователей. Используйте длинный пароль (не менее 15 символов), по возможности один из его символов не должен вводиться с клавиатуры[1].

Совет

Ни в коем случае не используйте пароль администратора предприятия для входа на рабочие станции пользователей. Существует достаточное число утилит, которые, не обнаруживая себя в системе, протоколируют нажатия всех клавиш. При необходимости включите при помощи групповой политики какую-либо учетную запись в число администраторов рабочих станций и используйте эту учетную запись для их администрирования.

Блокировка учетной записи пользователя

Одним из способов борьбы с подбором пароля учетной записи пользователя является ее блокировка после некоторого числа неудачных попыток входа. Эта опция включается через групповую политику организации.

На практике данное правило не имеет особого значения, поскольку прямой перебор паролей пользователя обычно уже не используется. Однако включение ее все же позволит несколько повысить защищенность систем. При этом значение порога числа неудачных попыток набора пароля не должно быть

[1] Иными словами, символ должен набираться через его код: <Alt>+*код*. Перечень таких символов можно найти в справочной документации к операционной системе в разделе, посвященном строгости паролей.

слишком малым. Во-первых, пользователи достаточно часто допускают ошибки при вводе своего пароля. Во-вторых, если такая ошибка будет ими допущена при указании сохраняемого пароля (например, они укажут необходимость сохранения пароля в параметрах доступа к Интернету или к почтовому серверу), то это приведет к нескольким автоматическим повторам ввода неверного пароля и последующей блокировке учетной записи.

Автор рекомендовал бы установить порог блокировки учетной записи на уровне 10—20 неудачных попыток ввода. При этом период, в течение которого будут считаться данные попытки, а также время, через которое произойдет автоматическая разблокировка учетной записи пользователя, можно установить порядка одного часа.

Примечание

Если к учетной записи предъявляются особые требования безопасности, то можно оставить только вариант ее ручного разблокирования, хотя это приведет к увеличению административной нагрузки, в том числе потребует и исследования каждого такого инцидента.

Блокировка учетных записей достаточно часто может возникать вследствие тех или иных неверных настроек, ошибок сохраненных паролей и т. п. Для исследования таких ситуаций можно загрузить комплект утилит — Account Lockout and Management Tools[1] (ALTools.exe), позволяющий проанализировать причины блокировки учетных записей. В комплект входят программы, предназначенные для анализа систем, вызывающих блокировки, средства просмотра параметров учетных записей и поиска данных на контроллерах домена.

LM/NTLM-аутентификация

В целях обратной совместимости серверы поддерживают использовавшиеся ранее протоколы аутентификации. К сожалению, эти протоколы на сегодня не являются безопасными и позволяют злоумышленнику достаточно легко узнать пароли. Например, LM Hash при создании хэша пароля разбивает его на группы по 7 символов, в результате время подбора таких двух пар существенно меньше времени подбора 14-символьного пароля.

Поэтому целесообразно настроить сеть на использование *только* NTLM2-протокола аутентификации. Для этого недостаточно просто включить NTLM2-аутентификацию, следует *отключить* все возможности использования старых методов.

---

[1] **http://www.microsoft.com/downloads/details.aspx?familyid=7af2e69c-91f3-4e63-8629-b999adde0b9e&displaylang=en**.

Переводя домен на использование только NTLM2-аутентификации, следует убедиться, что на всех клиентских системах установлены обновления, позволяющие использовать этот протокол. NTLM2 поддерживается для Windows NT 4.0 после установки SP4. Для систем с Windows 9*x* необходимо инсталлировать клиента службы каталогов с установочного диска Windows 2000.

Примечание

По умолчанию используется вариант шифрования с ключом длиной 56 байт. Чтобы использовать стойкий вариант шифрования на старых системах, необходимо установить MS Internet Explorer 4 или более позднюю версию и дополнить ее поддержкой 128-битного шифрования.

После установки необходимых обновлений следует настроить параметры домена. Во-первых, установить требование использования данного протокола в групповой политике (**Windows Settings | Security Settings | Security Options |** параметры **Network Security**).

Во-вторых, поскольку групповая политика не применяется к клиентам с предыдущими версиями Windows, то следует вручную настроить реестры *каждого такого компьютера*. Для этого необходимо в раздел `HKLM\System \CurrentControlSet\Control` добавить параметр `LMCompatibility:REG_DWORD`. Его значение следует установить равным 3[1] (использовать только NTLM2-аутентификацию).

В-третьих, в политике контроллеров домена следует запретить сохранение NTLM-хэшей, поскольку наличие такого хэша предоставляет злоумышленнику великолепную возможность расшифровки пароля пользователя при наличии доступа к контроллеру домена.

После перевода клиентских систем на использование только NTLM2-аутентификации следует обязательно проверить функционирование всех используемых программ, поскольку в условиях реального предприятия часть старых программ может потребовать сохранения возможности использования LM-аутентификации.

И только тогда, когда вы убедитесь в работоспособности системы, установите для контроллеров домена отказ в обработке LM/NTLM-запросов (определяется параметрами групповой политики).

Смарт-карты

Существуют различные технические решения, которые позволяют аутентифицировать пользователя, не прибегая к вводу пароля, например, по каким-

[1] Полный список значений можно посмотреть, например, в KB239869.

либо биометрическим показателям. Но наиболее используемым на практике методом является аутентификация на основе *смарт-карты*.

Смарт-карта представляет собой устройство, на которое можно с помощью специальных *считывателей* записывать (и считывать) информацию. Обычно на смарт-карте сохраняется сертификат пользователя, предназначенный для аутентификации его в системе. Чтобы сертификат не мог быть использован злоумышленником, он защищается специальным кодом — *PIN-кодом*. PIN-код — это не пароль пользователя в системе, это только защита на случай утери или кражи смарт-карты. Он не передается по сети (поэтому не может быть перехвачен анализаторами трафика) и используется только *локально* для доступа к сертификату. Поэтому он может быть достаточно коротким и удобным для запоминания.

В зависимости от объема памяти на карте, на нее принципиально можно записать несколько сертификатов, что позволит использовать смарт-карту для различных целей (например, вход пользователя в различные системы, хранение сертификатов для электронных подписей и т. п.).

Примечание

Поскольку в смарт-картах применяются сертификаты пользователей, то в организации должна быть развернута структура PKI и опубликованы шаблоны сертификатов для аутентификации пользователей с помощью смарт-карт.

Существуют две возможности записи сертификата пользователя на смарт-карту. Первая — это выполнение операции самим пользователем. В этом случае пользователь должен предварительно войти в систему, используя свой сетевой пароль, после чего начать операцию получения сертификата для аутентификации с помощью смарт-карты. Недостаток этого варианта состоит в необходимости первоначального входа в систему с обычным паролем.

Второй способ предполагает выдачу сертификата администратором. Для этого на компьютер, на котором будет выполняться эта операция, необходимо установить сертификат для выдачи сертификатов пользователям[1]. Чтобы выдать сертификат пользователю смарт-карты в этом случае, необходимо начать операцию запроса сертификата, указав в опциях тип запрашиваемого сертификата — *enroll agent*. Далее на очередном шаге следует выбрать соответствующего пользователя из списка.

Начиная с Windows 2003 Server, смарт-карта может использоваться и для входа в удаленную систему в режиме терминального доступа. Такая возмож-

[1] Так называемый *enroll agent*. Для этого необходимо опубликовать соответствующий шаблон на центре сертификатов и установить сертификат на компьютер. По умолчанию правом установки такого сертификата обладают только администраторы системы.

ность позволяет администратору не использовать свой сетевой пароль при операциях удаленного управления.

Смарт-карту можно использовать в любых операциях[1], требующих аутентификации пользователя. Например, в операции **Run As**. Для этого достаточно раскрыть список выбора пользователей в окне набора пароля, выбрать смарт-карту и набрать ее PIN-код (рис. 9.23).

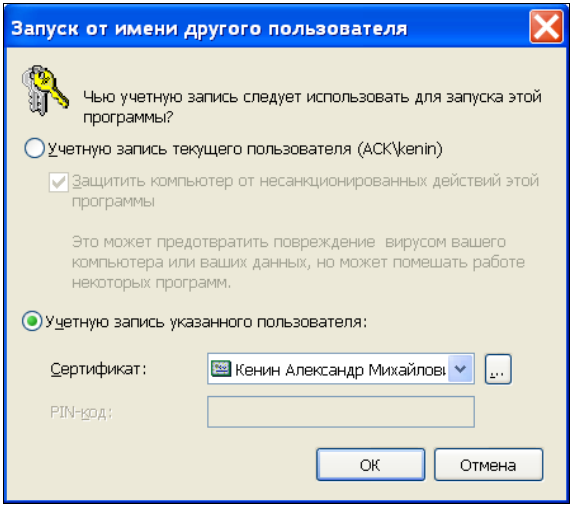


Рис. 9.23. Использование смарт-карты для аутентификации в операции **Запустить от имени…**

В случае предъявления повышенных требований к безопасности администратор может наложить некоторые условия на использование смарт-карт. Так, можно разрешить локальный вход на конкретный компьютер только с использованием смарт-карты (устанавливается через локальную политику безопасности компьютера; кроме того, данное требование можно включить в групповую политику заданного подразделения). Аналогичное требование можно предъявить и к пользователю: разрешить ему работу в системе только с помощью смарт-карты. Это условие реализуется через параметры учетной записи.

Кроме того, можно определить действия, выполняемые системой при вытаскивании смарт-карты (например, автоматически блокировать компьютер или производить отключение пользователя). Эти параметры также настраиваются через групповую политику.

[1] За некоторыми исключениями. Так, у автора не получалось использовать смарт-карту для аутентификации на других компьютерах при удаленной работе на терминальном сервере и т. д.

eToken

Для использования смарт-карт необходимо наличие на компьютерах специального устройства — *считывателя смарт-карт*. В настоящее время такими устройствами в нашей стране оборудована лишь незначительная часть компьютеров. Существует техническое решение, которое позволяет использовать технологию смарт-карт для входа в систему стандартной комплектации. Это eToken (или российский аналог ruToken от компании "Актив", **http://www.rutoken.ru/**, **http://www.guardant.ru/**).

eToken представляет собой компактное USB-устройство. Подключение eToken в USB-порт воспринимается системой как вставка смарт-карты, однако перед использованием eToken нужно установить на систему дополнительный драйвер этого устройства.

Стоимость eToken соизмерима со стоимостью считывателя смарт-карт, но если в организации необходимо обеспечить повышенный уровень безопасности только для отдельных пользователей, то данное решение будет экономически оправданным.

Восстановление пароля администратора

Существует несколько утилит, позволяющих заменить пароль администратора (в том числе и администратора домена). Среди коммерческих вариантов едва ли не самая популярная — это программа ERD Commander (**http://www.winternals.com/**). Программа создает загрузочный компакт-диск, который позволяет не только заменить пароль администратора, но и отредактировать настройки реестра системы, использовать сетевой доступ для копирования файлов (после загрузки система "видит" сеть) и выполнить другие операции конфигурирования систем на основе Windows NT/200*x*/XP/Vista/.

Среди бесплатно распространяемых программ можно отметить Offline NT Password Editor (**http://home.eunet.no/~pnordahl/ntpasswd/**), которая неоднократно успешно применялась автором для восстановления паролей на Windows NT 4.0, серверах и рабочих станциях Windows 2000, Windows XP. По информации с сайта программы ее можно использовать и для Windows Vista. Эта программа предоставляется в виде образа загрузочного CD с операционной системой Linux. Стартовав с такого диска, вы получаете доступ к реестру системы и можете заменить любой пароль. По умолчанию опции программы предполагают смену пароля локального администратора. Так что вам достаточно только соглашаться с предложениями программы на каждом ее шаге.

После того как пользователь заменит пароль администратора, он получит *полный* контроль над компьютером.

Человеческий фактор

В связи с постоянно совершенствующимися техническими мерами обеспечения безопасности злоумышленники все активнее начинают использовать для получения данных об информационной системе методы социальной инженерии. Представляясь новым работником или специалистом службы техподдержки, коммерческим агентом или интервьюером, можно попытаться получить сведения о структуре сети и расположении информационных сетевых служб, ознакомиться с действующими мерами обеспечения безопасности данных и т. п. В случае получения недостаточного объема информации от одного сотрудника, злоумышленник легко может обратиться ко второму, третьему и т. д. Широко распространены попытки использования различных анкет, запросов по электронной почте.

Исполнения каких правил поведения должны постоянно придерживаться сотрудники организации?

Не давать никакой информации в ответ на любые обращения по телефону, по электронной почте, при личных контактах лицам, если нет четкой уверенности в правомочности таких запросов.

Не сообщать никакой информации как личного, так и служебного характера в различных анкетах на страницах информационных серверов Интернета или пришедших по электронной почте.

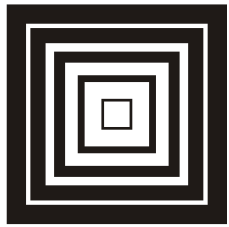
Не отвечать на любые не ожидаемые рассылки по электронной почте, даже если в письме содержится указание на возможность прекращения подписки. Не пересылать писем, содержащих служебную информацию, по почте в незашифрованном виде.

При работе в Интернете внимательно следить за URL сайтов, чтобы быть уверенными в работе с конкретной организацией (а не с сайтом, созвучным по написанию с реальной организацией, например имеющим адрес ***организация*.org** вместо ***организация*.net**).

Не посещать сайты, предоставляющие сертификат (по протоколу HTTPS), к которому у операционной системы компьютера нет доверия (высвечивается желтый знак предупреждения).

При контактах с сотрудником, впервые представившимся вам по электронной почте, принять меры к проверке его данных. При этом не следует пользоваться контактными данными, опубликованными в Интернете; проверьте данные о фирме иными путями, например, через справочные службы.

При обнаружении подобных попыток получения информации необходимо сообщать об этих фактах соответствующим работникам своей организации.



ГЛАВА 10

Виртуализация

Термин *виртуализация* в последнее время стал очень популярным. Говорят о виртуальной памяти, о виртуальных дисках, о виртуализации систем хранения данных и т. п. В рамках настоящего раздела под виртуализацией мы будем понимать создание независимых сред на одном компьютере для запуска различных операционных систем.

Почему виртуализация приобретает все большую популярность? Это вызвано тем, что ИТ-специалисты предпочитают оставлять каждому серверу только по *одной* задаче. Причин для этого много: при такой архитектуре катастрофический сбой одной службы не повлияет на функционирование других; в случае, если обновление программного обеспечения разрушит систему, другие задачи не пострадают; некоторые программы несовместимы друг с другом и специалисты хотят обезопасить себя от конфликтов, которые могут обнаружиться только в ходе эксплуатации и т. д.

Негативным следствием такого подхода является низкий процент использования возможностей оборудования. Если вы посмотрите, например, на загруженность процессора среднего сервера за некоторый промежуток времени, то вряд ли она будет составлять более 10—20%. То же можно сказать и про другие параметры. В этой ситуации применение *виртуальных* компьютеров может реально сэкономить средства организации за счет снижения количества "физических" серверов при повышении коэффициента использования существующего оборудования.

Виртуальный компьютер (или виртуальная машина, VM) представляет собой программу, которая позволяет запустить независимо друг от друга несколько операционных систем на одном компьютере, например, Windows 98 и Windows XP, Windows Server и Linux. Благодаря возросшей вычислительной мощности современных компьютеров и возможностям наращивания, администратор, используя технологии виртуальной машины, может на одном компьютере смоделировать практически любые конфигурации.

Программы виртуальных машин

Виртуальные машины представлены различными продуктами и реализованными в них подходами.

Лидером рынка виртуализации сегодня являются продукты VMware (www.vmware.com). Решения от VMware обеспечивают полную виртуализацию, имеются специальные драйверы, использующие аппаратные возможности платформ для повышения производительности виртуальных машин. Линейка представлена как свободно распространяемыми, так и коммерческими продуктами.

XEN Source (**www.xensource.com**, **www.virtualiron.com**) является лидером в направлении паравиртуализации и спонсором открытого проекта XEN. Программное обеспечение XEN работает *между* оборудованием и операционной системой, это некий *гипервизор* компьютера. В качестве базовой операционной системы в XEN выступает Linux. Особенностями данного продукта является возможность запуска немодифицируемых операционных систем на виртуальных машинах.

Широко используется для виртуализации операционных систем продукция SWsoft (**www.swsoft.com**, **www.openvz.com**, **www.parallels.com**). На базе линеек Virtuozzo для Windows и Linux имеется открытый проект OpenVZ. Программное обеспечение предоставляет удобное управление виртуальными машинами, причем код открыт для сторонних разработчиков. Поддерживается миграция систем в реальном режиме времени. Этой же компании принадлежит линейка Parallels, отличительной особенностью которой является виртуальная машина для MacOS.

Активную позицию заняла и компания Microsoft (**www.microsoft.com**), которая в силу распространенности своих продуктов будет оказывать серьезное влияние на развитие виртуализации. Сегодня в линейке Microsoft присутствуют как рабочие станции (Virtual PC), так и виртуальные серверы (Virtual Server). Предполагается, что в новой серверной операционной системе виртуализация будет встроенной[1].

Сегодня любая организация сможет выбрать для себя наиболее удобный и бесплатный продукт, который позволит внедрить средства виртуализации.

Виртуальный сервер или рабочая станция

Хотя виртуальные машины рабочих станций и серверов во многом идентичны, существуют некоторые отличия. Виртуальные рабочие станции предна-

[1] Хотя появиться она должна только через полгода после официального выпуска Windows Server 2008.

значены, в первую очередь, для отработки тех или иных решений. При помощи программы управления виртуальной машиной легко подключить к ней дополнительный ресурс в виде папки "основного" компьютера, можно копировать данные в виртуальную машину и наоборот, сохранять промежуточные конфигурации, к которым можно выполнить откат в случае необходимости и т. п.

Виртуальные серверы по большей части предназначены для постоянной работы операционной системы виртуальной машины. Возможности управления виртуальной машиной в них несколько сокращены, но зато присутствуют такие опции, как динамическое управление потребляемыми ресурсами, автоматический запуск виртуальной машины в случае перезагрузки основного компьютера и т. п.

Наиболее подходящий продукт выбирается в зависимости от назначения виртуальной машины в каждом конкретном случае. На практике возможен перенос виртуальной машины между системами управления различных производителей. Это позволяет администраторам в каждом случае использовать оптимальные варианты управления.

Лицензирование программного обеспечения виртуальных машин

При лицензировании программного обеспечения, используемого на виртуальных машинах, возникает много сложностей, особенно с лицензиями от Microsoft, применение которых не очевидно и в обычных условиях. Эта книга не посвящена вопросам практики лицензирования ПО, поэтому конкретные разъяснения необходимо уточнять на сайте разработчика (например, **http://www.microsoft.com/licensing/highlights/virtualization.mspx**).

Главное, что необходимо отметить — использование виртуальных сред не всегда требует приобретения дополнительных лицензий[1]. Так, лицензия на Windows Server 2003 R2 Enterprise Edition позволяет в один момент времени иметь один работающий физический сервер и 4 виртуальных. А лицензия на SQL 2005 Server (в варианте Server/CAL) Workgroup Edition, Standard Edition and Enterprise Edition разрешает запускать любое количество инстанций на сервере. Таких примеров можно привести много, лучше всего особенности лицензирования уточнять по документам изготовителя ПО.

---

[1] См. документ Microsoft "Licensing Microsoft Server Products with Microsoft Virtual Server and Other Virtual Machine Technologies" (**http://download.microsoft.com/download/6/8/9/68964284-864d-4a6d-aed9-f2c1f8f23e14/virtualization_brief.doc**).

Ресурсы виртуальных машин

Виртуальная машина, называемая *гостевой операционной системой*, использует ресурсы основного компьютера, носящего название *хост*.

Жесткие диски

К виртуальной машине может быть подключено несколько жестких дисков. Каждый жесткий диск представляет собой либо файл основного компьютера, либо его реальный раздел.

Программы управления позволяют эмулировать как IDE, так и SCSI-диски. Если вы создаете новую виртуальную машину, то для повышения производительности предпочтительнее выбирать вариант SCSI-устройств.

К создаваемой виртуальной машине можно подключить уже существующий диск (например, сделать копию файла виртуального диска). Таким образом легко клонировать виртуальные машины: достаточно создать шаблоны образов диска, на которые далее дополнительно устанавливать необходимые для полигона приложения.

Примечание

Образ диска Windows содержит уникальные идентификаторы операционной системы члена домена. Хотя и существуют специальные утилиты (см., например, **http://www.microsoft.com/technet/sysinternals/Security/NewSid.mspx**), позволяющие менять эти идентификаторы при клонировании жесткого диска, наиболее оптимальным вариантом является создание копии диска компьютера, не являющегося членом домена (выведенного из домена), переименование системы и последующее присоединение к домену. Еще один корректный способ заключается в использовании утилиты sysprep при подготовке виртуального диска к клонированию *(см. разд. "Автоматизация установки программного обеспечения" главы 14)*.

По умолчанию программа предлагает создать виртуальные жесткие диски достаточно большого размера (например, 16 Гбайт). Реально размер файла виртуального диска динамически увеличивается в зависимости от объема копируемой на него информации вплоть до указанного в настройках максимального значения. В процессе работы виртуальной машины файл диска может существенно превысить реально используемые значения, поэтому рекомендуется периодически проводить сначала дефрагментацию жесткого диска средствами гостевой операционной системы, после чего выполнить оптимизацию файла диска командами программы управления виртуальной машиной[1].

[1] Эта операция есть во всех программах управления, но может называться по-разному. Например, в VMware присутствует команда *дефрагментации* виртуального диска.

Примечание

Эти операции достаточно ресурсоемки и занимают длительное время. В связи с этим их следует планировать на периоды, когда виртуальную машину можно надолго отключить. Принципиально возможен еще один вариант сжатия диска путем создания его копии при помощи программы дублирования жестких дисков. В этом случае новый образ диска не будет включать в себя пустых участков.

Виртуальный диск может быть создан не только в процессе установки или путем копирования уже имеющегося образа. Существует несколько программ, при помощи которых можно сохранить образы жесткого диска реального компьютера, созданные в наиболее популярных программах, в формате виртуального диска. Например, файл виртуального диска может быть отредактирован программой WinImage версии 8 и старше (**http://www.winimage.com/**).

Ограничения по числу виртуальных дисков на одном компьютере определяются только свободным пространством жесткого диска основного компьютера. Однако следует учитывать падение производительности из-за одновременной работы с жестким диском нескольких систем. Вы можете даже получить сообщения об ошибках (тайм-ауты) дисковых операций. В этом случае можно либо распределить нагрузку по нескольким физическим дискам, либо применить более производительную систему хранения.

Откат состояния виртуальной машины

Программы управления виртуальными машинами имеют возможность включения функций отката: программа сохраняет в том или ином виде все изменения и позволяет в случае необходимости вернуться к предыдущему моменту времени.

Данную функцию следует использовать с осторожностью, поскольку при ее выполнении резко увеличивается задействование жесткого диска основного компьютера.

Использование реального жесткого диска в виртуальной машине

В виртуальной машине можно вместо файла виртуального жесткого диска использовать реальный физический. Однако для этого в системе необходимо иметь как минимум два диска — один для основного компьютера, второй — для размещения данных виртуальной машины.

Кроме того, в некоторых программах управления виртуальными машинами есть ограничения на одновременное использование на одном канале двух разных типов дисков (например, на одном канале IDE нельзя подключить

один реальный диск и один виртуальный CD-ROM). Данные особенности следует уточнить по сопроводительной документации.

Процессор

Виртуальная машина запускается как еще один процесс основной операционной системы. Несколько запущенных виртуальных машин будут делить между собой один процессор.

В случае виртуального сервера администратор имеет возможность регулировать выделяемые ресурсы: устанавливать относительные веса каждой виртуальной машины и определять максимальную загрузку процессора. Для виртуальной рабочей станции обычно можно только включить/выключить максимальный приоритет активной машины или установить "замораживание" виртуальной машины в фоне.

Примечание

Процессоры с поддержкой технологии hyper-threading отображаются в операционной системе как два процессора. Данная технология позволяет несколько повысить общую производительность системы, но в случае создания виртуальных машин очень часто она *ухудшает* производительность, особенно при высокой загрузке процессора. Поэтому отключите поддержку технологии hyper-threading в BIOS компьютера, который предполагается использовать для размещения виртуальных машин.

64 и 32

Если говорить о виртуальных машинах от Microsoft, то существуют версии программного обеспечения, обеспечивающего работу виртуальных машин, для установки как на 64-битную операционную систему, так и на 32-битную. Однако сами виртуальные машины могут быть только 32-битными.

В случае использования программного обеспечения VMware вы можете устанавливать 64-разрядную гостевую операционную систему.

Оперативная память

Обычно именно память является ограничителем количества одновременно запускаемых на одном компьютере виртуальных машин. Для каждой виртуальной машины необходимо выделить в ее настройках соответствующий объем памяти. Если на момент запуска виртуальной машины требуемого объема памяти не окажется, то ее старт не состоится. В этом случае можно, во-первых, попытаться уменьшить объем выделенной памяти до допустимого предела, во-вторых, закрыть приложения основного компьютера, чтобы высвободить используемую ими оперативную память.

Совет

После неудачной — из-за отсутствия свободной памяти — попытки запуска виртуальной машины можно через некоторое время повторить процедуру. Достаточно часто операционная система в этом случае высвобождает занимаемую память, сохраняя данные в файле подкачки, и появляется возможность запуска виртуального компьютера.

Виртуальные машины VMware позволяют освобождать неиспользуемую память, копируя данные на диск подобно виртуальной памяти основного компьютера. В результате можно одновременно запустить больше виртуальных машин, однако при этом увеличивается количество операций чтения/записи на жесткий диск, что сказывается на производительности как основной системы, так и виртуальных.

CD/DVD

К виртуальной машине может быть подключено несколько устройств чтения CD/DVD. В них можно заменять диски во время работы виртуальной машины, давая соответствующие команды управления (проще всего щелкнуть правой кнопкой мыши по пиктограмме диска в строке состояния и выбрать желаемую операцию).

Кроме того, в качестве диска можно подключать и образы CD/DVD, указывая путь к соответствующим файлам. Такой способ можно легко применить для копирования файлов с основного компьютера на виртуальный сервер Microsoft (программы создания образов CD выполняют создание файла диска очень быстро).

Сетевые адаптеры

Каждая виртуальная машина может иметь несколько виртуальных сетевых адаптеров. Настройки программы управления позволяют подключить эти адаптеры к реальной сети несколькими способами.

Во-первых, можно создать *мост*. В этом случае данные из сети, для которой настроен виртуальный адаптер, будут маршрутизироваться в сеть, к которой подключена сетевая карта компьютера, и наоборот. Второй вариант предусматривает использование технологии NAT для доступа к сети реального компьютера. Он позволяет не беспокоиться за возможные конфликты присваиваемых адресов (или за наличие свободных IP-адресов в случае автоматического назначения параметров виртуального адаптера), но имеет некоторые технические ограничения.

Третий способ заключается в создании изолированной сети. При этом виртуальные машины на одном физическом компьютере будут "видеть" по сети

только друг друга. Этот способ удобен при построении изолированного полигона.

Примечание

В случае необходимости каждый адаптер виртуальной машины может быть настроен по своему способу подключения к сети.

Один реальный сетевой адаптер можно использовать для работы в сети большого числа виртуальных компьютеров. В Интернете я встречал информацию о запуске на компьютере более 10 виртуальных систем, разделяющих одну физическую сетевую карту. Следует только учитывать, что при увеличении количества виртуальных машин полоса пропускания сетевого адаптера будет *распределяться* между ними, снижая скорость работы по сети каждой отдельной виртуальной машины.

В настоящее время существенная часть материнских плат выпускается с двумя сетевыми адаптерами, а стоимость отдельного сетевого адаптера также невелика. Поэтому оптимальным решением будет разделять одну сетевую карту для виртуальных машин, а вторую использовать для работы основной системы.

Порты

К виртуальной машине могут быть подключены последовательный и параллельный порты компьютера. При использовании программы от VMware возможно подключение и USB-портов (не поддерживается в Microsoft Virtual PC).

Безопасность

Для ограничения использования виртуальных машин только определенным кругом лиц следует установить права доступа на каталоги с их файлами. Файлы виртуальных дисков и конфигураций при использовании продуктов Microsoft имеют расширения: vhd — виртуальный жесткий диск, vnc — файл сетевой конфигурации, vmc — основная конфигурация.

Доступ к странице управления виртуальным сервером Microsoft определяется в настройках информационного сервера. По умолчанию задействован встроенный механизм аутентификации (Integrated Windows), предотвращающий доступ анонимных пользователей. Включение режима основной аутентификации (Basic) необходимо только в случаях использования виртуального сервера не в условиях домена.

Примечание

Рекомендуется использовать управление виртуальной машиной только по защищенным каналам связи (SSL), как при работе на административной страни-

це, так и через консоль управления (VMRC, Virtual Machine Remote Control). Этот совет особенно актуален при переключении на стандартный режим идентификации, поскольку в этом случае имена пользователей и их пароли доступа будут пересылаться по сети в *открытом* виде.

Если виртуальная машина[1] размещена за межсетевым экраном, то следует открыть на нем порты 5900 (порт по умолчанию для управления), 1024 (порт по умолчанию для открытия страницы администрирования на Web-сервере), порты 137 и 138 для TCP и UDP (используются при аутентификации).

При создании новой конфигурации пользователь должен определить тип операционной системы, которую предполагается установить в этой конфигурации, и задать некоторые параметры настройки (объем выделяемой виртуальной машине памяти, возможность "отката" своих действий и т. п.). После запуска конфигурации программа выводит окно, имитирующее экран компьютера, в котором необходимо выполнить первоначальную установку операционной системы точно так же, как на отдельном физическом компьютере: форматирование диска, выбор устанавливаемого ПО, регистрация компьютера в домене и т. п.

Расширения виртуальных машин

Сделать работу с виртуальной машиной более удобной — использовать мышь как в хосте, так и в гостевой операционной системе; иметь возможность копировать данные между ними; динамически менять размер окна отображения и т. п. — можно, установив *расширения* виртуальных машин (virtual machine additions) после инсталляции операционной системы виртуальной машины. После запуска команды установки расширений, находящейся в меню программы управления, к виртуальной машине подключается CD-ROM, с которого производится запуск установки. После завершения процедуры установки и перезагрузки виртуальной машины становятся доступными описанные выше функции.

Примечание

Процедуру установки расширений в случае использования операционных систем, отличных от Microsoft, следует выполнить вручную. Для систем Linux данная процедура описана в *разд. "Тестирование Linux на виртуальной машине" главы 2*. Обратите внимание, что расширения для Linux-систем появились и в виртуальном сервере от Microsoft. Их можно загрузить со страницы **http://www.microsoft.com/downloads/details.aspx?FamilyID=BF12642F-77DC-4D45-AE4E-E1B05E0A2674&displaylang=en**.

[1] Описываемые ниже примеры относятся к MS Virtual PC.

Автоматический запуск виртуальных машин

При использовании виртуального сервера можно настроить автоматический запуск виртуальных машин после перезагрузки основной системы. Такой вариант возможен только при определении учетной записи, с правами которой будет запускаться виртуальная машина.

Виртуальные рабочие станции также можно запускать автоматически, если настроить соответствующие параметры командной строки и поместить необходимый вызов в автозагрузку. Однако такой старт будет происходить только после входа пользователя в систему.

Выключение виртуальных машин

Существует несколько возможностей выключения виртуальной машины. Во-первых, можно завершить работу виртуальной машины выключив ее с сохранением данных при помощи команды **Завершить работу**. Во-вторых, можно сохранить состояние виртуальной машины. В этом случае ее работа как бы заморозится; после восстановления вы сможете продолжить операции. Такой способ напоминает переход в режим сна (hybernate). В-третьих, можно просто "выключить" питание виртуальной машины, выполнив команду turn off. При последующем запуске возможна потеря несохраненной информации.

Примечание

При переводе ноутбука в режим сна рекомендуется сначала сохранить состояние виртуальной машины.

Обычно при использовании виртуального сервера отдельные машины настраивают на автоматический запуск после включения основного компьютера и сохранение состояния при его выключении. Если на вашем компьютере размещено несколько виртуальных машин, то процесс их выключения с сохранением данных может существенно затянуться. В результате основная операционная система воспримет такую ситуацию как зависание прикладной программы с отсутствием ответа в течение заданного промежутка времени. Виртуальная машина будет аварийно завершена, что может вызвать проблемы при ее следующей загрузке. Чтобы зарезервировать время на сохранение параметров виртуальных машин в случае перезагрузки основной системы, измените значение параметра реестра `WaitToKillServiceTimeout` в ветви `HKLM\SYSTEM\CurrentControlSet\Control\`, установив необходимое время ожидания.

Операции в виртуальных машинах

Копирование

Виртуальные машины поддерживают копирование данных методом "drag and drop". Однако копировать данные можно только из виртуальной машины на основную или наоборот. Если вам необходимо скопировать данные между несколькими виртуальными машинами, их следует сначала скопировать, например, на рабочий стол основного компьютера, и только потом — в другую виртуальную машину.

Подключение папки основного компьютера к виртуальной системе

На рабочих станциях в качестве сетевого ресурса виртуальной машины можно подключить любую папку основного компьютера даже при отсутствии у нее подключения к сети, рис. 10.1.

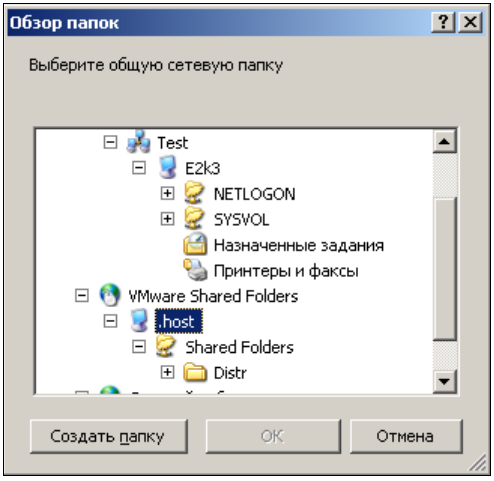


Рис. 10.1. Подключение папки хоста к гостевой машине для совместного использования

Эту операцию можно выполнить или при помощи соответствующих команд программы управления, или щелкнуть по пиктограмме на панели состояния виртуальной машины в нижней части окна и указать параметры совместно используемой папки.

Подключение CD, дискет и других устройств чтения/записи

Эти операции также удобно выполнять через соответствующие пиктограммы в строке состояния. Достаточно щелкнуть по пиктограмме и указать, например, образ CD-ROM, который необходимо "вставить" в дисковод виртуальной машины.

Сочетание управляющих клавиш

Для посылки сочетания <Ctrl>+<Alt>+<Del> виртуальной машине обычно используется <Ctrl>+<Alt>+<Ins>. Кроме того, данную команду можно вызвать из меню управления виртуальной машиной.

Без установки расширений при щелчке мышью внутри окна виртуальной машины курсор мыши начинает перемещаться *только* в пределах виртуальной машины. Чтобы "освободить" его, по умолчанию используется правая клавиша <Alt>.

Переключение между режимами отображения виртуальной машины в окне и в полном экране осуществляется нажатием сочетания правой клавиши <Alt>+<Enter>.

Совместимость программного обеспечения с виртуальными системами

Виртуальная машина, естественно, отличается от реальной системы. Поэтому возможны случаи, когда использовать виртуальную машину для запуска определенных приложений невозможно.

В случае возникновения проблем с настройкой программного обеспечения следует проверить на сайте изготовителя наличие или отсутствие проблем совместимости. Например, в KB897614 отмечается, что с Microsoft Virtual Server несовместимы следующие продукты самого изготовителя: Microsoft Speech Server, Microsoft ISA Server 2000/2004, Microsoft SharePoint Portal Server, Microsoft Identity Lifecycle Manager 2007, Microsoft Identity Integration Server 2003, Microsoft Identity Integration Feature Pack. Часть продуктов (см. KB897613) поддерживается только после установки определенного пакета обновлений: Microsoft Certificate Services, Microsoft Exchange Server, Microsoft Systems Management Server и т. д.

Создание виртуальных машин

Не обязательно создавать новую виртуальную машину путем установки гостевой операционной системы с нуля. Программы управления предлагают различные варианты ускорения операций.

Миграция компьютера на виртуальную машину

Достаточно часто встречается необходимость перенести на виртуальную машину реально работающую систему. Обычно программы создания виртуальных машин позволяют выполнить такую операцию.

На виртуальную машину Microsoft Virtual Server 2005 подобный перенос осуществляется с помощью дополнительного программного обеспечения — Virtual Server Migration Toolkit. VSMT позволяет перенести работающую систему *только* на англоязычную версию Virtual Server в редакции Enterprise (Virtual PC не поддерживается), при этом в системе должна быть развернута служба Automated Deployment Services (ADS). Естественно, что такие требования не всегда реализуемы в небольших организациях, прежде всего, по финансовым соображениям.

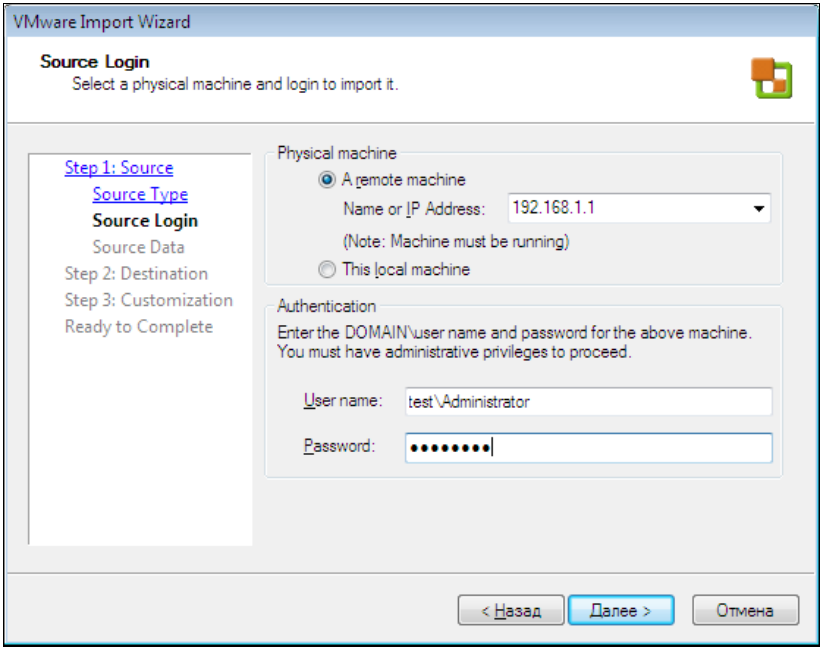


Рис. 10.2. Импорт реальной системы на виртуальную машину при помощи мастера

Более удобно использовать в этих целях виртуальные машины от VMware. Они имеют специальные мастера, которые позволяют мигрировать рабочую систему на виртуальную машину (рис. 10.2).

Создание виртуального диска как копии физического

Программы управления виртуальными машинами позволяют создать виртуальный жесткий диск-копию работающей системы. Эта операция обычно выполняется при помощи мастера создания жесткого диска, но иногда она "запрятана" достаточно далеко и соответствующие шаги не очевидны. Рассмотрим необходимые операции для создания виртуальной машины в Microsoft Virtual PC на основе работающей системы.

Операция создания виртуального диска на основе копирования существующего физического проводится в два этапа. На первом этапе создается виртуальный диск-ссылка на физический. На втором этапе этот диск преобразуется в динамически расширяемый виртуальный диск.

Для создания диска-ссылки откройте программу Virtual PC и выберите в меню **File** команду **Virtual Disk Wizard**. После начала работы мастера запустите вариант **Create a new virtual disk** и укажите **A virtual hard disk**. Не вводя имя диска, нажмите кнопку **Browse**, выберите путь для создаваемого файла виртуального диска и введите его имя. Сохраните настройки (**Save**) и продолжите работу мастера, нажав на кнопку **Next.**

В параметрах виртуального диска — **Virtual Hard Disk Options** — укажите опцию **Linked to a hard disk (Advanced)**. Подтвердите запрос программы, после чего укажите жесткий диск, на основе которого предполагается создать виртуальный. Завершите операцию (**Finish**).

На втором этапе преобразуйте полученный диск в динамически расширяемый. Для этого *снова* запустите мастер создания виртуального диска (**File | Virtual Disk Wizard**). Выберите опцию редактирования существующего диска (**Edit an existing virtual disk**), укажите на сохраненный в ходе первого этапа операций файл и выполните операцию **Open**. Далее укажите вариант **A dynamically expanding virtual hard disk** и путь, где нужно сохранить созданный виртуальный диск. Завершите операцию (**Finish**). В зависимости от размеров физического диска процесс создания виртуального может занять существенное время.

Примечание

Для создания виртуального диска описанным способом необходимо иметь не менее двух дисков: сохранить файл виртуального диска на тот же физический диск, с которого копируется информация, невозможно.

Контроль параметров производительности

Анализ параметров производительности гостевой операционной системы имеет некоторые особенности.

Счетчики производительности

Для анализа производительности системы часто используется снятие показаний счетчиков производительности. В случае виртуальных машин необходимо пользоваться счетчиками не самой виртуальной машины, а параметрами специального объекта основной операционной системы. Например, в случае VMware Workstation он носит название "VMware" (рис. 10.3).

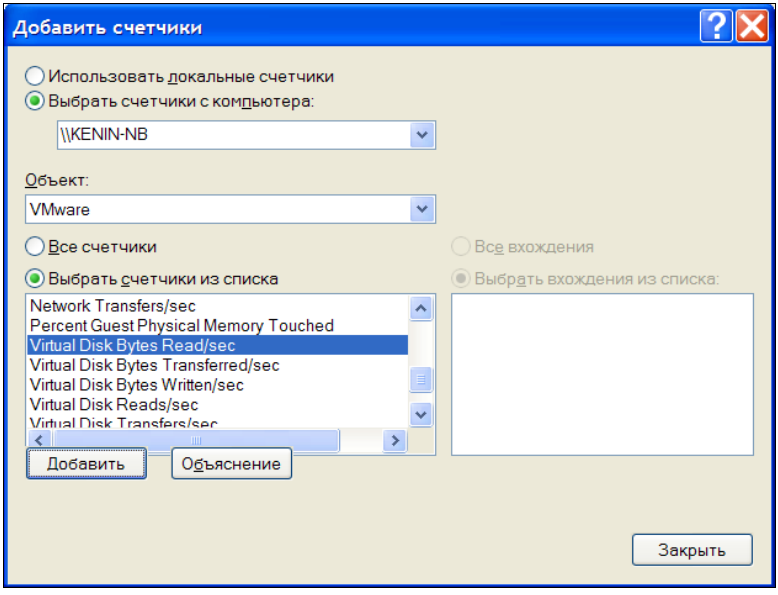


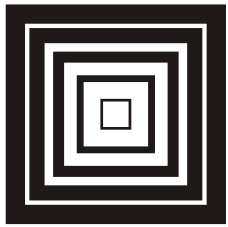
Рис. 10.3. Выбор счетчиков для оценки производительности виртуальной машины

Следует выбрать данный объект в списке программы **Производительность** и добавить для просмотра необходимые значения (показатели активности жесткого диска, использования оперативной памяти и т. п.).

Советы по повышению производительности виртуальных систем

Следующие советы помогут улучшить показатели работы систем, особенно в случае запуска на одном компьютере нескольких виртуальных машин:

- используйте для размещения файлов виртуальных дисков быстрые физические диски. По возможности применяйте решения на SCSI-дисках или RAID-массивах. При наличии в системе нескольких физических дисков распределяйте по ним файлы гостевых операционных систем равномерно;
- вместо динамически расширяемых виртуальных дисков используйте диски фиксированного размера;
- отключите поддержку технологии hyper-threading в BIOS основного компьютера;
- периодически дефрагментируйте виртуальные диски средствами установленных на них операционных систем, после чего производите дефрагментацию файла виртуального диска средствами программы управления;
- не включайте на виртуальных машинах различные визуальные эффекты, 3D-эффекты и т. п;
- установите два сетевых адаптера: один используйте для основной системы, другой разделите между всеми виртуальными машинами.



ГЛАВА 11

Порядок настройки и определения неисправностей

Отказы информационной системы все в большей степени влияют на эффективность бизнес-процессов предприятия, поэтому одна из главных задач администратора работающей системы состоит в *предупреждении* отказов и максимальном сокращении времени простоя обслуживания.

Прежде чем начать...

Если отказ все же случился, не спешите сразу же начинать что-то *делать*. Попробуйте успокоиться, может быть, выпить кофе и только после этого приступать к активной деятельности.

Прежде всего, попытайтесь получить о неисправности максимум информации как от пользователей, так и по данным объективного контроля. Составьте предварительный перечень возможных причин отказа с оценкой времени устранения по каждой позиции. Старайтесь не начинать ремонт с наиболее затратных позиций, если только вы абсолютно не уверены, что именно они явились причиной неисправности.

Протоколируйте все свои шаги. Часто, если систему не удается восстановить за короткое время, без таких записей очень сложно вернуться к начальной точке.

Если вы долго не можете справиться с отказом, попробуйте рассказать о неисправности кому-либо еще. Во-первых, пытаясь объяснить проблему, вы разложите ее для себя "по полочкам". Во-вторых, советы неспециалистов часто могут направить вас на неожиданный путь решения.

Обязательно составьте какой-нибудь документ по результатам инцидента, чтобы специалисту, который придет на ваше место, было легче ориентироваться в состоянии системы.

Пять девяток

Цель, которую ставят изготовители оборудования и разработчики программного обеспечения, — достичь доступности информационной системы на "пять девяток" — 99,999%. При круглосуточной работе этот показатель соответствует примерно пяти минутам простоя *за год*.

Конечно, достижение такого показателя требует весьма существенных затрат как на соответствующее оборудование, так и на обслуживание, нереальных для малых и средних организаций. В то же время в силах системного администратора как наладить работу по предупреждению отказов, так и создать условия для оперативного восстановления информации.

Отказ в обслуживании может возникнуть вследствие отказа любого элемента системы: повреждения кабельной системы, неполадок в работе коммутирующих устройств, выхода из строя узлов компьютера, зависания операционной системы, ошибок программного обеспечения бизнес-уровня и уровня приложений и т. п.

- **Неисправности кабельной подсистемы.**

  Автору несколько раз на практике приходилось сталкиваться с ситуацией, когда сбои в работе программ (ошибки копирования файлов, "зависания" приложений, работающих с сетевыми ресурсами, и т. п.) вызывались некачественными кабельными соединениями. Причем подобные неисправности могут иметь достаточно случайный характер (например, при переломе кабеля и восстановлении/пропадании сигнала при незначительном изгибе).

  Обычно места возникновения таких неисправностей легко локализуются. Достаточно проверить участки кабельной структуры, рядом с которыми велись те или иные строительные работы, и проконтролировать патч-корды пользователей (особенно те, которые имеют следы перегибов и т. п.). Тем более, что средства диагностики (индикаторы на сетевых адаптерах и коммутаторах) позволяют сразу же найти отказавший сегмент.

Примечание

Если в вашей организации создана отказоустойчивая структура сети с дублированием каналов и устройств, то следует регулярно проверять ее состояние при помощи любой программой сканирования сети, способной обнаруживать изменения топологии. В противном случае единичный отказ не будет обнаружен, и вы столкнетесь с серьезной аварией в случае второго отказа.

- **Неисправности активного (коммутационного) оборудования.**

  Несмотря на часто декларируемую "пожизненную" гарантию, активные устройства (концентраторы, коммутаторы, маршрутизаторы, кабельные

модемы и т. п.) могут зависать, выходить из строя, неадекватно вести себя в особых ситуациях.

Заподозрить неисправность такого устройства достаточно сложно именно по причине малой вероятности подобных отказов. Но уже после первого обнаруженного отказа детектирование последующих случаев не вызывает сложностей.

- **Неисправности аппаратной части компьютеров.**

  Это весьма тяжело детектируемые неисправности, особенно если происходят достаточно случайно. Обычно стараются резервировать (с возможностью горячей замены) наиболее часто отказывающие узлы — жесткие диски и блоки питания.

  Жесткие диски обычно объединяют в RAID-массивы того или иного уровня с возможностью горячей замены. При необходимости жесткой экономии можно создать такие массивы программным способом и использовать SATA-диски. Поскольку RAID обычно конфигурируется с избыточной надежностью, то единичный отказ жесткого диска сохраняет работоспособность устройства хранения. Администратору необходимо либо постоянно следить за состоянием RAID, либо автоматизировать получение предупреждения о возникновении отказа, иначе второй отказ может привести к краху системы.

  Применение систем с резервированием других узлов (например, памяти) часто экономически не оправдано. Если необходимо обеспечить работоспособность службы при выходе из строя аппаратной части компьютера, обычно применяют *кластерные* решения (параллельная работа нескольких компьютеров; обзор данных решений выходит за рамки этого издания). Прежде всего, это касается серверов баз данных, почтовых систем и т. п.

- **Ошибки программного обеспечения.**

  Основная часть отказов Windows-систем связана с ошибками в программном обеспечении. Как уже говорилось, это могут быть ошибки самой операционной системы или использованного прикладного продукта.

  Если проблема возникала только один раз, то выявить ее причины обычно практически невозможно. Если событие повторилось, то администратору следует тщательно проанализировать всю сопутствующую информацию и выявить события, связанные с инцидентом. Чем тщательнее будет проведен предварительный анализ, тем больше вероятность точного решения. Следует попытаться изолировать данную неисправность от других событий и составить необходимый план действий, предусматривающий возможность операций "отката", если лечение проблемы вызовет другие отказы.

Кроме непосредственного решения возникшей проблемы администратор должен обратиться к поиску аналогичных инцидентов и рекомендаций по их разрешению в той или иной базе знаний.

Где найти помощь

Устранение неисправностей в информационной системе практически невозможно без обращения к внешним источникам знаний. Существует несколько ресурсов, где системный администратор может получить "подсказку".

- **Windows Help.**

  Первое, к чему необходимо обратиться при возникновении любой проблемы в работе компьютера, — это встроенная справочная система. С каждой новой версией Windows эти системы становятся все более содержательными и полезными (если только вы знаете, что хотите найти, и правильно формулируете условия поиска).

- **Resource Kit.**

  Если необходима информация, уточняющая те или иные аспекты настройки операционной системы, описывающая тонкости ее использования, то следует обратиться к документации, содержащейся в пакете программ Resource Kit.

  Resource Kit — это дополнительный набор утилит, которые предназначены для опытных пользователей и администраторов систем. Например, пакет для Windows Server содержит утилиты, которые позволяют протестировать процессор в режиме максимальной загрузки, зарегистрировать программу в качестве службы, выполнить различные операции управления компьютером в режиме командной строки с использованием сценариев и т. п. Обычно в состав пакета включено несколько сотен таких утилит.

  Кроме этого, в пакете присутствует справочная документация, которая подробно описывает функционирование различных служб операционной системы. Если вы испытываете сложности в настройке определенных функций Windows, то в данной документации обычно можно найти необходимое пояснение.

  Пакет Resource Kit существует только на английском языке, так что для его использования необходимо обладать хотя бы минимальным знанием технического английского языка.

- **Онлайновая база данных Microsoft.**

  Громадный объем документации содержится на сайте корпорации Microsoft по адресу **http://msdn.microsoft.com/**. В различных разделах этого ресурса вы можете найти как описания работы отдельных компонентов

операционной системы, так и технические статьи, содержащие сведения об обнаруженных ошибках и методах их устранения.

Онлайновая справочная база Microsoft локализована. Страницы с русской версией сайта корпорации можно найти по адресу **http://www.microsoft.com/rus/**, однако следует учитывать, что англоязычные материалы публикуются оперативнее переводов.

- **Материалы Интернета.**

Способы разрешения многих проблем, особенно если таковые случились не только у одного пользователя, можно найти на многочисленных сайтах сети Интернет. В первую очередь это специализированные сайты, посвященные конкретным прикладным вопросам, сайты известных специалистов, другие серверы, на которых хранятся различные справочные материалы (например, на многих серверах Сети хранятся ответы на типовые вопросы по функционированию системы — FAQ). Такие ресурсы легко находятся при помощи обычных поисковых серверов Интернета.

- **Конференции Интернета.**

Если вы не нашли описания своей проблемы на таких узлах Сети, то можно обратиться с соответствующим вопросом в специализированную телеконференцию. Не стоит надеяться, что вы гарантированно получите ответ, но обращение в конференцию является одним из наиболее эффективных способов получения необходимой помощи. Обычно, ту или иную подсказку по проблеме удается найти поиском по сообщениям в тематической конференции.

Примечание

Подобные конференции обычно поддерживаются как на сайтах разработчиков, так и на других ресурсах, посвященных компьютерной тематике. Определенную помощь может оказать изучение списка конференций, поддерживаемых новостным сервером вашего провайдера.

- **Техническая поддержка производителя.**

Крупные производители программного обеспечения имеют специализированные службы для оказания технической поддержки. Обращение в такую службу обычно помогает существенно сократить время решения возникшей проблемы, особенно если уровень подготовки технических специалистов на предприятии недостаточен для квалифицированного сопровождения инфраструктуры.

Обычно подобная поддержка является платной услугой, причем уровень цен не позволяет заказывать ее малым и средним организациям. Постепенно начинает развиваться сервис коммерческого предоставления технической поддержки третьими фирмами. К сожалению, в этом вопросе очень

много субъективных факторов, влияющих на качество такого сопровождения, поэтому решение о приобретении пакета данной поддержки должно приниматься индивидуально с учетом анализа опыта других предприятий.

Обнаружение неисправностей сетевой инфраструктуры

С одной стороны, неисправности кабельной системы достаточно легко обнаружить. Существуют специальные сканеры, которые тестируют кабельные линии связи и сообщают, удовлетворяет ли линия заданному стандарту или нет (см., например, рис. 3.7). Если, например, превышена величина допустимого затухания сигнала, то можно сначала попробовать заменить коннекторы на концах линии. Если это не поможет, то следует проложить новое соединение. С другой стороны, такие тестеры достаточно дороги, и далеко не каждая даже крупная организация их имеет. Хотя для тестирования кабельной подсистемы можно привлечь внешнюю фирму, но, учитывая достаточную дороговизну таких работ, часто основные неисправности пытаются выявить собственными силами.

Минимальным средством проверки кабельной витой пары является обычный тестер. С его помощью можно проверить целостность пар проложенного кабеля. Обычно администраторы изготавливают (из кабельной розетки) оконечное устройство, в котором замыкают пары кабеля. В результате диагностику можно провести, измеряя сопротивление между жилами только с одного конца.

Примечание

Косвенным признаком целостности кабеля может служить индикатор на сетевом адаптере. Если он горит, то кабель, скорее всего, исправен, в противном случае следует искать повреждения на линии.

Для анализа состояния инфраструктуры можно использовать программы, предназначенные для мониторинга сетевого трафика. Одна из наиболее популярных и функциональных программ этого класса — это Observer производства Network Instruments, LLC (**www.networkinstruments.com**).

Примечание

Программа для мониторинга сети из состава Windows (Network Monitor) позволяет перехватывать пакеты, передаваемые по сети, но не содержит серьезных средств анализа полученных данных. Observer — коммерческий продукт, но для проведения анализа состояния сети можно воспользоваться бесплатно предоставляемой версией ограниченного срока пользования (trial-версией).

На рис. 11.1 представлен фрагмент окна программы Observer, которое отображает данные по пропускной способности портов маршрутизатора. Для их получения используются стандартные параметры SNMP для маршрутизатора; информация запрашивается и отображается на графике каждые 2 секунды. Четко видно, что загрузка одного из портов составляет в среднем 70—80%. Фактически это означает исчерпание ресурсов пропускной способности канала (на рисунке показаны данные маршрутизатора, установленного на канале доступа в Интернет с ограниченной пропускной способностью).

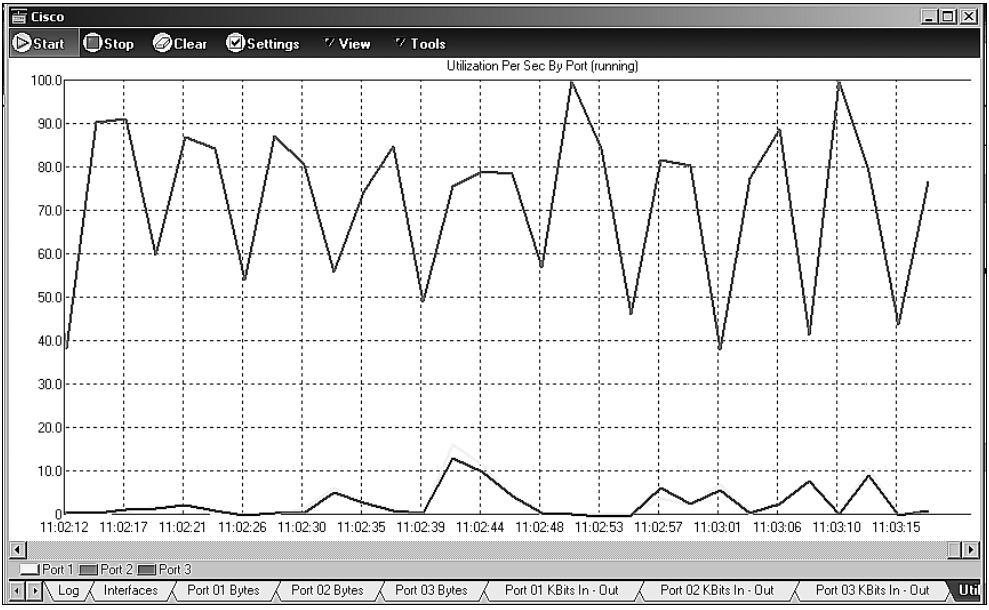


Рис. 11.1. Мониторинг состояния сети по SNMP

Примечание

На рис. 11.1 показано окно коммерческой программы, однако аналогичные данные могут быть получены и при помощи бесплатных утилит. Например, на сайте **www.mrtg.org** можно найти программу Multi Router Traffic Grapher (и ее исходные коды) для отображения данных статистики маршрутизатора. Изначально программа предназначалась для Linux, но имеется также ее бесплатная версия для Windows, работающая на Perl.

Объем данных, которые можно получить о работе активного оборудования удаленно, зависит от установленных моделей и должен быть уточнен по технической документации.

При проведении анализа сети обратите внимание на перечисленные далее параметры.

- **Коэффициент использования пропускной способности сети.**

  Сеть Ethernet обеспечивает уверенную работу при загруженности не более 30—40%. При увеличении нагрузки резко возрастает число коллизий в сети, падает реальная производительность системы. Если какие-либо сегменты показывают высокую нагрузку, то следует предпринять меры для расшивки этого узкого места. Например, заменить сетевое оборудование на более производительное, подключить агрегированные каналы связи[1].

- **Число ошибочных пакетов.**

  Сниффер[2] позволяет получить данные о числе коллизий в интересуемых сегментах, о числе пакетов, содержащих те или иные ошибки (ошибки CRC, слишком малые или слишком длинные пакеты и т. п.). Соответствующая статистика может быть получена в разрезе каждого отдельного сетевого устройства.

  При нормальной работе число ошибочных кадров не должно превышать десятых долей процента передаваемой информации. Обычно большой процент ошибок контрольной суммы свидетельствует о низком качестве сети (контакты, помехи в кабеле, неисправности портов оборудования). Неверные длины пакетов — признак неисправности сетевых адаптеров и их драйверов.

- **Величина коллизий.**

  В нормально работающей сети величина коллизий не должна превышать нескольких процентов. Большая величина — это признак низкого качества сети (локальные коллизии), наличие ошибок адаптеров или неверного проектирования сети (late collision[3]).

- **Загрузка маршрутизаторов.**

  С помощью программы-сниффера можно получить данные о загрузке маршрутизаторов и других устройств, применяемых в сети предприятия. Эта статистика позволит судить о реальной нагрузке и наличии в системе узких мест (см. рис. 11.1).

Примечание

Обычно программы типа Observer можно использовать и для оценки загруженности серверов приложений. Часто такие программы имеют собственные гене-

---

[1] Технология объединения каналов соответствует стандарту IEEE 802.3ad. В связи с наличием некоторых дополнений (например, объединение каналов не на одном, а на различных коммутаторах) может иметь проприетарное название (EtherChannel и т. п.).

[2] Сетевой анализатор. Программа, которая перехватывает передаваемые по сети пакеты и позволяет анализировать полученные данные.

[3] Late collision — это коллизия, обнаруживаемая после передачи первых 64 байтов. Причиной late collision часто бывает большое количество повторителей в локальной сети.

раторы пакетов, которые позволяют проанализировать время отклика удаленных систем в зависимости от частоты запросов.

Неисправности аппаратной части компьютера

Легко обнаружить неисправность аппаратной части компьютера, если она приводит к его полной неработоспособности, тогда как выявить "исчезающую" неисправность, обусловленную проблемами "железа", крайне сложно. Как правило, компьютер в таких случаях прекрасно проходит специальное тестирование, но все же более-менее постоянно "подвисает" на определенных задачах.

В случае подозрения на аппаратную неисправность необходимо вначале выполнить следующие операции:

1. Обновить BIOS материнской платы компьютера до последней версии изготовителя.
2. Выполнить чистую установку операционной системы (без каких-либо "лишних" прикладных программ), после чего установить все обновления от ее изготовителя.
3. Установить последние версии драйверов[1] для материнской платы, видеоадаптера и т. п.
4. Если неисправность наблюдается в прикладном программном обеспечении, то следует установить его и все имеющиеся для него обновления.

После выполнения этих операций нужно попытаться воспроизвести неисправность. Если неисправность продолжает периодически возникать, то такой блок следует передать на техническое обслуживание.

Примечание

На практике часто встречаются случаи, когда простая замена одних узлов на аналогичные даже той же модели ликвидирует такие исчезающие неисправности.

По опыту работы, наиболее ненадежными узлами компьютерных систем являются жесткие диски. Следующей часто встречающейся причиной нестабильной работы является некачественная память. Отказывают и материнские платы, и процессоры, и периферийные устройства.

---

[1] Драйверы оборудования прилагаются к системному блоку. Вам следует обязательно проверить наличие на сайте производителя новых версий, и если они обнаружены, то скачать и установить именно их. Обратите внимание, что при наличии сертифицированных версий и новых разработок (бета-версии) следует устанавливать только последние сертифицированные варианты.

Часто причиной нестабильной работы компьютера бывает тепловой режим блока.

Контроль теплового режима работы системы

Одним из самых ненадежных узлов компьютера являются вентиляторы охлаждения. Они используются для поддержания необходимого теплового режима процессора, видеоадаптера, в блоке питания и т. п. Количество вентиляторов варьируется в зависимости от модели компьютера.

Обычно через полтора-два года эксплуатации компьютера дешевые модели вентиляторов снижают скорость вращения лопастей или даже могут полностью остановиться. Современные материнские платы имеют в поставке программы, которые автоматически контролируют скорость вращения вентиляторов и температурный режим внутри системного блока. При наличии таких программ их следует обязательно установить и своевременно реагировать на их сообщения. При отсутствии средств контроля необходимо периодически[1] визуально контролировать скорость вращения лопастей вентилятора и своевременно заменять[2] неисправные.

Примечание

На процессорах Intel Pentium 4 предусмотрен специальный термодатчик. Если он зафиксирует превышение определенного температурного порога, то процессор автоматически перейдет на пониженную скорость работы, чтобы снизить температуру и не допустить выхода элементов из строя.

Температура внутри корпуса компьютера может повыситься не только из-за ухудшения качества вентиляторов. Так, причиной перегрева могут стать дополнительные устройства (дополнительные жесткие диски), установленные в компьютер. Вполне возможно, что конструкция корпуса просто не рассчитана на такое количество оборудования. Свою лепту вносят и крайне жаркие дни, количество которых постоянно увеличивается в последние годы.

Все эти причины могут привести к перегреву компьютера и, как следствие, возникновению сбоев в его работе или даже выходу из строя.

В оценочных целях можно использовать следующие цифры. Температура внутри корпуса компьютера обычно на 15—20 градусов превышает температуру окружающей среды, поэтому администратор должен начать предпринимать срочные меры, если температура внутри серверного шкафа превысит (ориентировочно) 30 °C.

---

[1] При каждом вскрытии системного блока.

[2] Допустимо смазывать оси вентиляторов специальной смазкой. Но после такой операции следует проверять данные вентиляторы не реже одного раза в три-четыре месяца.

Восстановление данных с жестких дисков

В Windows не предусмотрено никаких штатных средств для лечения жестких дисков, кроме программы `chkdsk`. Эта утилита позволяет проверить целостность файловой системы и "закрыть" сбойные участки жесткого диска, но практически бесполезна в случае серьезных повреждений.

Наиболее часто применяемыми средствами для восстановления информации с жестких дисков являются программы Easy Recovery (Ontrack Data Recovery, Inc., **www.ontrack.com**) и GetDataBack (RunTime Software, **www.runtime.org**).

Эти программы позволяют восстановить данные даже с тех дисков, которые не определяются в BIOS компьютера. Имеются возможности восстановления диска после форматирования, "сборки" файлов на основе их типа и т. п.

Использование данных программ достаточно очевидно. Сначала производится анализ структуры жесткого диска, предлагается определить восстанавливаемый раздел и тип файловой системы, после чего начинается поиск информации. Найденный список можно при необходимости отфильтровать по тем или иным критериям (например, восстанавливать только файлы документов), а затем выполнить восстановление.

Примечание

Восстановление всегда производится на другой диск, чтобы не повредить исходные данные. Поэтому при отсутствии сетевых подключений необходимо позаботиться о дополнительном устройстве хранения.

Если возникли дефекты устройства хранения данных (чаще всего переносные устройства — дискеты, реже — жесткие диски, компакт-диски), то обычно повреждается лишь небольшой участок файла. Но это, как правило, приводит к тому, что соответствующий файл не открывается в программе его редактирования.

Для восстановления таких поврежденных файлов разработано много утилит, которые можно найти в Сети. При этом чем популярнее формат файлов данных, тем больше вероятность того, что для этого типа информации существуют утилиты восстановления. Например, существуют утилиты восстановления для офисных файлов (Microsoft Word, Excel, Access, PowerPoint), для файлов личных папок офиса (pst), архива (zip), баз данных (dbf) и т. п. Версии этих утилит меняются с модификацией основных программ, поэтому я отошлю читателя к самостоятельному поиску в Интернете.

Принцип работы таких утилит достаточно прост. Они анализируют структуру файла, находят поврежденный блок данных и восстанавливают структуру файла так, чтобы он мог быть открыт в основной программе с минимальными потерями.

Восстановление "упавших" систем

Если операционная система на базе Windows NT перестала нормально загружаться, то администратор имеет несколько возможностей восстановления ее работоспособности штатными средствами:

- загрузка в безопасном режиме;
- загрузка последней удачной конфигурации — вариант загрузки выбирается после нажатия клавиши <F8> в момент старта системы;
- восстановление системы из консоли восстановления;
- восстановления из программы установки.

  Если администратор готов к возможным отказам, то он сможет запустить процесс восстановления с использованием сохраненных настроек и данных (например, *режим автоматического восстановления*). Эта операция возможна при запуске процесса установки ОС с дистрибутивного компакт-диска.

  Если у администратора нет сохраненных настроек, то можно попытаться провести восстановление системы путем новой установки в режиме восстановления *(см. разд. "Режим восстановления в Windows XP с сервис-паком" далее в этой главе)*;
- использование программ сторонних разработчиков.

  Существует большое количество программ, реализующих дополнительные возможности восстановления, например, путем создания точек восстановления и последующего "отката" к ним неисправной системы при загрузке с соответствующего компакт-диска *(см. разд. "Использование программ типа ERD Commander" далее в этой главе)*.

Загрузка в безопасном режиме

В варианте загрузки в безопасном режиме можно решить следующие проблемы:

- ошибки конфигурации системного программного обеспечения;
- сбои из-за установки новых устройств или программ, в том числе и ошибки, возникшие вследствие установки сервис-паков и обновлений.

Загрузка последней удачной конфигурации

Загрузка последней удачной конфигурации поможет в случаях:

- ошибок конфигурации во время последней сессии;
- установки неверного драйвера устройства.

Думаю, что каждый администратор не раз использовал эти режимы, и необходимости более подробного объяснения нет.

Консоль восстановления

За длительную практику автора подавляющее большинство случаев отказа загрузки систем на базе Windows NT было связано с нарушениями структуры жесткого диска (повреждения загрузочного сектора, загрузочных и системных файлов) или с последствиями установки новых устройств (драйверов). Эти неисправности можно устранить при помощи *консоли восстановления* (recovery consol), появившейся в версии Windows 2000[1].

Примечание

Перед тем как использовать консоль восстановления, необходимо попытаться загрузить систему в одном из описанных выше безопасных режимов или в режиме последней удачной конфигурации.

Консоль восстановления — это режим командной строки, в котором можно загрузить проблемную операционную систему. В этом режиме доступен ограниченный набор команд, с помощью которых можно выполнить операции настройки системы и восстановления структуры жесткого диска. Так, можно восстановить загрузочные секторы, скопировать любые файлы с компакт-диска на жесткий диск, выполнить проверку диска (и устранить ошибки) с помощью программы `chkdsk`, изменить параметры запуска служб операционной системы (например, отключить ту или иную службу) и т. п. Полный перечень команд доступен при вызове справки в режиме командной строки (`help /?`).

Консоль восстановления можно добавить заблаговременно как дополнительный вариант загрузки операционной системы, если вызвать команду установки операционной системы с ключом `/cmdcons` (`i386\winnt32.exe /cmdcons`).

Обычно же необходимость использования консоли восстановления возникает внезапно, когда на вашем компьютере отсутствует соответствующий вариант загрузки. В этом случае в режим консоли восстановления можно перейти следующим способом:

1. Укажите в BIOS компьютера вариант загрузки с компакт-диска.
2. Вставьте в устройство чтения компакт-дисков дистрибутив операционной системы[2] и начните с него установку Windows.

---

[1] Начиная с Windows Vista, в качестве среды восстановления используется Windows PE *(см. разд. "Варианты восстановления Windows Vista" далее в этой главе)*.

[2] При необходимости можно использовать загрузочные CD и другой версии операционной системы.

3. Когда программа установки спросит, что вы хотите выполнить, выберите операцию восстановления операционной системы.
4. На следующем шаге выберите вариант загрузки консоли восстановления.

Программа проанализирует установленные на жестком диске операционные системы, а затем предложит вам выбрать каталог, в котором находится восстанавливаемая версия, и ввести пароль, соответствующий учетной записи администратора.

Примечание

Если папка установки системы (файлы реестра) повреждена, то вы попадете в командную строку программы без запроса пароля. В этом случае следует обязательно проверить и восстановить структуру диска. Если на компьютере повреждена загрузочная область жесткого диска, то для входа в консоль восстановления (если под рукой нет компакт-диска с дистрибутивом) приготовьте загрузочные дискеты для соответствующей версии Windows и включите в файл boot.ini следующую строчку:

```
C:\CMDCONS\BOOTSECT.DAT="Windows Recovery Console" /cmdcons
```

Перечислим основные операции, которые приходится выполнять в режиме консоли восстановления.

- **Восстановление загрузочных областей диска.**

  Для этой цели следует использовать команды `fixboot` и `fixmbr`.

Примечание

Если у вас на диске установлена только одна операционная система, то можно проигнорировать предупреждения, которые будут выводиться командами.

- **Восстановление отсутствующих загрузочных или системных файлов.**

  Поскольку в режиме консоли восстановления доступен привод CD-ROM, то вы можете просто скопировать нужные файлы с дистрибутива в соответствующие папки. Обратите внимание, что буквы логических дисков в режиме консоли восстановления могут не совпадать с названием логических дисков в работающей системе. Вам следует ориентироваться, например, по размерам дисков, находящимся в них папкам и т. п.

- **Проблемы со службой (драйвером нового устройства).**

  Воспользуйтесь командой `listsvc` для отображения списка служб и устройств и командой `enable` для отключения подозрительных служб (драйверов).

- **Восстановление структуры жесткого диска.**

  Выполняется стандартно с использованием команды `chkdsk`. Единственное, что программа может запросить у вас, — вручную указать путь к

файлу библиотек, используемому при запуске этой утилиты (если повреждена системная папка; следует указать папку на компакт-диске).

- **Нарушения реестра.**

  Часто система не может загрузиться из-за нарушений структуры реестра, причем не помогает даже выбор последней удачной конфигурации. Попробуйте вручную восстановить последнюю копию той ветви реестра, о которой сообщает программа загрузки[1]. Для этого перейдите в каталог SYSTEM32\CONFIG, найдите файл реестра и переименуйте его (по умолчанию текущие файлы не имеют расширения), после чего скопируйте (переименуйте) одноименный файл с расширением sav в файл без расширения. Другое место, откуда можно взять файлы копий реестра системы, — это точки восстановления *(см. разд. "Восстановление реестра из файлов точек восстановления системы" далее в этой главе)*.

  После выполнения операции перегрузите систему в нормальном режиме.

Добавление новых типов устройств хранения в консоль восстановления

Если компьютер загружается с устройства хранения данных, драйвер которого не входит в стандартную поставку Windows, то для входа в режим консоли восстановления необходимо нажать клавишу <F6> и вставить дискету с драйверами изготовителя устройства. Например, при использовании RAID-контроллера или загрузке с жесткого диска SATA.

Во-первых, это неудобно: нужно искать дискету с драйверами. Во-вторых, не всегда возможно. Так, в практике автора был случай, когда необходимо было использовать консоль восстановления на системе с RAID-контроллером, но без дисковода A:\.

В подобных случаях следует добавить вручную данные драйвера к списку устройств. Для этого нужно модифицировать дистрибутив операционной системы.

Вначале в том же каталоге, где находится папка I386, нужно создать папку OEM, а в ней — папку Textmode. В папку Textmode нужно скопировать все файлы от изготовителя, необходимые для установки дополнительного устройства. Обычно это файлы <*driver*>.sys, <*driver*>.dll, <*driver*>.inf, <*driver*>.cat, txtsetup.oem, хотя в конкретном случае могут присутствовать не

[1] Поврежденные файлы реестра можно заменить и с помощью ERD Commander *(см. разд. "Использование программ типа ERD Commander" далее в этой главе)*. Но если файл реестра сохранил структуру и программа ERD Commander открыла его, то у пользователя не будет возможностей для его замены, кроме полного отката к точке восстановления.

все файлы[1] (<*driver*> соответствует названию файла от изготовителя оборудования). Скопируйте также эти файлы в папку PnP-драйверов.

В файле ответов, который используется для установки системы, создайте секцию `[MassStorageDrivers]` и включите в нее названия устройств по следующему образцу:

```
"Adaptec 2940..." = "OEM"
```

Эта строка должна соответствовать данным секции `[SCSI]` файла изготовителя оборудования txtsetup.oem.

В файле ответов создайте также секцию `[OEMBootFiles]` и перечислите в ней все файлы, находящиеся в папке Textmode:

```
[OEMBootFiles]
<driver>.sys
<driver>.dll
<driver>.inf
<driver>.cat
Txtsetup.oem
```

Убедитесь, что в файле ответов в секции `[Unattended]` присутствует выражение `OemPreinstall=Yes`.

Примечание

Файл txtsetup.oem должен содержать раздел идентификации оборудования для PnP-устройств — `[HardwareIds.scsi.`*yyyyy*`]`, где *yyyyy* соответствует названию службы. Если такого раздела нет, его нужно добавить. Описание соответствующих операций можно найти в файле deploy.chm на дистрибутивном диске системы.

Включить в файл txtsetup.sif драйверы, которые необходимо загрузить на первом этапе установки системы, можно и прямым редактированием. Хотя эта операция предполагает несколько дополнительных шагов, она может быть выполнена для существующей установки (см., например, **http://greenmachine.msfnhosting.com/READING/addraid.htm**).

Режим восстановления в Windows XP с сервис-паком

В Windows XP SP2 существует возможность восстановления работоспособности системы в режиме восстановления программы установки. Часто этот способ является самым простым для неподготовленного пользователя.

[1] Список всех необходимых файлов легко уточнить, если просмотреть содержимое файла txtsetup.oem.

Если система перестала запускаться, загрузите ее с установочного CD и начните установку. После того как вы укажете для установки диск, на котором операционная система была установлена ранее, программа обнаружит это и предложит произвести *восстановление*. При подтверждении выбора данного режима установка продолжится, внешне не отличаясь от обычной, однако после ее завершения вы обнаружите, что все ранее установленные программы сохранили свою работоспособность.

Режим восстановления не доступен, если:

- для восстановления используется не тот вариант дистрибутива, с которого была установлена система (например, делается попытка восстановления с дистрибутива на другом языке);
- в системе возникли серьезные повреждения (например, разрушения файловой структуры, в результате чего программа не может обнаружить папки установленной системы).

После такого восстановления необходимо сразу же установить все обновления, имевшиеся на исходной системе, поскольку в противном случае возможно возникновение ошибок в работе.

Варианты восстановления Windows Vista

В состав Windows Vista включена специальная среда для восстановления операционной системы, которая запускается при загрузке компьютера с установочного диска. В некотором смысле это аналог консоли восстановления Windows XP, только исполненный на основе Windows PE (Windows Preinstallation Environment), который сменил "загрузочные дискеты" Windows, и содержит ряд *автоматизированных* операций по восстановлению загрузки.

Для использования средств восстановления необходимо загрузиться с установочного диска Windows Vista. При обнаружении проблем система автоматически начнет операции проверки, пытаясь восстановить работоспособность (рис. 11.2).

Восстановление реестра из файлов точек восстановления системы

Последние версии ОС автоматически сохраняют значения основных настроек в *точках восстановления*. Восстановление прежних настроек штатно предусмотрено только при работе операционной системы (в Vista — также при загрузке с CD). Однако администратор может использовать сохраненные параметры в режиме консоли восстановления или запустить программы типа ERD Commander, позволяющие выполнить откат к точке восстановления в режиме загрузки с компакт-диска (рис. 11.3).

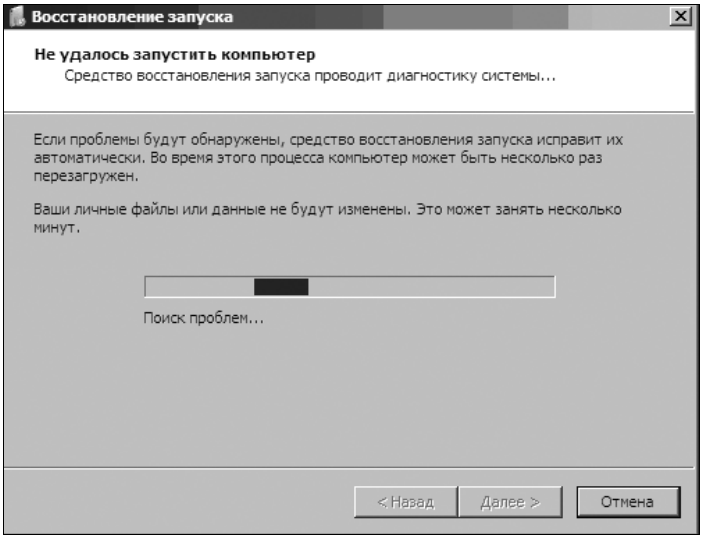


Рис. 11.2. Попытка автоматического восстановления системы

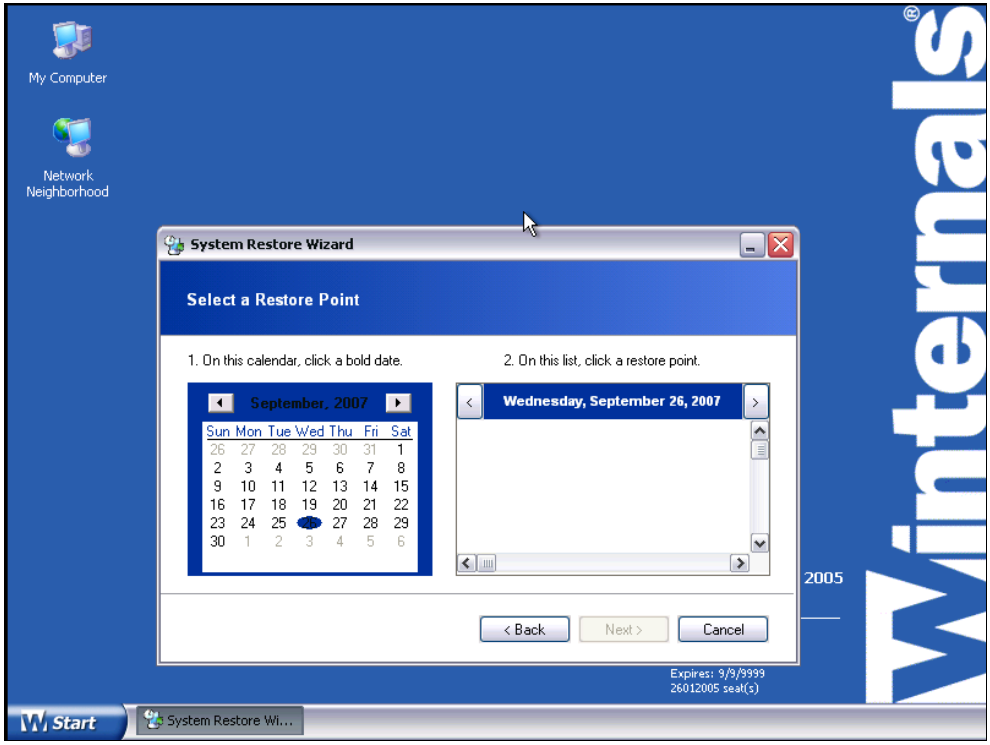


Рис. 11.3. Мастер отката к предыдущим точкам восстановления системы при загрузке с внешнего CD (пакет ERD Commander 2005)

Значения реестра системы сохраняются в папках точек контрольного восстановления системы — System Volume Information. Эти параметры обычно более точно соответствуют последним настройкам системы, чем копии реестра, например, в папке \Windows\Repair[1]. По умолчанию (при использовании NTFS) содержимое папки с точками восстановления недоступно пользователю. Чтобы получить доступ к этим данным в режиме нормальной работы ОС, необходимо добавить текущему пользователю соответствующее право на папку System Volume Information, например:

```
cacls "C:\System Volume Information" /E /G <имя_пользователя>:F
```

При работе в консоли восстановления права доступа не контролируются, поэтому в указанную папку можно "зайти" с помощью обычных команд.

В папке System Volume Information сохраняются данные точек восстановления в каталогах с именами, аналогичными _restore{CFA91D90-58C3-4176-A156-29790E9DAF6B} (после restore идет значение GUID).

Следует зайти в папку, которая соответствует самой поздней дате восстановления, открыть в ней каталог RP*номер* и зайти в папку snapshot.

В папке snapshot сохранены файлы реестра, правда, под именами, отличающимися от тех, которые используются в папке конфигурации. Поэтому для замены файлов реестра администратору необходимо скопировать файлы, перечисленные в табл. 11.1, в папку \Windows\System32\Config и переименовать их так, как указано в правом столбце.

Таблица 11.1. *Соответствие имен файлов*

Имя файла в папке восстановления	Имя файла после переименования
_REGISTRY_USER_.DEFAULT	DEFAULT
_REGISTRY_MACHINE_SECURITY	SECURITY
_REGISTRY_MACHINE_SOFTWARE	SOFTWARE
_REGISTRY_MACHINE_SYSTEM	SYSTEM
_REGISTRY_MACHINE_SAM	SAM

Примечание

К сожалению, программа копирования режима консоли восстановления не поддерживает использование масок, поэтому для копирования нескольких файлов придется выполнить соответствующее число операций. Также в этом режиме

[1] Здесь и далее в примерах этого раздела считается, что система установлена в папку C:\Windows. Иначе следует заменить название каталога.

не работает функция завершения набора имени файла по первым символам, что потребует точного ручного ввода всех используемых в операциях имен файлов и папок.

Использование программ типа ERD Commander

Специально для восстановления проблемных систем были разработаны программы, позволяющие выполнить загрузку компьютера с компакт-диска и получить доступ к жесткому диску системы. Самой известной программой такого типа является пакет ERD Commander от Winternals Software LP (**www.winternals.com**).

ERD Commander 2005[1] позволяет выполнить запуск системы с компакт-диска в оболочке, внешне идентичной интерфейсу Windows XP. После запуска пользователь получает доступ к жесткому диску (может просматривать файлы, редактировать их, сбросить права доступа к файловым объектам и т. п.), имеет возможность выполнять сетевые операции (можно предоставить папки для совместного доступа и подключиться к другим ресурсам). Можно выбрать любую точку отката из числа сохраненных и восстановить состояние системы на момент ее создания. Есть возможность заменить пароль администратора. Доступны оснастки управления службами системы (можно изменить тип запуска и т. п.) и другие возможности.

Автор встречался с несколькими версиями "доработанных" загрузочных дисков, в которых были добавлены опции запуска популярных прикладных программ (файловых менеджеров, программ восстановления диска и т. п.). В случае необходимости подобное расширение функций может осуществить и сам администратор, редактируя образ CD, сформированный данной программой.

На взгляд автора наличие программы типа ERD Commander должно быть обязательным в арсенале системного администратора.

Восстановление удаленных данных

Восстанавливать один-два файла, удаленных пользователем, из резервной копии — занятие неблагодарное, прежде всего из-за длительности операции (обычно объемы файлов резервных копий составляют несколько гигабайт). Удобнее воспользоваться технологиями, позволяющими восстанавливать

[1] ERD Commander является частью пакета Administrator's Pak (на момент подготовки книги последняя версия этого пакета была 5), который содержит целый набор утилит для восстановления систем. Например, утилиту Remote Recover, позволяющую запустить компьютер с дискеты и подключить его локальные диски к удаленной консоли. Таким образом можно выполнить операции (заменить файлы, сбросить пароль администратора и т. п.), необходимые для восстановления системы.

удаленные данные. Это программы-аналоги Корзины Windows, технология Volume Shadow Copy и различные утилиты для восстановления данных.

Корзины

"Штатная" Корзина Windows малоэффективна прежде всего из-за того, что при значительном числе операций удаляемые файлы в нее не перемещаются. Так происходит при удалении файлов по сети или из командной строки. Однако, наряду со стандартной, существует много вариантов Корзин, ориентированных на локальную систему (например, Norton Protected Recycle Bin) и позволяющих восстановить практически любой удаленный файл.

Конечно, в условиях компьютерной сети более функциональны специализированные серверные решения, такие как Executive Undelete от Executive Software International, Inc.

Эта программа может быть централизованно установлена администратором на рабочие станции и позволяет выполнять операции восстановления как непосредственно пользователем, так и администратором при подключении к Корзине по сети.

Восстановление из теневых копий

В Windows 2003 и Windows Vista имеется возможность восстановления предыдущей версии документа. Эта технология называется *теневое копирование* (shadow copy) и суть ее состоит в создании по определяемому администратором графику копий информации. Создание такой копии можно произвести в том числе и для открытых файлов (тех, с которыми в момент создания копии ведется работа). Одновременно может храниться несколько копий документов, созданных в разные моменты времени (рис. 11.4), предел определяется только размером дискового пространства, отведенного для данной операции. Резервирования нескольких сотен мегабайт диска может хватить на хранение промежуточных копий за несколько месяцев интенсивной работы.

Технология теневого копирования позволяет, во-первых, осуществлять резервное копирование *всех* данных (ранее штатная программа ntbackup при создании копий пропускала файлы, к которым она не могла получить доступ; иными словами, те файлы, которые редактировались пользователем). Во-вторых, у пользователей появилась прекрасная возможность без всяких дополнительных затрат иметь *несколько версий* документа. Например, после внесения очередных правок вы поняли, что более правильным решением был предыдущий вариант договора. Если он не был сохранен в качестве отдельного документа, то вернуться к прежним формулировкам ранее было затруднительно. При использовании технологии теневого копирования достаточно посмотреть перечень предыдущих версий документа и восстановить необходимую.

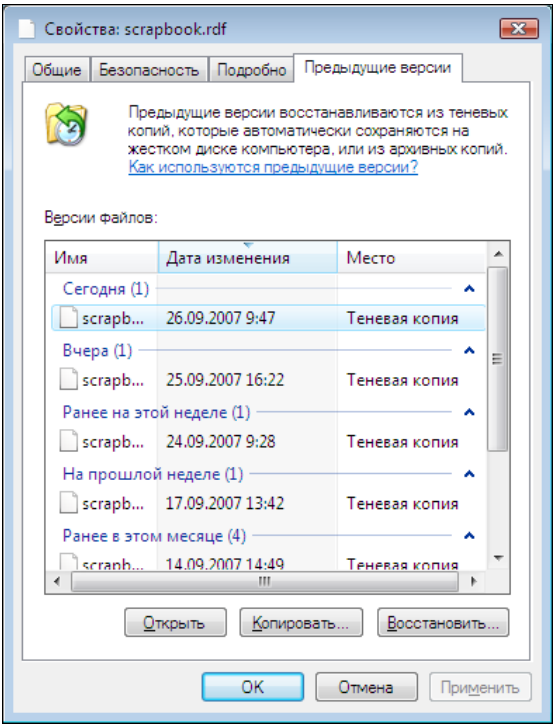


Рис. 11.4. Просмотр предыдущих версий файла на Windows Vista

Для работы с предыдущими версиями файлов пользователям Windows XP необходимо установить специального клиента. Его установочные файлы находятся в папке установки сервера по пути Windows\system32\clients\twclient\ и далее — в зависимости от типа платформы клиента. После установки этой программы при открытии свойств файла в сетевой папке появляется дополнительная вкладка **Предыдущие версии**. На этой вкладке можно выполнить необходимые операции восстановления информации. В Windows Vista возможность создания предыдущих версий включена в состав операционной системы рабочей станции. Причем данная возможность доступна и для файлов локального диска[1].

В Windows Vista теневые копии создаются в момент формирования точек восстановления (обычно раз в день). При необходимости операцию можно выполнить вручную (через задачу *Центр архивации и восстановления*). В Windows 2003 необходимо настроить расписание создания теневых копий, используя задачу **Управление компьютером** | **Общие папки**, где в динами-

[1]В Windows 2003 функции восстановления предыдущих версий были доступны пользователям только для сетевых папок сервера.

ческом меню следует выбрать задачу создания теневых копий и далее настроить ее параметры (рис. 11.5).

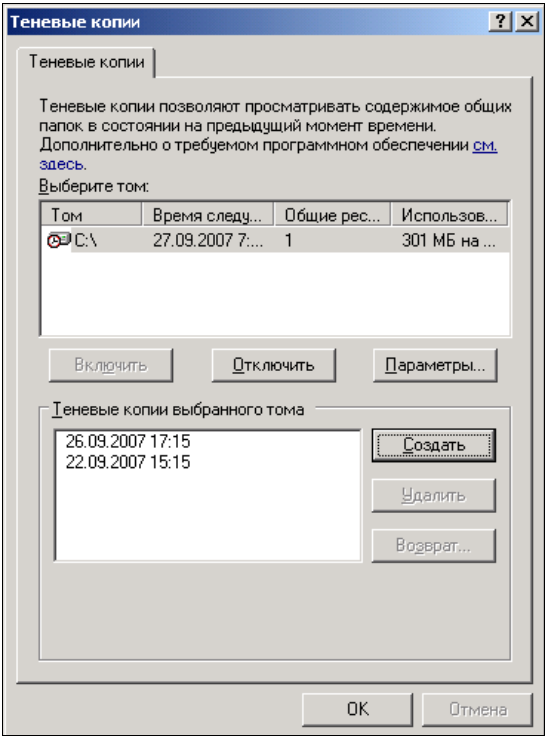


Рис. 11.5. Настройка расписания создания теневых копий в Windows 2003

Утилиты для восстановления данных с диска

Принцип действия таких утилит основан на том, что операционная система при удалении файлов не стирает информацию, а просто отмечает соответствующие места жесткого диска как *свободные*. Программы восстановления либо анализируют таблицы размещения файлов в поиске таких меток, либо просматривают содержимое всего диска и в зависимости от структуры данных делают попытку восстановить файл в том или ином известном формате.

Возможность успешного восстановления зависит от многих факторов, но обычно даже через несколько дней можно восстановить большую часть удаленных данных.

Примечание

Поскольку информация считывается непосредственно с жесткого диска, то такие программы позволяют восстановить данные также в случае повреждения диска и после его форматирования.

Одними из лучших программ для восстановления данных являются Easy Recovery и GetDataBack. Использование их не представляет особой сложности, поскольку все операции снабжены соответствующими *мастерами*.

Аудит

Неисправность системы практически невозможно определить без обращения к файлам протоколов. Протоколы работы могут создаваться практически всеми основными службами Windows, программами установки, а также прикладным программным обеспечением.

Поскольку на ведение журналов затрачиваются вычислительные мощности системы, то по умолчанию (в случае нормальной работы) большинство событий не фиксируется. Включение протоколирования осуществляется в случае необходимости, в том объеме, который позволяет найти неисправность, и только на период настройки системы.

Администратор обычно не ограничивается штатными средствами. Для аудита используются любые доступные утилиты сторонних разработчиков, контролирующие систему в реальном режиме времени. На рис. 11.6 приведен пример подобной программы, которая отображает результаты доступа к службе каталогов домена Windows. При этом вы можете видеть, какая программа и какой запрос адресовала к AD, оценить ответ службы, скорость его формирования и т. п.

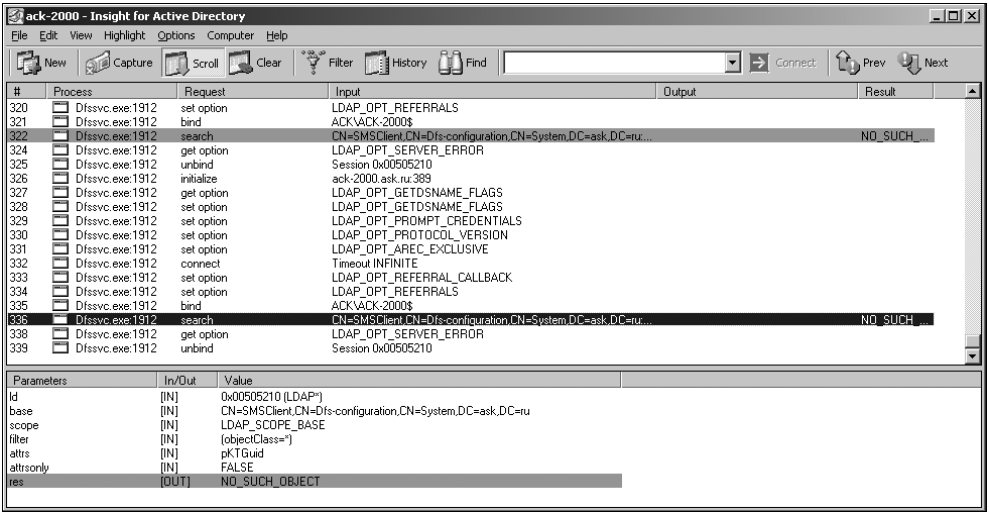


Рис. 11.6. Insight for Active Directory протоколирует все попытки доступа к службе каталогов на контроллере домена

Протоколирование работы системы

Информация о событии может быть записана как в специальный файл[1], так и в протоколы системы — *журналы* (event log). По умолчанию на рабочей станции имеются три журнала: приложений, безопасности и системы; их количество может быть увеличено (на контроллерах домена за счет добавления журнала DNS, репликации и т. п.). Перечень событий, заносимых в журналы приложений и системы, определяется разработчиками системных и прикладных программ. Иногда они предоставляют пользователю возможность в настройках программы выбирать объем протоколирования, но обычно влиять на количество информации, заносимой в данные протоколы, нельзя. Объем протоколируемых событий безопасности, напротив, практически целиком определяется администратором[2].

Просмотр журналов системы

Протоколирование работы системы ведется непрерывно, поэтому считать записи журналов обычными программами вам не удастся — нужный файл всегда "занят" системой. Для просмотра применяется специальная программа Просмотр событий (рис. 11.7), вызов которой выполняется через **Панель управления | Административные задачи | Просмотр событий**; эту задачу можно вызвать и из консоли управления компьютером.

После запуска программы и выбора нужного журнала в окне будут показаны зафиксированные в нем события. Описание предоставляет краткие характеристики события. Список возможных сообщений приведен в документации Resource Kit, но анализ ситуации в общем случае невозможен без обращения к онлайновой справочной базе Microsoft.

Поскольку в журнале событий могут содержаться десятки тысяч записей, то программа просмотра позволяет отфильтровывать записи по любому критерию и производить поиск нужного события.

Примечание

Обратите внимание, что с помощью программы просмотра можно знакомиться с событиями не только на локальном, но и на удаленном компьютере сети. Для этого достаточно выбрать операцию подключения к удаленному компьютеру и указать его имя.

---

[1] Имя файла и его расположение следует уточнить по технической документации. Например, можно включить протоколирование модемных соединений, которое позволит выявить причины нестабильности соединения. Файлы протоколов ведут почтовые серверы, серверы удаленного доступа, информационные серверы Интернета, брандмауэры и т. д. В каждом конкретном случае необходимо обратиться к соответствующему техническому описанию.

[2] На персональном компьютере данный протокол по умолчанию не ведется.

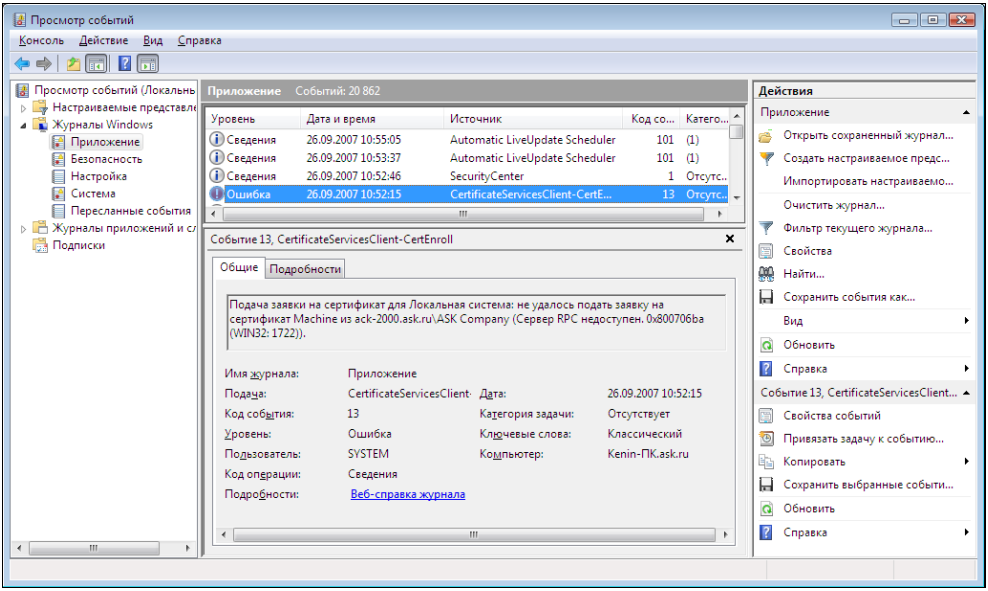


Рис. 11.7. Средство просмотра журнала событий в Windows Vista

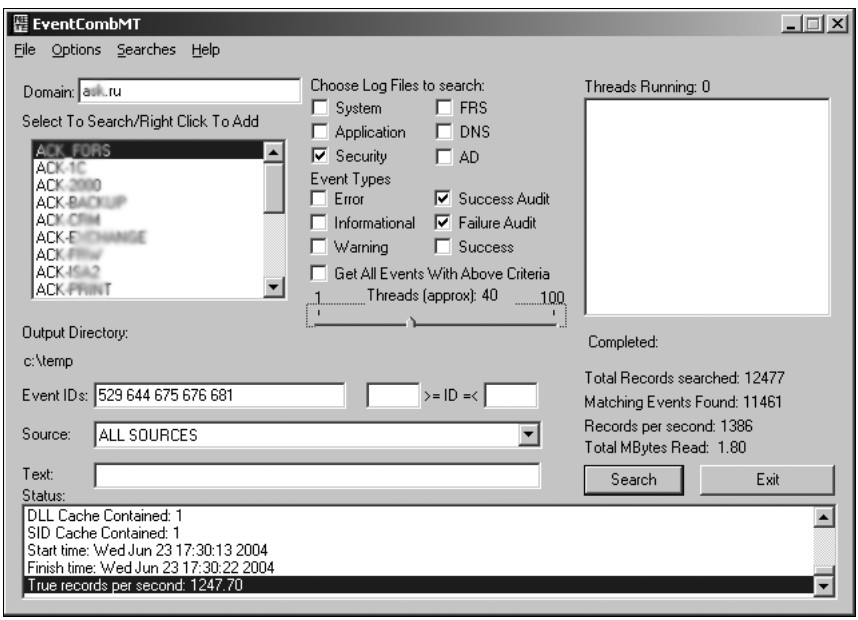


Рис. 11.8. Окно утилиты EventCombMT

Обычно администратору приходится периодически просматривать журналы событий с нескольких компьютеров. В Windows 2003 Server включен скрипт EVENTQUERY.vbs, который позволяет вывести события как с локального, так и с удаленных компьютеров, используя необходимые фильтры (по дате, по номеру события, типу и т. п.). При желании использовать графический интерфейс при поиске событий в журналах можно обратиться к специальной утилите — EventCombMT, бесплатно загружаемой с сервера Microsoft (рис. 11.8).

Утилита EventCombMT позволяет просматривать данные протоколов работы сразу нескольких систем. Администратор может задать желаемые условия поиска (номер события, имена компьютеров для анализа, диапазон дат и т. п.). Утилита содержит несколько встроенных описаний условий поиска, например, по ошибкам DNS, FRS, жестких дисков, службы каталогов. Результаты работы программа сохраняет в виде текстовых файлов.

Настройка параметров журналов

Одной из важных характеристик журнала является его объем и поведение системы при достижении установленного порога. Объем журнала выбирается исходя из интенсивности использования компьютера и принятой политики безопасности (например, сколько времени нужно хранить данные для последующего "вычисления" злоумышленника).

Обычно выбирается вариант, когда при достижении заданного лимита самые старые события автоматически стираются, освобождая место новым. При этом следует учитывать, что злоумышленник может специально сгенерировать за короткое время такое количество записей в журнале, что описание его несанкционированных действий просто будет стерто новыми событиями.

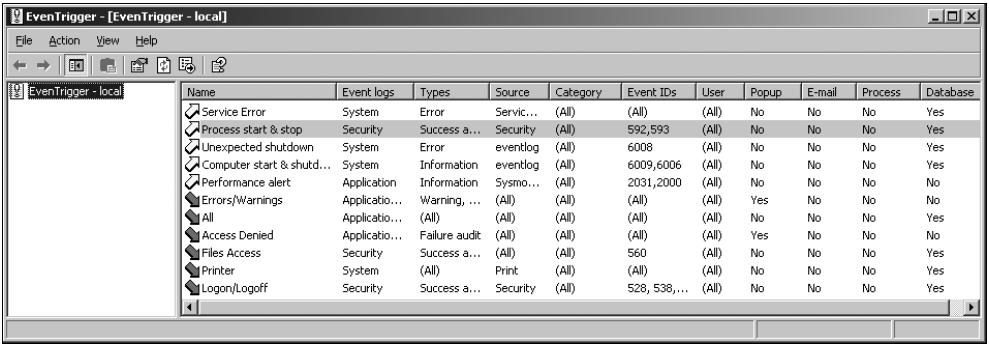
Если же выбран вариант хранения определенного количества записей, то злоумышленник может сначала переполнить журнал и только потом произвести необходимые ему действия. Они уже не будут записаны в протокол.

При повышенных требованиях к безопасности системы следует наладить сохранение журналов событий в специальной базе. Для этого проще всего использовать запускаемые по определенному графику специализированные утилиты для чтения журналов. Существуют различные коммерческие и бесплатные программы, которые могут независимо сохранять данные, заносимые в журналы системы, и осуществлять те или иные действия в случае возникновения определенных событий. Например, записывать в базу данных параметры заданий на печать (кто, какой документ, сколько страниц и т. п. распечатал на данном принтере).

На рис. 11.9 представлен пример такой программы — EvenTrigger от компании IS Decisions (**www.eventrigger.com**). Программа позволяет запускать

сценарии в соответствии с возникающими событиями, отправлять сообщения на пейджер или по электронной почте, заносить данные в ODBC-базы. С программой поставляется несколько предварительно сформированных триггеров (на события остановки служб, неудачного входа в систему, события печати и т. п.).

Подобные функции реализованы и во многих других программах, доступных системным администраторам (GFI LANGuard Security EventLog Monitor, Microsoft Operation Management Server и т. д.).



Name	Event logs	Types	Source	Category	Event IDs	User	Popup	E-mail	Process	Database
Service Error	System	Error	Servic…	(All)	(All)	(All)	No	No	No	Yes
Process start & stop	Security	Success a…	Security	(All)	592,593	(All)	No	No	No	Yes
Unexpected shutdown	System	Error	eventlog	(All)	6008	(All)	No	No	No	Yes
Computer start & shutd…	System	Information	eventlog	(All)	6009,6006	(All)	No	No	No	Yes
Performance alert	Application	Information	Sysmo…	(All)	2031,2000	(All)	No	No	No	No
Errors/Warnings	Applicatio…	Warning, …	(All)	(All)	(All)	(All)	Yes	No	No	No
All	Applicatio…	(All)	(All)	(All)	(All)	(All)	No	No	No	Yes
Access Denied	Applicatio…	Failure audit	(All)	(All)	(All)	(All)	Yes	No	No	No
Files Access	Security	Success a…	(All)	(All)	560	(All)	No	No	No	Yes
Printer	System	(All)	Print	(All)	(All)	(All)	No	No	No	Yes
Logon/Logoff	Security	Success a…	Security	(All)	528, 538,…	(All)	No	No	No	Yes

Рис. 11.9. Окно программы EvenTrigger

Для событий, связанных с безопасностью особо защищаемых систем (контроллеров), можно выбрать вариант прекращения функционирования сервера по достижении заданного объема журнала. Если злоумышленник попытается скрыть свои действия и переполнит журнал записями, то система заблокируется до вмешательства администратора непосредственно с консоли.

Ручная очистка журнала может быть проведена при наличии административных прав для учетной записи. Для этого следует отметить необходимый журнал и в меню его свойств выбрать операцию **Стереть все события**. Система предложит сначала сохранить журнал в виде файла (это можно сделать для архива или последующей обработки другими программами), а потом удалит все записи и внесет событие об очистке журнала.

Протоколирование пользовательских событий

Разработчики программного обеспечения могут легко реализовать функции записи любых событий в системные журналы, но добавить возможность записи дополнительных событий в уже существующие программы невозможно. Администратор может записывать новые события, только запуская те или иные специализированные утилиты. Начиная с Windows 2003, такая команда входит в состав самой операционной системы. Это команда EVENT-

CREATE. С ее помощью можно записать в любой журнал событие заданного типа (информация, ошибка и т. п.). Использование утилиты подробно описано в ее справке (`EVENTCREATE /?`), к которой мы отошлем читателя.

Автоматизация реагирования на события журнала

Для систем более ранних, чем Windows 2003 Server администратору, чтобы настроить автоматическое исполнение определенных команд в ответ на заданные события, фиксируемые в журнале, нужно было периодически считывать информацию из журналов и самостоятельно ее анализировать. Операция достаточно легко могла быть реализована с помощью сценариев, однако требовала некоторого опыта программирования. В Windows Server 2003 появилась команда, которая позволяет легко настраивать автоматический запуск любых программ при возникновении заданного события. Это команда `EVENTTRIGGERS`.

Справочная система к этой команде подробно описывает, как создать триггер, настроенный на появление определенного события, поэтому мы не будем останавливаться на этом описании.

В Windows Vista добавление автоматически выполняемого действия настраивается из динамического меню события (команда **Привязать задачу к событию**) с использованием Мастера создания простой задачи.

Настройка аудита событий безопасности

Объем событий, которые фиксируются в журнале безопасности, целиком определяется настройками системы, и их журналирование по умолчанию на рабочих станциях не ведется. Наиболее полный объем аудита событий безопасности можно установить при наличии на диске файловой системы NTFS.

Чтобы начать протоколирование событий безопасности, необходимо сначала *разрешить аудит* событий безопасности в политике безопасности[1]. Если администратор хочет отслеживать доступ к файлам и принтерам, то следует *задать объекты*, для которых должен осуществляться аудит событий.

Примечание

Политика безопасности включает возможность аудита как успешных, так и неудачных событий для различных объектов. Не следует без необходимости вести аудит всех событий, поскольку это может привести к нерациональной загрузке компьютера и потери производительности.

[1] Это может быть сделано как локально — в локальной политике безопасности, так и централизованно — путем задания соответствующих параметров в групповой политике.

Если необходимо вести протокол работы с файлами, то следует включить аудит доступа к объектам, после чего в свойствах объекта на вкладке **Безопасность** следует нажать кнопку **Дополнительно** и выбрать вкладку **Аудит**. Затем нужно добавить сведения о том, какие действия и от каких пользователей следует фиксировать в журнале.

Настройка дополнительного протоколирования

Помимо записей в системные журналы многие программы позволяют вести собственные протоколы. Например, практически все программы установки имеют дополнительные опции запуска, включающие расширенные режимы протоколирования. Такие задачи, как сервер маршрутизации и удаленного доступа, сервер DNS, подключения по требованию и т. п., позволяют в своих настройках указать необходимость протоколирования основных событий.

Часть программ протоколирует свои события и сохраняет данные в папке *%Windir%*\debug\. Это такие задачи, как служба репликации файлов, сетевой вход, операции подключения к домену и т. п. Просмотрите этот каталог, чтобы ознакомиться с имеющейся на вашем компьютере информацией.

Кроме того, для некоторых задач (служб) протоколирование с целью отладки может быть включено через реестр системы. Приведу небольшую сводку настройки протоколирования различных задач Windows (табл. 11.2).

Примечание

Файлы протоколов достаточно сложно анализировать вручную. Существуют различные программы, позволяющие автоматизировать данную операцию, например, отфильтровать и отсортировать записи по каким-либо критериям и т. п. Такие программы легко найти как в свободных ресурсах Интернета, так и у самих разработчиков ПО (например, утилита LogParser от Microsoft).

Анализ производительности

Зачастую на администратора компьютерной сети небольшого предприятия ложится выбор приобретаемых моделей компьютеров. В большинстве случаев покупается типовая на данный момент конфигурация у того поставщика, с которым организацию (администратора) связывают длительные отношения. Как правило, многие организации не могут позволить себе приобретение компьютерных брендов, поэтому большинство эксплуатируемых у них моделей собрано специалистами региональных предприятий из отдельных блоков. На сбалансированность таких конструкций часто обращается немного

Таблица 11.2. *Настройка дополнительного протоколирования*

Событие	Метод включения	Примечание
Модем (протоколирование процесса установки соединения)	Включается через свойства модема (Панель управления) на вкладке **Дополнительно**	Журнал просматривается из этой же программы
PPP соединения	Включается в оснастке управления RRAS	Включение трассировки возможно также командой `netsh` (ras set tracing PPP enable)
Schannel	Включается добавлением параметра `SCHANNELEventLogging` типа `REG_DWORD` в ветку реестра `HKLM\System\CurrentControlSet\Control\SecurityProviders`	Допустимые значения параметра и их действие: • 0 — нет протокола; • 1 — запись только ошибок; • 2 — запись только предупреждений; • 4 — запись информации и удачных сообщений
Security Configuration Client Processing (SceCli, применение групповой политики)	Включается добавлением параметра `ExtensionDebugLevel` типа `DWORD` в ветку реестра `HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{827D319E-6EAC-11D2-A4EA-00C04F79F83A}` со значением, равным 2	Файл протокола создается в папке %systemroot%\ security\logs
Windows Installer[1] (протоколирование установки программ, использующих msi-файлы)	Включается через групповую политику: **Конфигурация компьютера | Административные шаблоны | Windows Components | Windows Installer**. Протокол создается в папке %TEMP%	Рекомендуется использовать именно групповую политику, хотя протоколирование может быть включено и путем создания ключа `Logging` типа `Reg_SZ` в ветке реестра `HKLM\Software\Policies\Microsoft\Windows\Installer` с параметрами, указанными в описании групповой политики

[1] Для протоколирования отдельных установок можно использовать ключи запуска программы-установщика, включающие все возможные опции протоколирования. Ключи можно уточнить по онлайновой базе знаний. Отметим только, что полное протоколирование ведется при наличии ключа `/l*vx`. Для стандартного протоколирования можно использовать ключ `/LIME`. При этом командная строка для запуска программы установки должна выглядеть следующим образом: `msiexec /i A:\Example.msi /LIME c:\logfile.txt` (в примере не приведены другие ключи, кроме назначения опций протоколирования и указания на файл дистрибутива).

***Таблица 11.2** (продолжение)*

Событие	Метод включения	Примечание
Протоколирование изменений реестра программой установки	Включается установкой параметра `LogLevel` в ветке реестра `HKLM\Software\Microsoft\Windows \CurrentVersion\Setup\` в значение `0000FFFF`	После устранения неполадок следует вернуть значение параметра в 0, поскольку размер файла setupapi.log существенно возрастает
Kerberos Event Logging	Включается добавлением в раздел `HKLM\SYSTEM \CurrentControlSet\Control\Lsa\Kerberos\Parameters` параметра `LogLevel` типа `REG_DWORD` в значение `0x1`	Не забудьте удалить этот параметр после завершения наблюдения, поскольку данное протоколирование создает существенную нагрузку на систему
User Environment Debug Logging	Включается добавлением в `HKLM\Software\Microsoft\WindowsNT\CurrentVersion \Winlogon` параметра `UserEnvDebugLevel` типа `REG_DWORD`	Значения можно комбинировать по правилу `OR` (ИЛИ), например, объединив `NORMAL` и `LOGFILE`, получим `0x00010001`. Лог-файл Userenv.log создается в папке %SystemRoot%\Debug\UserMode\. Допустимые значения параметра: • `NONE` — `0x00000000`; • `NORMAL` — `0x00000001`; • `VERBOSE` — `0x00000002`; • `LOGFILE` — `0x00010000`; • `DEBUGGER` — `0x00020000`
Изменение объема сообщений при включении/выключении системы и входе в сеть	Рекомендуется изменять уровень детализации сообщений через групповую политику **Конфигурация компьютера | Административные шаблоны | System |** параметр **Verbose vs normal status messages**	Возможно включение установкой параметра `verbosestatus` типа `DWORD` в ветке реестра `HKLM\SOFTWARE\Microsoft \Windows\CurrentVersion\Policies \System` в значение `1`. Параметр `DisableStatusMessages` в ветке реестра `HKLM\SOFTWARE \Microsoft\Windows\CurrentVersion \Policies\System\`, равный 1, отключает сообщения

***Таблица 11.2** (продолжение)*

Событие	Метод включения	Примечание
Протоколирование печати	Включается в окне настроек принтера: **File | Server Properties |** вкладка **Advanced**. Далее следует выбрать необходимые опции	Протоколирование событий производится в system log. Протокол принтера в большинстве случаев некорректно отображает число напечатанных принтером страниц. Если необходимо получить статистику использования принтера различными пользователями, то следует запускать программы третьих фирм, перехватывающие и анализирующие очередь печати
Протоколирование DHCP	Включается в оснастке управления DHCP в меню **Action** на вкладке свойств **General**	Файл протокола по умолчанию создается в папке %windir%\System32\Dhcp
Протоколирование DNS	Включается в оснастке управления DNS	При детальном протоколировании сохраняется вся информация, получаемая и отправляемая сервером
Протоколирование брандмауэра доступа в Интернет (Internet Connection Firewall, ICF)	Включается в настройках соответствующего подключения на вкладке **Дополнительно | Settings | Security Logging Options**	Можно протоколировать как успешные соединения, так и отказы в передаче данных
Oakley log (протоколирование IKE)	Включается добавлением в раздел `HKLM\SYSTEM\CurrentControlSet\Services\PolicyAgent\Oakley` параметра `EnableLogging` типа `REG_DWORD` со значением `1`	Протокол (файл Oakley.log) пишется в папку %SystemRoot%\debug
IPSec	Настраивается командой `set config property=ipsecdiagnostics value` *x*, где *x* может принимать значения от 0 до 7. Возможно также настройка через параметр `EnableDiagnostics` типа `REG_DWORD` ветки реестра системы `HKLM\System\CurrentControlSet\Services\IPSec\`	Значение 7 соответствует максимальному уровню диагностики, 0 — отключенному протоколированию. Более подробные сведения можно найти в справочной документации

***Таблица 11.2** (окончание)*

Событие	Метод включения	Примечание
Протоколирование службы каталогов	Включается изменением значений параметров в ветке `HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics`	В этой ветви представлено несколько десятков параметров (Security, MAPI Interface, Replication Events, Knowledge Consistency Checker, Backup и др.). Вам необходимо изменить значение того из них, диагностику которого планируется проводить. По умолчанию значения всех параметров равно 0; при этом протоколируются ошибки и типовые события. Максимальный уровень протоколирования — 5
Протоколирование WMI	• Включается при помощи следующих параметров реестра в ветке `HKLM\SOFTWARE\Microsoft\WBEM\CIMOM:Logging`; • `Logging Directory` — имя папки с файлом протокола; • `Log File Max Size` — размер файла протокола	Параметр `Logging` может принимать следующие значения: 0 — протоколирование отключено; 1 — включено; 2 — подробное протоколирование. При превышении указанного значения размера файла протокола создается новый файл, а старому присваивается расширение lo_. Настройка также возможна через **Мой компьютер | Управление | Службы и приложения | Управляющий элемент WMI | Свойства |** вкладка **Ведение журнала**
Протоколирование DCOM	В разделе реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole` создайте параметры типа `REG_DWORD` со значениями `1` `ActivationFailureLoggingLevel` и `CallFailureLoggingLevel`	События будут заноситься в журналы приложений и системных событий. Для начала протоколирования достаточно перезапустить приложение. Для отключения ведения протокола установите значения указанных параметров в 0
Протоколирование Automatic Update (Windows Server 2003)	В ветку реестра `HKLM\Software\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update` добавить параметр `DebugType` типа `REG_DWORD` со значением `1`	Файл протокола Wupdlog.txt создается по следующему пути: \Program Files\Windowsupdate\Wupd\System\
Расширенное протоколирование политики ограничений ПО	В ветку реестра `HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers` добавить строковый параметр `LogFileName`	Этот параметр должен содержать путь к файлу протокола. Не забудьте удалить параметр после выполнения анализа ситуации

внимания, поскольку производительность современных моделей обычно существенно превосходит требования, предъявляемые на индивидуальных рабочих местах, и если производительность компьютера перестает удовлетворять потребности пользователя, то взамен его приобретают более совершенную модель.

Однако во многих случаях причиной неудовлетворительной работы является какое-либо узкое место в конфигурации системы ("бутылочное горлышко", Bottleneck). И "расшивка" его может оказаться экономически существенно более оправданной, чем замена всей компьютерной системы. Кроме того, при покупке компьютера для использования в специализированных целях правильная конфигурация сможет сэкономить существенные средства.

Примечание

На компьютерах с Windows 9*x* о причинах недостаточной производительности можно судить только по косвенным признакам, например, по проценту загрузки процессора, в то время как о недостатке оперативной памяти можно сделать вывод по повышенной активности жесткого диска при нормальных условиях работы (постоянно "горит" лампочка, показывающая обращения к жесткому диску).

Удовлетворенность производительностью системы — субъективная оценка. Она зависит от объема выполняемых пользователем бизнес-задач, частоты тех или иных операций и т. п. Обычно IT-специалисту необходимо проанализировать влияние многих параметров. Например, медленная работа Web-приложения, используемого сотрудниками предприятия, может быть вызвана недостаточным качеством канала передачи данных, низкой производительностью брандмауэра, нехваткой ресурсов сервера интернет-приложений, проблемами сервера с базами данных и т. д.

В операционных системах на базе ядра Windows NT для анализа состояния системы существуют специальные встроенные средства. Прежде всего, это программа **Производительность** (Performance Monitor).

Примечание

Существует программа от Microsoft — Server Performance Advisor, которая формирует отчет по параметрам производительности системы. Эта программа позволяет оперативно собрать необходимые для первичного анализа показатели и оформить их в виде бумажного отчета. Продукт доступен для бесплатной загрузки.

В Windows Vista возможности программ мониторинга состояния существенно расширены. Так, программа **Монитор ресурсов** (рис. 11.10) позволяет администратору легко выявить программы, влияющие на загруженность того или иного ресурса компьютера.

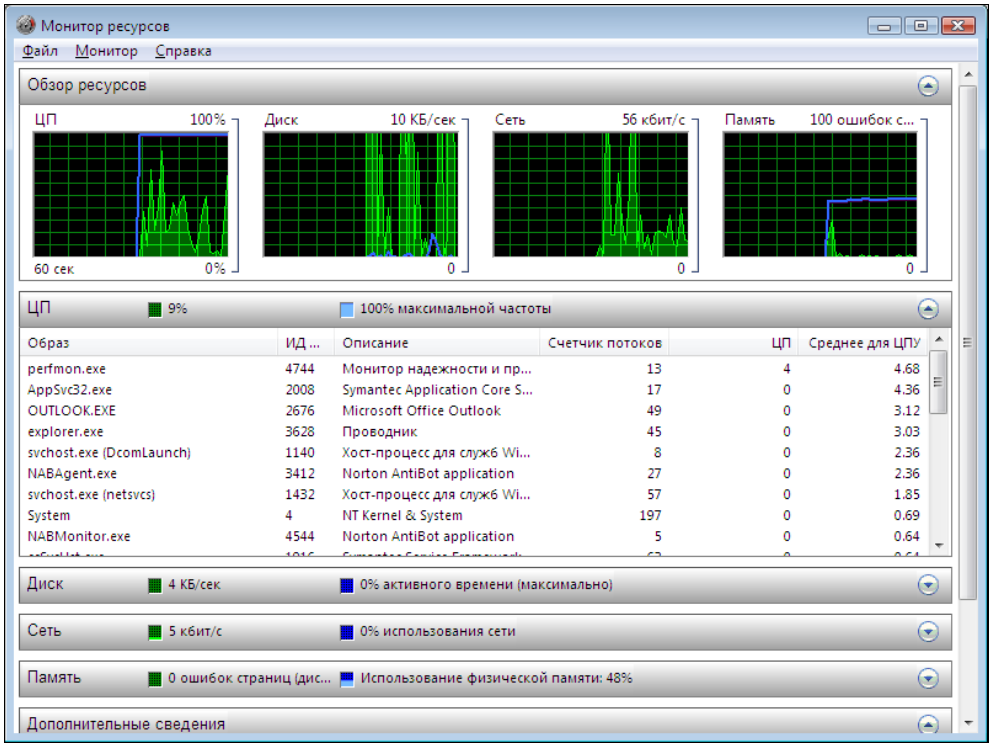


Рис. 11.10. Монитор ресурсов в Windows Vista позволяет администратору оценить вклад, вносимый различными процессами в загрузку системы

Задача *Производительность*

Программа (задача) **Производительность** (Performance Monitor) предназначена для отображения данных производительности системы, контроля соответствующих параметров с возможностью реагирования на превышение устанавливаемых пороговых значений (например, запуском исполняемого файла) и для составления отчетов о работе системы (в том числе и в формате HTML).

Оснастка задачи включает две программы: *монитор системы* и *журналы счетчиков и оповещений*.

Счетчики состояния системы

В операционной системе на базе Windows NT существует большое количество так называемых *счетчиков*. Счетчики *постоянно* содержат численные параметры, которые характеризуют определенные процессы как самой операционной системы, так и прикладных программ. Если разработчики устанав-

ливаемого ПО предусмотрели свои счетчики, то они добавляются в перечень отображаемых этой программой.

Примечание

Счетчики содержат данные постоянно, независимо от того, запущена программа системного монитора или нет. Если вы хотите, чтобы работа самой программы при отображении данных вносила минимальные искажения в параметры производительности, то запускайте ее с низким приоритетом (`start /low`). При возможности снятие показаний счетчиков целесообразно выполнять с другого компьютера[1].

Программа монитора позволяет отображать состояние большого количества счетчиков. Поскольку их точная интерпретация требует специальных знаний операционной системы, то на практике обычно используют несколько интегральных показателей, а к более тщательному анализу прибегают в достаточно редких случаях.

Кроме наблюдения за показателями в различных графических представлениях (линейном графике, гистограмме и т. п.), программа позволяет вести протокол счетчиков, например, автоматически снимая показания каждые 10 минут; а также задавать границы, по достижению которых система выдаст предупредительное сообщение и может запустить заданную вами программу. Эти настройки могут помочь при проведении долговременных исследований производительности системы и текущего контроля ее состояния. Например, при обследовании компьютера целесообразно получить статистику его загруженности за достаточно длительный период — порядка суток.

Основные узкие места системы

Для объективной оценки производительности системы следует в период замеров выполнять обычные для данного компьютера операции. Например, для рабочей станции это открытие файлов, их печать, чтение электронной почты, работа в программах офиса или выполнение текущих операций в базе данных и т. п. Чем больше такие операции будут соответствовать типовым вариантам использования компьютера, тем точнее получатся рекомендации на основе анализа показаний счетчиков.

Узким местом производительности компьютера обычно становится один из следующих компонентов:

- процессор;
- оперативная память;

[1] В параметрах программы нужно указать сетевое имя того компьютера, показания счетчиков которого предполагается контролировать.

- дисковая подсистема;
- сетевой адаптер.

Примечание

Существенное влияние на производительность оказывает качество драйверов. При возможности следует установить в систему последние имеющиеся версии.

Оценка производительности процессора

В качестве заголовка к описанию счетчика приведено название объекта и параметра, предназначенного для оценки производительности процессора, в программе **Производительность** (Performance Monitor).

- **Processor\% Processor Time.**

  При нормальных условиях эксплуатации процессор должен быть загружен лишь незначительно. Конечно, если какая-либо программа в текущий момент времени выполняет серьезные вычисления, то загрузка в 90% и выше — это нормальный показатель. В среднем же величина загрузки процессора не должна превышать 20—40%. Если данный показатель выше 50—70%, то необходимо заменить процессор на более производительную модель[1] или перенести на другие компьютеры часть выполняемых задач.

Примечание

Поскольку современные компьютеры имеют возможность снижать скорость своей работы (например, в случае перегрева процессора), предварительно убедитесь, что высокая загрузка процессора не связана со снижением его тактовой частоты. Для этой цели можно использовать показания программ, контролирующих состояние датчиков системы.

Средняя загрузка процессора отображается также в программе **Диспетчер задач**.

- **Processor\% Privileged Time.**

  Счетчик важен для оценки загрузки процессора системными задачами. Если величина загрузки привилегированного режима составляет 40% и выше, то это свидетельствует о необходимости серьезно проанализировать работу операционной системы, проверить состояние узлов компьютера и обновить драйверы устройств. Кроме того, такое значение может свидетельствовать о неоптимальной архитектуре выполняемых задач: например, сервер многократно передает клиенту небольшие порции данных вместо

[1] В общем случае, это замена CPU на модель с большей тактовой частотой. Для рабочих станций, кроме того, это может быть замена линейки Celeron на Pentium. Для серверных систем в качестве варианта можно рассматривать установку CPU той же тактовой частоты, но с большим объемом кэша L2.

того, чтобы централизованно выполнить вычисления и сообщить только итоговый результат[1].

- **System\Processor Queue Length (all instances).**

  Показатель отображает длину очереди заданий, которые необходимо выполнить процессору. Средняя величина очереди заданий, равная двум и выше, свидетельствует о том, что процессор *не успевает* выполнять все задачи[2].

  Происходит это потому, что в системе одновременно выполняются различные процессы, которые случайным образом формируют задания процессору на обслуживание требующихся им вычислений. Процессор не успевает переключаться между ними и оперативно "выполнять" возникающие требования. В результате эти задания становятся в очередь, процент использования процессора остается низким (основное время тратится на переключения между заданиями), в то время как система крайне медленно реагирует на команды.

  Большая длина очереди может быть обусловлена не только большим количеством одновременно выполняющихся заданий, но и неисправностью какого-либо устройства, например, сетевого адаптера, генерирующего большое количество прерываний в единицу времени. Для локализации этой причины следует провести анализ параметра **Processor\Interrupts/sec** *(см. далее)*.

  Если высокое значение параметра очереди заданий является следствием большого количества задач, которые одновременно должен выполнять компьютер, то выходом является либо снятие некоторых вычислений[3], либо перераспределение задач между несколькими компьютерами, либо замена модели на более производительную. Пользователь практически не имеет возможности оптимизировать процесс переключения между различными задачами. Можно только попробовать изменить приоритет приложений и фоновых задач (на вкладке **Дополнительно** задачи **Система** в Панели задач) и проверить результат.

- **Processor\Interrupts/sec.**

  Счетчик показывает количество запросов к процессору на обработку. Максимальное число прерываний, которое может обработать процессор,

---

[1] В этом случае большой удельный вес привилегированного режима объясняется значительным числом операций передачи по сети небольших пакетов данных.

[2] При этом очень часто средний процент загрузки процессора остается сравнительно небольшим.

[3] Часто многие процессы не являются необходимыми для данной системы. Например, можно отключить режим онлайнового контроля вирусов, если не поступают новые данные, или отказаться от индексирования файлов. Кроме того, можно отключить службы Windows, которые не используются на данной системе.

зависит от его типа. Для разных процессоров эта величина колеблется от 500 до 2000 прерываний в секунду.

Поскольку высокое значение данного счетчика может быть следствием неисправности оборудования, следует выяснить, что является источником повышенного количества запросов в единицу времени. Для этого можно задействовать счетчики объекта Thread, например **%Processor Time**. Эти счетчики отображают в том числе состояние каждого потока, который запускается отдельным процессом. Переключив отображение монитора системы на гистограмму, вы можете увидеть процесс, который монополизирует ресурсы компьютера.

Примечание

Бездействие компьютера также относится к процессу. Поэтому для удобства не следует включать отображение этого параметра на графике.

Оценка использования оперативной памяти

В случае недостаточной производительности не лишним будет убедиться, что в системе установлена наиболее быстродействующая марка модулей оперативной памяти (например, если материнская плата поддерживает несколько модификаций — PC2700 и PC3200).

- **Объем свободной памяти.**

  Если значение объема свободной оперативной памяти приближается к 4—5 Мбайт, то это свидетельствует о недостатке памяти. Вам следует подумать о добавлении в систему новых модулей оперативной памяти.

  При нормальных условиях работы должно быть свободно не менее 30% объема виртуальной памяти. Если эта величина меньше, то следует увеличить размер файла подкачки. В Windows 200*x*/XP/Vista система имеет возможность самостоятельно менять размер файла подкачки. Если пользователь выбрал ручные установки, то ему следует изменить действующие параметры в сторону увеличения. Рекомендуемое значение файла подкачки — от объема оперативной памяти плюс 12 Мбайт до 1,5—2 объема оперативной памяти в зависимости от выполняемых в компьютерной системе задач.

  Объем свободной физической памяти можно также посмотреть в программе **Диспетчер задач**.

- **Memory\Pages/sec.**

  Одним из самых интегральных показателей использования оперативной памяти является счетчик, демонстрирующий количество запросов страниц памяти из файла подкачки на диске. Критическое значение данного показателя составляет около 20 единиц. Когда системе не хватает физической

памяти для текущей работы, она начинает обмен страницами памяти с файлом подкачки. Постоянный интенсивный обмен — 20 и более страниц в секунду — свидетельствует о недостатке оперативной памяти. Выход — добавить физическую память.

Оценка дисковой подсистемы

Счетчики дисковой подсистемы в Windows NT 4.0 по умолчанию отключены в целях повышения производительности. Их включение выполняется командой `diskperf -y` с последующей перезагрузкой системы).

- **LogicalDisk (PhysicalDisk)\Avg. Disk Queue Length.**

  Счетчик показывает среднюю очередь заданий (операций записи или чтения) для соответствующего диска. Интерпретация данного параметра достаточно проста: если существует очередь на дисковые операции (значение счетчика достигает 1 и более), то это означает, что диски не справляются с записью/чтением информации.

  Какие могут быть варианты решения проблемы при обнаружении узкого места в дисковой подсистеме?

  Прежде всего следует убедиться, что в системе установлено достаточно оперативной памяти. В противном случае повышается нагрузка на виртуальную память, что приводит к увеличению количества служебных дисковых операций.

  Обратите внимание, чтобы на дисках было достаточно свободного места (не менее 20% их объема). Проведите дефрагментацию дисков, уменьшите или исключите использование сжатия и шифрования файлов на тех дисках, на которых выявлена проблема низкой производительности. Отключите дополнительные задачи, ведущие запись информации на диск (например, откажитесь от протоколирования событий безопасности и т. п.).

  При возможности следует разместить информацию на различных физических дисках[1], а лучше — на томах с чередованием записи данных, причем такую RAID-конфигурацию в крайнем случае можно создать и программным способом из нескольких дисков. Наиболее быстрой и отказоустойчивой является конфигурация RAID 0+1[2].

---

[1] Например, на одном физическом диске расположить файл подкачки, на другом — рабочие базы данных. В случае сервера баз данных на одном диске сохранять файлы баз данных, а на другом — файлы протоколов (log files). При этом не забывайте, что не следует подключать диски различной производительности к одному контроллеру.

[2] Наиболее часто используемая на практике конфигурация RAID — RAID5, практически не уступая RAID10 в операциях *чтения*, весьма существенно проигрывает по производительности в операциях *записи*.

Если эти операции не приведут к успеху, следует искать возможность приобрести более быструю дисковую подсистему.

Примечание

Опытные пользователи могут также попытаться поэкспериментировать с параметрами структуры диска, например, изменить размер кластера.

- **% Disk Time.**

Счетчик показывает процент времени, в течение которого система "занята" операциями ввода/вывода. Значения счетчика, достигающие 50%, свидетельствуют о необходимости использования более быстрой дисковой подсистемы.

Примечание

В случае снижения производительности системы при наличии активных дисковых операций, администратор имеет возможность отключить запись имен файлов в формате 8.3 и запись времени последнего доступа к файлу (в ветви `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Filesystem` установить в значение 1 параметры `NtfsDisable8dot3NameCreation` и `NtfsDisableLastAccess` соответственно).

Оценка работы сетевого адаптера

Для использования счетчика **Network Segment: % Net Utilization** должен быть установлен драйвер Network Packet Protocol из программы Network Monitor.

Счетчик отображает текущую загрузку сегмента компьютерной сети, к которому подключен компьютер. Для сети, выполненной по стандарту Ethernet, — а это практически все локальные компьютерные сети,— величина утилизации сети равная 60% считается критической; на практике следует внимательно проанализировать работу сети уже при достижении порога утилизации порядка 30—40%[1]. При необходимости столь интенсивной пересылки данных следует перейти на сеть с более высокой производительностью или выделить нагруженные участки в отдельный сегмент. Следует также постараться заменить сетевые концентраторы коммутаторами.

Примечание

Дорогие сетевые адаптеры позволяют "забрать" на себя часть вычислений, обычно выполняемых процессором компьютера. Например, подсчитывать кон-

[1] Администраторы обычно используют для оценки состояния сети различные SNMP- и RMON-мониторы, которые имеют возможность автоматически высылать предупреждения при достижении установленных пороговых значений.

трольные суммы пакетов, выполнять некоторые расчетные операции при шифрованном трафике, собирать сегментированные TCP/IP-пакеты и т. п. Соответствующие возможности следует уточнить по описанию данных устройств и внести дополнительные настройки в параметры сетевых устройств Windows.

В случае особой интенсивности сетевого трафика администраторы могут настроить некоторые параметры TCP/IP-протокола через реестр системы (например, размеры передаваемого окна или число пакетов, после приема которых нужно высылать подтверждение получения данных). Эти настройки следует уточнить по описанию операционной системы.

Примечание

Одним из способов повышения пропускной способности является также агрегирование каналов связи: установка в сервер второго (третьего и т. д.) сетевого адаптера и распределение передаваемой информации по всем каналам. Данное объединение реализуется программным обеспечением сетевых адаптеров наиболее известных вендоров (например, ProSet для адаптеров изготовления фирмы Intel).

Счетчики прикладных программ

После установки программного обеспечения (SQL, Axapta, Exchange и т. п.) число параметров, отображаемых в задаче **Производительность**, может увеличиваться. Анализ данных таких счетчиков следует проводить по технической документации соответствующего программного продукта.

В большинстве случаев показания счетчиков будут полезны только для высококвалифицированных специалистов служб технической поддержки, хотя администраторы могут использовать некоторые интегральные показатели при оценке состояния системы.

В любом случае конечным итогом анализа таких счетчиков будет вывод о достаточности или о необходимости добавления одного из следующих ресурсов: процессора (в том числе понимая под этим и замену платформы на более производительную модель), оперативной памяти, дисковой подсистемы, сетевого адаптера.

Дополнительные возможности Vista

Большей частью такие данные счетчиков и журналов предназначены для специалистов служб технической поддержки. Как уже было отмечено, в Windows Vista объем таких данных существенно увеличен (рис. 11.11) и сделана попытка автоматизации поиска проблемы: при ее возникновении собранные данные передаются в фирму-разработчик, и делается попытка автоматического поиска решения в базе знаний. К сожалению, на текущий момент практически все автоматизированные средства решения формируют

бесполезные советы или информируют об отсутствии решения, предлагают обратиться к разработчику стороннего ПО и т. п. Будем надеяться, что ситуация изменится по мере роста базы знаний и отработки технологий.

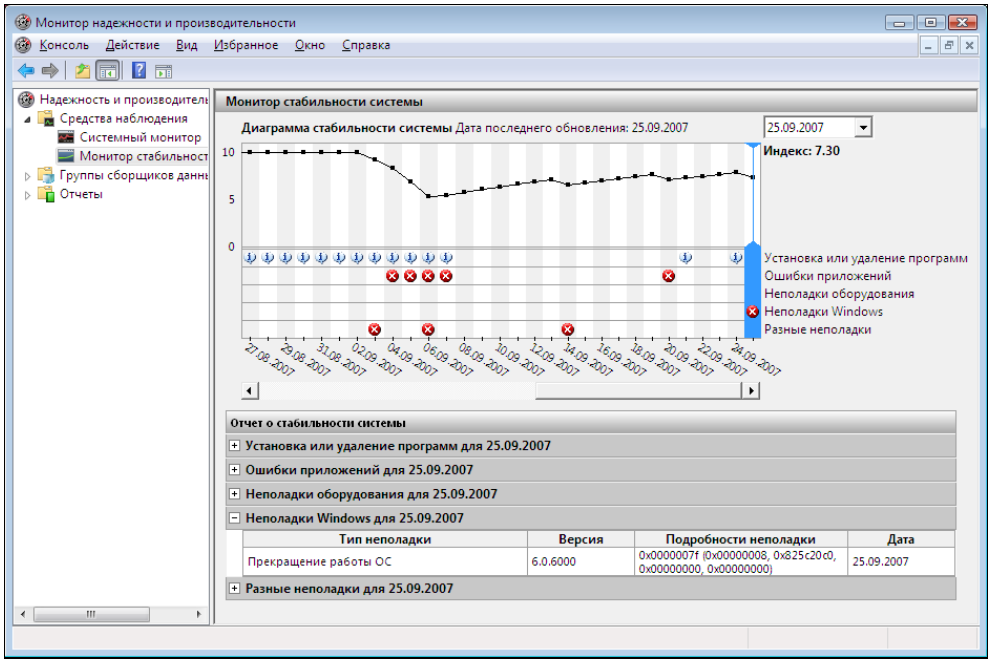


Рис. 11.11. Монитор надежности и стабильности операционной системы Windows Vista

Server Performance Advisor

Для серверов Windows 2003 Server разработчик предлагает специальную программу для комплексного анализа производительности — Server Performance Advisor[1] (рис. 11.12). Эта программа практически в автоматическом режиме собирает значения различных счетчиков операционной системы и программного обеспечения и формирует комплексный отчет.

На рис. 11.12 показана часть отчета, сформированного программой по результатам обследования производительности сервера. Как правило, необходимость в подобных отчетах возникает при подготовке материалов для руководителя соответствующего подразделения. К сожалению, возможностей оперативного формирования печатной версии документа в программе не предусмотрено.

[1] Программу можно бесплатно загрузить с сайта разработчика.

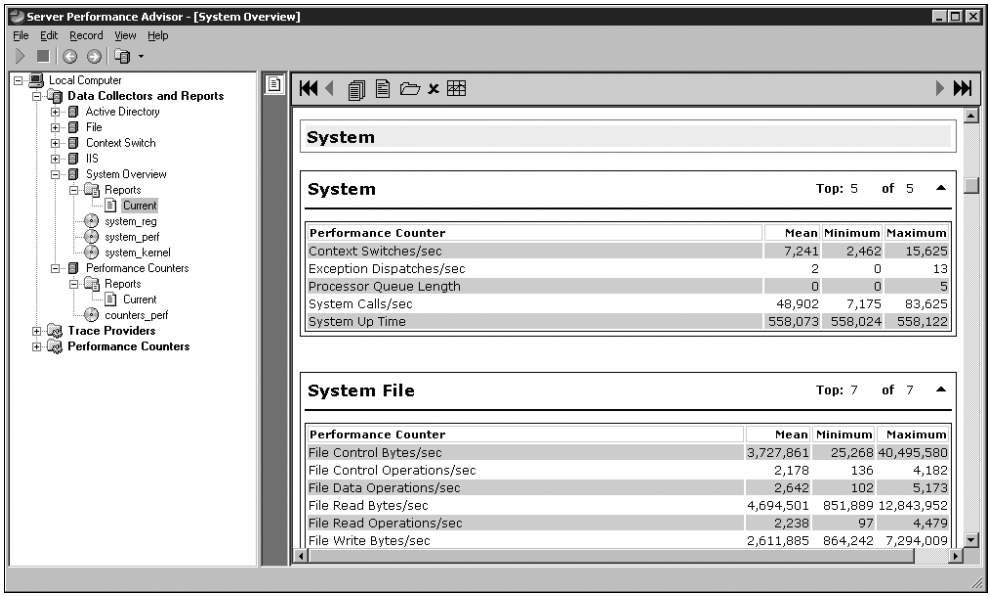


Рис. 11.12. Server Performance Advisor

На момент подготовки книги программа была несколько "сыра": практически во всех случаях использования ее автором возникали ошибки автоматической интерпретации тех или иных показаний или выдавались, например, предупреждения, что загрузка сетевого адаптера составляет 378 792% от максимального значения.

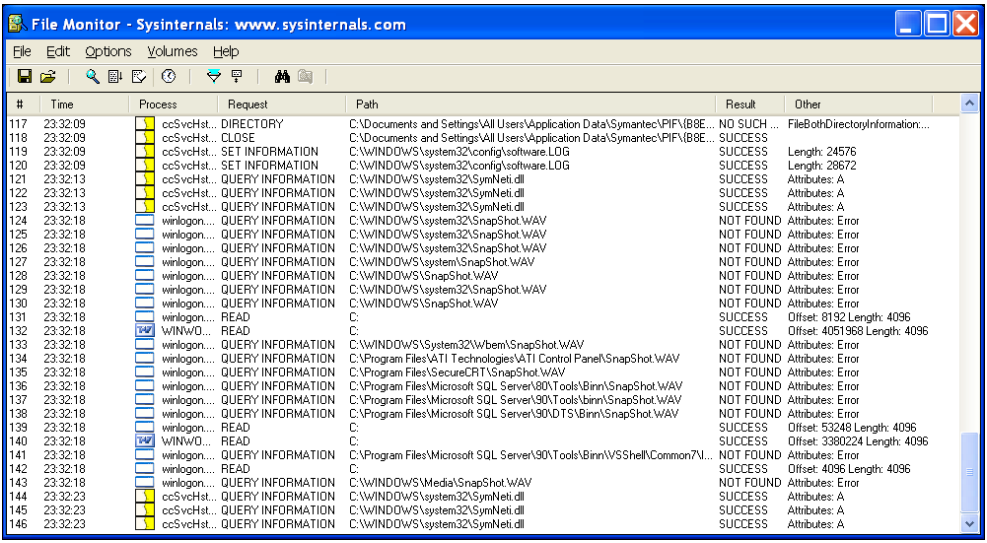
Программа полезна, прежде всего, тем, что позволяет собрать за одну операцию показания многих счетчиков и усреднить их за некоторый период времени, т. е. фактически помогает сделать первичный обзор состояния системы с тем, чтобы впоследствии более углубленно изучать причины конкретных узких мест. Опциями программы можно настроить детализацию сбора информации и включить в анализ различные подсистемы. Значения усредненных показателей, получаемых программой, следует использовать для дальнейшего углубленного анализа производительности.

Программа предназначена для серверов Windows 2003 Server и требует для установки выполнения некоторых условий (например, поддержку .NET), что не позволяет ее использовать без дополнительных настроек на всех системах.

Диагностика доступа к ресурсам компьютера

Для поиска проблем администратору часто необходимо отслеживать процессы доступа программ к файлам, к реестру системы и т. д. Наблюдение за та-

кими процессами может существенно помочь в выяснении причин сбоев. В этом случае можно воспользоваться бесплатными утилитами, доступными для загрузки с сайта **www.sysinternals.com**. Окно одной из таких утилит представлено на рис. 11.13.



#	Time	Process	Request	Path	Result	Other
117	23:32:09	ccSvcHst...	DIRECTORY	C:\Documents and Settings\All Users\Application Data\Symantec\PIF\{B8E...	NO SUCH ...	FileBothDirectoryInformation:...
118	23:32:09	ccSvcHst...	CLOSE	C:\Documents and Settings\All Users\Application Data\Symantec\PIF\{B8E...	SUCCESS	
119	23:32:09	ccSvcHst...	SET INFORMATION	C:\WINDOWS\system32\config\software.LOG	SUCCESS	Length: 24576
120	23:32:09	ccSvcHst...	SET INFORMATION	C:\WINDOWS\system32\config\software.LOG	SUCCESS	Length: 28672
121	23:32:13	ccSvcHst...	QUERY INFORMATION	C:\WINDOWS\system32\SymNeti.dll	SUCCESS	Attributes: A
122	23:32:13	ccSvcHst...	QUERY INFORMATION	C:\WINDOWS\system32\SymNeti.dll	SUCCESS	Attributes: A
123	23:32:13	ccSvcHst...	QUERY INFORMATION	C:\WINDOWS\system32\SymNeti.dll	SUCCESS	Attributes: A
124	23:32:18	winlogon....	QUERY INFORMATION	C:\WINDOWS\system32\SnapShot.WAV	NOT FOUND	Attributes: Error
125	23:32:18	winlogon....	QUERY INFORMATION	C:\WINDOWS\system32\SnapShot.WAV	NOT FOUND	Attributes: Error
126	23:32:18	winlogon....	QUERY INFORMATION	C:\WINDOWS\system32\SnapShot.WAV	NOT FOUND	Attributes: Error
127	23:32:18	winlogon....	QUERY INFORMATION	C:\WINDOWS\system\SnapShot.WAV	NOT FOUND	Attributes: Error
128	23:32:18	winlogon....	QUERY INFORMATION	C:\WINDOWS\SnapShot.WAV	NOT FOUND	Attributes: Error
129	23:32:18	winlogon....	QUERY INFORMATION	C:\WINDOWS\system32\SnapShot.WAV	NOT FOUND	Attributes: Error
130	23:32:18	winlogon....	QUERY INFORMATION	C:\WINDOWS\SnapShot.WAV	NOT FOUND	Attributes: Error
131	23:32:18	winlogon....	READ	C:	SUCCESS	Offset: 8192 Length: 4096
132	23:32:18	WINWO...	READ	C:	SUCCESS	Offset: 4051968 Length: 4096
133	23:32:18	winlogon....	QUERY INFORMATION	C:\WINDOWS\System32\Wbem\SnapShot.WAV	NOT FOUND	Attributes: Error
134	23:32:18	winlogon....	QUERY INFORMATION	C:\Program Files\ATI Technologies\ATI Control Panel\SnapShot.WAV	NOT FOUND	Attributes: Error
135	23:32:18	winlogon....	QUERY INFORMATION	C:\Program Files\SecureCRT\SnapShot.WAV	NOT FOUND	Attributes: Error
136	23:32:18	winlogon....	QUERY INFORMATION	C:\Program Files\Microsoft SQL Server\80\Tools\Binn\SnapShot.WAV	NOT FOUND	Attributes: Error
137	23:32:18	winlogon....	QUERY INFORMATION	C:\Program Files\Microsoft SQL Server\90\Tools\binn\SnapShot.WAV	NOT FOUND	Attributes: Error
138	23:32:18	winlogon....	QUERY INFORMATION	C:\Program Files\Microsoft SQL Server\90\DTS\Binn\SnapShot.WAV	NOT FOUND	Attributes: Error
139	23:32:18	winlogon....	READ	C:	SUCCESS	Offset: 53248 Length: 4096
140	23:32:18	WINWO...	READ	C:	SUCCESS	Offset: 3380224 Length: 4096
141	23:32:18	winlogon....	QUERY INFORMATION	C:\Program Files\Microsoft SQL Server\90\Tools\Binn\VSShell\Common7\I...	NOT FOUND	Attributes: Error
142	23:32:18	winlogon....	READ	C:	SUCCESS	Offset: 4096 Length: 4096
143	23:32:18	winlogon....	QUERY INFORMATION	C:\WINDOWS\Media\SnapShot.WAV	NOT FOUND	Attributes: Error
144	23:32:23	ccSvcHst...	QUERY INFORMATION	C:\WINDOWS\system32\SymNeti.dll	SUCCESS	Attributes: A
145	23:32:23	ccSvcHst...	QUERY INFORMATION	C:\WINDOWS\system32\SymNeti.dll	SUCCESS	Attributes: A
146	23:32:23	ccSvcHst...	QUERY INFORMATION	C:\WINDOWS\system32\SymNeti.dll	SUCCESS	Attributes: A

Рис. 11.13. Программа протоколирует операции доступа к файлам компьютера

Диагностика службы каталогов

Следствием неисправностей функционирования службы каталогов (Active Directory, AD) неизбежно являются отказы информационной системы. В обязанности системного администратора входит предупреждение отказов, своевременное их обнаружение и устранение в сжатые сроки.

На работоспособность AD оказывают влияние как "собственные" службы, так и подсистемы, обеспечивающие функционирование сетевой инфраструктуры: службы динамического назначения параметров протокола и разрешения имен (DHCP, DNS, WINS), службы аутентификации пользователей (Net Logon, Kerberos), репликации данных (FRS), синхронизации времени, собственные службы AD: KDC (Key Distribution Center), KCC (Knowledge Consistency Checker), ISTG (Intersite Topology Generator), TRS (Time Reference Server) и т. д.

Поэтому работы по поиску неисправностей должны включать анализ всех компонентов системы, начиная от проверки кабельной структуры.

Обнаружение неисправностей AD

Системный администратор должен принять максимум усилий, чтобы обнаружить и правильно интерпретировать первые предвестники неисправности AD. В первую очередь этому поможет анализ файлов протоколов систем. Особое внимание необходимо уделить событиям, перечисленным в табл. 11.3.

Таблица 11.3. *Перечень файлов, подлежащих анализу*

Источник	Номер события
FRS	13508, 13509, 13512, 13522, 13567, 13568
Netlogon	5774, 5775, 5781, 5783, 5805
NTDS	1083, 1265, 1388, 1645
UserEnv	1085
W32Time	13, 14, 52-56, 60-64

К сожалению, появление записей об ошибках в протоколах событий, как правило, уже свидетельствует о наличии проблем. Конечно, можно включить расширенные возможности аудита *(см. разд. "Настройка дополнительного протоколирования" ранее в этой главе)*, но в нормальных условиях эта настройка обычно не используется, поскольку снижает полезную производительность системы. Если администратор хочет своевременно обнаруживать проблемы функционирования AD и ликвидировать их еще до того момента, как они приведут к сбоям служб бизнес-структуры, следует использовать любую систему мониторинга реального времени.

В качестве одной из таких систем в настоящей книге упомянут Microsoft Operation Management Server 2005, но администратор может применить любое решение, оптимально подходящее для конкретных условий его организации. Главное, чтобы в нем была реализована функция активного контроля критичных для данной организации служб AD.

Следует внимательно относиться ко всей информации пользователей. Например, информация о том, что система второй раз запросила смену пароля пользователя, может косвенно свидетельствовать о проблемах репликации двух контроллеров AD.

Средства тестирования AD

Для проверки функционирования службы каталогов можно использовать любые утилиты, которые взаимодействуют с AD.

В первую очередь это три стандартные консоли управления AD: пользователи и компьютеры, доверительные отношения и домены, сайты. В состав

Resource Kit входит ряд утилит, которыми можно воспользоваться для диагностирования проблемы. Это `dcdiag`, специально предназначенная для тестирования AD. Кроме того, для тестирования инфраструктуры можно воспользоваться утилитами, перечисленными в табл. 11.4.

Таблица 11.4. *Утилиты для тестирования инфраструктуры*

Утилита	Для чего используется
netdiag.exe	Проверка сетевой инфраструктуры
netdom.exe	Проверка и управление доверительными отношениями
nltest.exe	Проверка состояния secure channel
ntfrsutl.exe	Управление службой репликации файлов
dsastat.exe	Анализ состояний AD на различных контроллерах
repadmin.exe	Проверка репликации данных AD, возможности инициировать частичную или полную репликацию заданного контекста
replmon.exe	Контроль репликации данных и запуск ручной репликации (графическая утилита)

Можно также воспользоваться утилитами, позволяющими отображать необходимую структуру AD и менять параметры объектов (табл. 11.5).

Таблица 11.5. *Утилиты для отображения структуры AD и изменения параметров объектов*

Утилита	Для чего используется
ADSI Edit	Просмотр и редактирование объектов AD, установка списков доступа (access control lists, ACLs)
ldp.exe	Взаимодействие с AD по протоколу LDAP

Для проверки сетевых соединений и их качества можно использовать любые утилиты из состава операционной системы *(см. разд. "Диагностика IP-протокола" главы 3)*. Кроме того, при анализе и настройке AD придется использовать оснастки управления DNS, монитора производительности, утилиту редактирования реестра, утилиту управления AD с возможностью модификации ее метаданных — ntdsutil.exe и т. д.

Хочу посоветовать приобрести утилиту Insight for Active Directory, автономную или в составе Winternals Administrator's Pak 5.0 (**http://www.winternals.com/**), позволяющую наблюдать ответы службы каталогов в реальном времени (см. рис. 11.6).

Проверка разрешения имен

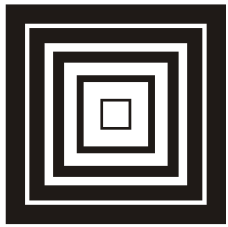
Как уже было сказано, комплексную проверку доступности служб AD можно осуществить с помощью утилиты `dcdiag`. Но поскольку она устанавливается дополнительно, то в оперативных случаях следует быть готовым выполнить простейшие проверки стандартными средствами операционной системы. Обычно достаточно проконтролировать возможность разрешения имен с помощью типовых утилит *(см. разд. "Диагностика IP-протокола" главы 3)*. Следует проверить достижимость контроллера домена по его краткому (без доменного суффикса) и полному имени, а также разрешение адресов служб AD. Соответствующая структура DNS создается автоматически, и обычно достаточно проконтролировать ее наличие в оснастке управления сервером DNS. Если такая возможность отсутствует, то нужно вручную, с помощью `nslookup`, выполнить попытку разрешения имен[1], перечисленных в табл. 11.6.

Таблица 11.6. *Перечень имен, проверяемых в процессе теста*

Имя	Тип записи	Чему соответствует
_ldap._tcp.dc._msdcs.<*DNS_имя_домена*>	SRV	Контроллер домена
_ldap._tcp.pdc._msdcs.<*DNS_имя_домена*>	SRV	Эмулятор первичного контроллера
_ldap._tcp.gc._msdcs.<*DNS_имя_леса*>	SRV	Сервер глобального каталога
_kerberos._tcp.dc._msdcs.<*DNS_имя_домена*>	SRV	Расположение службы Kdc

Обратите внимание на весьма простую операцию, удачное выполнение которой зависит от правильности настройки системы разрешения имен и от функционирования контроллера домена. Попробуйте открыть следующий сетевой ресурс: \\<*DNS_имя_домена*>\SYSVOL. Если попытка неудачна, то либо в организации неверно настроено разрешение имен, либо контроллер домена неработоспособен.

[1] Для разрешения имен служб (записи типа SRV) следует в `nslookup` предварительно выполнить команду `set type=all` или `set type=srv`. Обратите также внимание, что в операции разрешения имени сервера глобального каталога указывается имя леса, а не домена. Обычно в малых организациях эти имена совпадают.



ГЛАВА 12

Цифровые сертификаты

Сегодня практически единственной возможностью обеспечить безопасность данных, как при передаче их по сети, так и при хранении, является криптографическая защита (шифрование). Наиболее распространенным вариантом является шифрование с использованием двух ключей, для которого важную роль играют цифровые сертификаты. Они необходимы для шифрования файловой системы и использования служб управления правами доступа к документам, при создании писем с электронной подписью или с шифрованным содержанием, для функционирования IPSec, для идентификации информационных серверов и т. д.

Всем пользователям и администраторам систем следует четко понимать, что сертификаты, электронные подписи и т. п. — это только часть системы безопасности, не работающая "в отрыве" от других компонентов. Письмо, содержащее электронную подпись Иванова, совсем не подтверждает факт написания этого письма известным вам человеком. Что мешает другому пользователю получить сертификат на имя и фамилию данного человека в каком-либо центре сертификации? Например, даже установив свой центр выдачи сертификатов. На этом основаны многие технологии мошенничества, когда создаются фиктивные интернет-магазины, главной целью которых является сбор номеров и личных кодов пластиковых расчетных карт. Да, вы передаете свои данные по зашифрованным каналам связи, но вы отдаете их мошенникам...

Рассмотрим основные понятия, используемые при защите данных.

Симметричное шифрование

Самый простой способ организовать защищенный обмен информацией — это иметь "с каждой стороны" уникальный пароль. Если каждый участник знает такой пароль, то с помощью хорошо разработанных методов криптографии можно организовать безопасную передачу данных. Причем аутентификация

каждого участника обмена информацией выполняется очень легко: если данные расшифровываются, значит, они поступили от того человека, который знает данный пароль. Если данные не расшифровываются, то они либо изменены в процессе передачи, либо отправлены/читаются не тем, кому "положено". При этом предполагается, что для защиты используемого ключа (пароля) от несанкционированного доступа приняты надежные меры.

Методы *симметричного*[1] *шифрования* широко известны и хорошо проверены. Информация надежно шифруется и не может быть взломана за короткое время. Конечно, при необходимости серьезной защиты пароль должен состоять из большого количества символов. Используют несколько стандартных размеров пароля, например: 512, 1024, 2048, 4096 байтов и т. д. Чем длиннее пароль, тем надежнее защита, но при этом существенно замедляются процессы шифрования/дешифрования. На практике длина пароля выбирается из компромисса между скоростью работы и надежностью защиты информации.

Примечание

Понятно, что пароль длиной в тысячу символов ввести с клавиатуры практически невозможно, поэтому его сохраняют в виде файла на съемном носителе, а чтобы никто другой не мог использовать этот пароль, сам файл пароля закрывается каким-либо пользовательским паролем. Принято называть такой длинный пароль (в виде файла) *ключом*.

По данной технологии сейчас строится работа многих финансовых учреждений с онлайновым обслуживанием клиентов: перед началом работы вы получаете ключевую дискету, которая используется для удостоверения личности в процессе последующей работы.

Если пароль будет дискредитирован (например, ключевая дискета утеряна либо похищена), то вы сообщаете об этом в соответствующие службы организации, выдавшей дискету. После этого вы должны *прибыть в эту организацию лично за новым ключом*. При личной встрече уполномоченные представители этой организации проверят ваши документы и только после этого выдадут новый ключ.

Шифрование с помощью двух ключей

Технология симметричного шифрования удобна всем: операции шифрования и дешифрования выполняются быстро, сама технология надежна и т. п. Проблема только в том, *как безопасно передать ключ* при использовании обыч-

[1] Шифрование именно потому и называется симметричным, что с каждой стороны используется одинаковый пароль.

ных, открытых каналов связи. Конечно, можно рассылать пароли по запросу, например спецпочтой, но это далеко не самый быстрый и дешевый способ. Если использовать открытые каналы связи для передачи информации, то всегда существует вероятность, что кто-то сможет "расположиться" между участниками и, перехватывая весь трафик, соответствующим образом его модифицировать.

Проблема была решена после разработки методов *шифрования, основанных на двух ключах.*

При этой технологии пользователь получает два взаимосвязанных ключа, один из которых принято называть *открытым*, а другой — *закрытым (личным)*. Ключи связаны друг с другом (являются парой), но восстановить один из них по-другому очень трудно даже теоретически. Можно считать, что практически невозможно. При шифровании данных используется всегда два ключа: один ключ (личный) того пользователя, который шифрует данные, а другой (публичный) — того, кому эти данные предназначены. Причем для расшифровки данных могут быть использованы *только* вторые ключи пары.

Поэтому появилась возможность хранить один из ключей пары в открытой сети, поскольку он используется только для шифрования данных. Этот ключ стали называть *открытым ключом*. Второй ключ, нужный для процесса дешифрования, следует хранить в безопасном месте, поскольку доступ к нему злоумышленника означает возможность дешифровки данных.

Шифрование информации с использованием двух ключей при существующих сегодня алгоритмах — более медленная операция, чем в случае применения одного ключа (метода симметричного шифрования). Поэтому на практике шифрование с использованием двух ключей производится только на этапе аутентификации клиента сервером. Далее создается случайный секретный ключ, известный обоим участникам, который и используется для быстрого шифрования/дешифрования данных.

Основная проблема в данном типе шифрования — это необходимость каким-то образом подтвердить принадлежность открытого ключа конкретному пользователю. Кто мешает мне создать пару ключей и назваться при этом чужим именем? А если кто-то сможет перехватывать все передаваемые данные, то он будет способен подменять открытые ключи другого человека своими[1]. В связи с этим возникла необходимость в электронном документе, который удостоверял бы принадлежность открытого ключа. Таким документом стал цифровой сертификат, выдаваемый центром сертификации.

---

[1] Например, если я смогу перехватить передаваемый по электронной почте открытый ключ и заменить это письмо на другое, со своим ключом, то при всех следующих операциях я смогу дешифрировать передаваемые закрытые данные своим ключом, а потом вновь шифровать их для другого участника. Такую подмену обнаружить практически невозможно.

Цифровой сертификат

Цифровой сертификат является по своей сути аналогом бумажного удостоверения пользователя, но только в электронном виде. Основная задача сертификата — подтвердить принадлежность открытого ключа данному пользователю.

Реально цифровой сертификат — это электронный документ, который содержит открытый ключ пользователя и набор данных, описывающих владельца сертификата. Цифровой сертификат подписывается закрытым ключом центра сертификации, что гарантирует целостность его данных. Срок действия цифровой подписи, а значит, и сертификата установлен законодательно и равен одному году.

В соответствии с Законом Российской Федерации "Об электронной цифровой подписи" № 1-ФЗ от 10 января 2002 года в цифровом сертификате должны содержаться:

- уникальный регистрационный номер сертификата ключа для подписи, даты начала и окончания срока действия сертификата ключа подписи, находящегося в реестре удостоверяющего центра;
- фамилия, имя и отчество владельца сертификата ключа для подписи или псевдоним владельца. В случае использования псевдонима удостоверяющим центром вносится запись об этом в сертификат ключа подписи;
- открытый ключ электронной цифровой подписи;
- наименование средств электронной цифровой подписи, с которыми используется данный открытый ключ электронной цифровой подписи;
- наименование и место нахождения удостоверяющего центра, выдавшего сертификат ключа подписи;
- сведения об отношениях, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение.

Кроме того, в сертификаты включаются дополнительные технические параметры (используемый алгоритм шифрования, длина ключа и т. п. — набор параметров зависит от используемого международного стандарта, в соответствии с которым выдается сертификат).

При выполнении операций программа проверяет данные сертификата и при наличии ошибок (таких как истечение срока полномочий сертификата, его отзыв центром сертификации и т. п.) выводит соответствующее сообщение.

Как уже упоминалось, сертификат подтверждается цифровой подписью удостоверяющего центра. В свою очередь это означает, что мы должны доверять

такому центру сертификации *(см. разд. "Доверенные центры сертификации" далее в этой главе)*.

Структура Public Key Infrastructure

Несмотря на кажущуюся простоту применяемых принципов, использование шифрования на основе открытых ключей является надежным только при наличии определенной инфраструктуры, а именно:

- должны существовать удостоверяющие центры, которые выдают ключи, подтверждают их принадлежность и которым доверяют пользователи, обменивающиеся информацией;
- необходимо функционирование системы отзыва сертификатов (в случае утери ключа, увольнения сотрудника, если у него был служебный ключ и т. п.);
- должны быть разработаны способы перекрестной сертификации (если я доверяю центру сертификации А, а центр сертификации А доверяет центру сертификации Б, то я должен доверять и сертификатам, выданным центром Б);
- программное обеспечение клиентов должно уметь выполнять все необходимые операции и взаимодействовать с различными системами сертификации и существующими стандартами

и т. п.

Поэтому говорят, что для использования технологии шифрования на базе открытого ключа необходимо наличие инфраструктуры открытого ключа — Public Key Infrastructure (PKI).

Центр сертификации

В структуре PKI особую роль имеют *удостоверяющие центры* (или *центры сертификации*). Что такое удостоверяющий центр? Это "некто", кто выдает пользователю электронное удостоверение, которому должны доверять другие пользователи. Проведем аналогию с бумажными документами. Мы имеем паспорт, который служит документом в любой точке страны. Он выдается нам органами внутренних дел в соответствии с законодательством. У нас есть и иные документы, удостоверяющие личность, например, пропуск на предприятие, однако он имеет силу (ему "верят") только в пределах территории учреждения, которое его выдало. Какой бумажный документ вы будете использовать при приобретении авиабилета? А к какому центру сертификации следует обратиться за получением "документа", которому бы доверяли дру-

гие пользователи Сети? В условиях отсутствия единого руководства Интернета такого *единого центра просто не может быть*.

Создать удостоверяющий центр очень легко. Соответствующее программное обеспечение входит в пакет установки, например Windows Server 200*x*. Но что следует сделать, чтобы документы, выданные таким центром, "работали"?

Доверенные центры сертификации

Поскольку сертификаты может выдавать практически кто угодно, неизбежно должна была возникнуть технология выделения той части центров сертификации, которым пользователь будет доверять и признавать их цифровые документы. Эта технология была реализована созданием перечня *доверенных центров сертификации*.

Доверенные центры сертификации — это те центры, сертификатам которых доверяет данный пользователь (компьютер).

Существуют центры сертификации, сертификаты которых уже включены в пакет установки Windows. Такие центры изначально отнесены к доверенным корневым центрам сертификации (этот перечень можно увидеть в окне свойств обозревателя — см. **Свойства обозревателя** | закладка **Содержание** | кнопка **Сертификаты**; второй способ просмотра — это использование оснастки управления сертификатами). Но администратор может легко изменить этот список, исключив некоторые центры из списка или добавив новые.

Перед включением центра сертификации в число доверенных необходимо получить его сертификат. Как получить его и проверить, что это сертификат именно данного центра, — отдельная задача.

После получения сертификата его следует установить на компьютер. Для этого используется мастер установки сертификатов. Он запускается либо после двойного щелчка по файлу сертификата, либо вручную из оснастки управления сертификатами при помощи следующих действий:

1. Наберите в командной строке `mmc` и нажмите клавишу <Enter>. На экране появится пустая консоль управления; выберите в меню консоли команду **Добавить или удалить оснастку**.
2. Появится диалоговое окно **Добавить/удалить оснастку**. Нажмите в данном окне кнопку **Добавить**.
3. В диалоговом окне **Добавить** выберите строку **Сертификаты** и нажмите кнопку **Добавить**.
4. В появившемся окне выберите требуемый вариант: если вы хотите установить сертификат для всего компьютера (для всех пользователей, которые будут на нем работать), то используйте вариант "компьютер", если хотите

управлять сертификатом только своей учетной записи, то отметьте вариант "моя учетная запись".

5. Закройте все окна с сохранением результатов.

В результате у вас появится оснастка управления сертификатами, в которой можно выполнить любую операцию управления сертификатом: удалить сертификат, импортировать новый сертификат и поместить его в группу доверенных, запросить новый сертификат и т. д. Например, чтобы импортировать сертификат и сделать его доверенным, следует вызвать команду импорта, выбрать опцию дополнительных установок и указать хранилище, в которое будет установлен новый сертификат.

Примечание

При создании в Windows центров сертификации предприятия, интегрированных со службой каталогов, они автоматически становятся доверенными центрами сертификации данного предприятия. Если администратор решает использовать автономные центры, то для них необходимо установить доверие описанным способом.

Такое большое внимание списку доверенных центров сертификации мы уделяем потому, что если вы захотите использовать сертификат от центра, не включенного в данный список, то программа выдаст предупреждение об отсутствии доверительных отношений с данным центром. На практике при появлении такого предупреждения в подавляющем большинстве случаев пользователь, даже не разбираясь в причинах данного оповещения, прекратит работу, например, с письмом, подписанным с использованием этого сертификата.

Установка центра сертификации

Программное обеспечение, необходимое для установки удостоверяющего центра, входит в состав дистрибутивов серверов Windows 2000/2003. Для установки достаточно только отметить соответствующую опцию в списке компонентов Windows (по умолчанию центр сертификации не устанавливается). Однако перед тем как установить центр, необходимо тщательно продумать будущую структуру сертификатов организации. Выдаваемые сертификаты содержат адрес центра сертификации, поэтому желание, например, изменить имя такого компьютера приведет к невозможности работы с уже выданными сертификатами. Кроме того, компьютеры, на которых установлены центры сертификации предприятия, не могут быть удалены из домена и т. п.

Так же тщательно должны быть продуманы организационные меры. Какова будет процедура выдачи сертификатов, как выдавать особо ответственные

сертификаты (например, их можно выдавать только при наличии нескольких цифровых подписей различных сотрудников), как будет защищен сервер сертификатов и т. д.

Центр сертификации можно установить автономно (на любой компьютер, независимо от членства в домене) и в составе предприятия (только интегрированно со службой каталогов). Преимущество автономного центра сертификации в том, что вы можете произвольно определить в нем любые параметры (имя, назначение центра и т. п.). За счет интеграции со службой каталогов центры сертификации предприятия позволяют автоматизировать ряд операций, поскольку сертификатам таких центров уже установлено доверие: можно автоматизировать выдачу сертификатов, используется принятая в домене система безопасности при выдаче сертификатов и т. п.

Центр сертификации может быть *корневым* ("выше" его нет центра сертификации, поэтому сертификат такого удостоверяющего центра подписывается *собственной* подписью этого центра) или *подчиненным* (сертификат такого центра подписан каким-либо *другим* центром сертификации). На предприятии (в лесу доменов) может быть установлен только один корневой центр сертификации. В то же время вы можете установить столько автономных корневых центров сертификации, сколько необходимо для работы.

Вначале мастер установки удостоверяющего центра запрашивает тип центра сертификации, который предполагается установить. Далее следует выбрать технические параметры центра и ввести его описание. Если к центру не предъявляются особые требования, то для таких параметров, как длина используемого ключа шифрования, можно установить значения по умолчанию. Обратите внимание, что данные, определяемые в описании центра при работе мастера установки, будут включены в состав сертификатов, поэтому целесообразно вводить их, например, на английском языке, с указанием международных кодов телефонных номеров и т. п.

Примечание

При установке подчиненного автономного центра сертификации следует выбрать опцию дополнительных настроек и указать операцию импорта ключа, выданного для установки такого центра.

Настройка центра сертификации

Сразу после установки центр сертификации уже может выдавать сертификаты основных типов: для идентификации пользователя, для шифрования файлов и т. п. В зависимости от потребностей организации центр сертификации сервера Windows 2003 позволяет определить типы сертификатов, которые будут им выдаваться.

В этой же оснастке администратор может увидеть список выданных центром сертификатов, отозвать сертификат, выполнить операцию резервного копирования или восстановления центра.

Центр сертификации выдает сертификаты, основываясь на *шаблонах*. Шаблоны (templates) содержат информацию о том, для каких целей выдается данный тип сертификата. Каждый шаблон имеет параметры безопасности, которые определяют, кто управляет использованием данного шаблона и какие лица могут получить сертификат данного типа.

Примечание

Администратор может изменить эти параметры безопасности. Например, если вы предполагаете предоставить право выдачи сертификатов для смарт-карт конкретному пользователю, то необходимо предоставить такое право данному сотруднику в шаблоне типа enroll.

Публикация шаблонов сертификатов

По умолчанию центр сертификации выдает только типовые сертификаты. Если вы хотите, например, получить сертификат для подтверждения сервера IAS или внедрить у себя корпоративную политику, предусматривающую хранение ключей в службе каталогов, то необходимо настроить сервер для выдачи сертификатов соответствующих типов. Эта операция называется *публикацией шаблона сертификата*.

Для этого в оснастке **Центр сертификации** нужно выделить папку шаблонов Шаблоны сертификатов (рис. 12.1) и в меню ее свойств выполнить операцию публикации нового шаблона (**Создать | Выдаваемый шаблон сертификата**). После чего достаточно выбрать необходимый шаблон из показанного списка и завершить операцию.

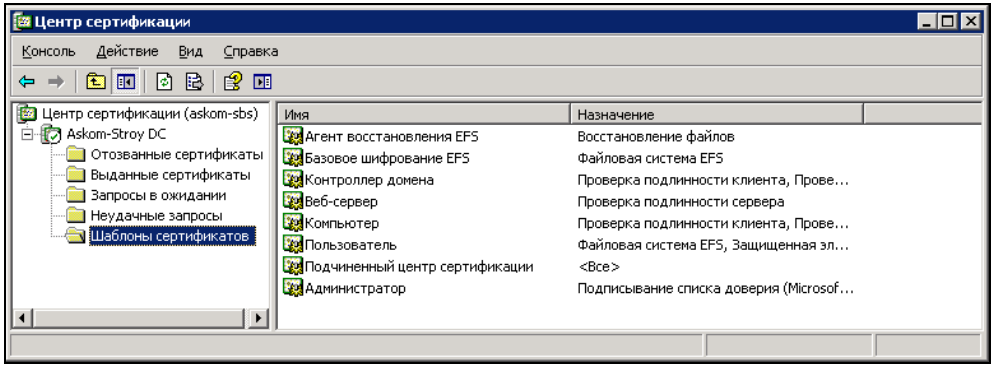


Рис. 12.1. Центр сертификации на основе Windows 2003

Примечание

Некоторые типы сертификатов доступны только в центре сертификации Enterprise версии Windows 2003.

Опубликованные таким образом шаблоны используют значения по умолчанию. Иногда необходимо откорректировать часть параметров, таких как срок действия сертификата, круг пользователей, которые могут его запрашивать, ужесточить алгоритм шифрования и т. п. В этом случае придется менять свойства соответствующих шаблонов. Обычно рекомендуется исходные шаблоны не править, а скопировать их в новый шаблон, который уже и откорректировать в соответствии с существующими требованиями.

Для управления свойствами шаблона необходимо открыть оснастку, выбрав пункт **Управление** в динамическом меню для папки **Шаблоны сертификатов**, после чего выделить необходимый сертификат и приступить к редактированию его свойств (рис. 12.2).

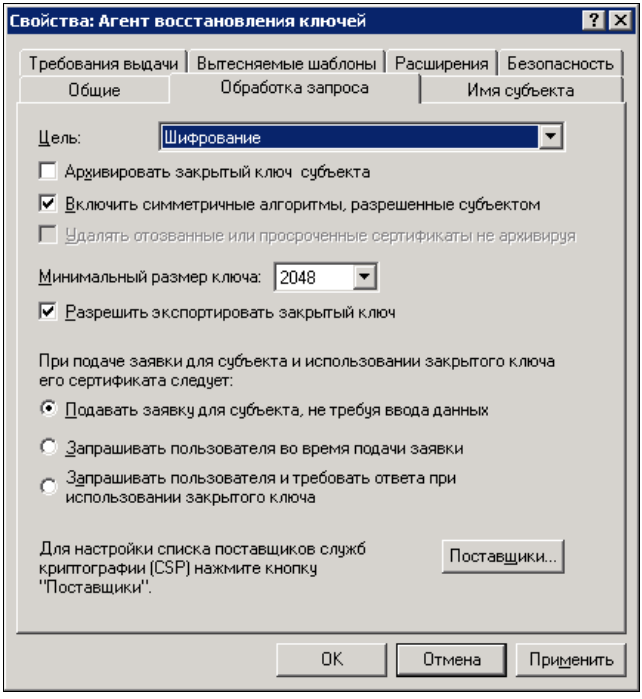


Рис. 12.2. Окно редактирования свойств шаблона сертификата

Резервное копирование центра сертификации

Администраторы могут выполнять резервное копирование центра сертификации независимо от создания копии всей операционной системы. Чтобы

провести резервное копирование только центра сертификации[1], необходимо открыть оснастку его управления и выбрать операцию резервного копирования, после чего указать путь (резервное копирование производится в пустую папку), тип (полное или инкрементальное) и защитить получаемый архив паролем.

Восстановление центра сертификации не представляет особой сложности. Если необходимо восстановить центр сертификации *после переустановки операционной системы*, то следует учесть, что "чистая" установка ведет к созданию *новых ключей*[2] центра сертификации. Поэтому перед восстановлением следует сначала установить тот сертификат, который был сохранен при операции резервного копирования[3], после чего при установке службы центра сертификации выбрать в дополнительных опциях вариант использования имеющегося на компьютере сертификата. Для этого при установке **Службы сертификации** нужно выбрать опцию **Измененные параметры создания пары ключей и сертификата ЦС**. На следующем шаге мастера установки следует выбрать опцию **Использовать существующий ключ** и указать на нужный ключ (при необходимости сертификат можно просмотреть). В завершение процедуры нужно восстановить базу центра сертификации.

Если восстановление производится не на новый компьютер, а на уже работающую систему, и если на диске сохранились файлы центра сертификации (установленный сертификат центра и папка CertLog), то восстановление можно провести *без наличия файлов резервного копирования*. Для этого после выбора установленного сертификата (аналогично выше описанному способу) на следующем шаге мастера надо отметить пункт использования существующей базы данных центра сертификации.

Примечание

После восстановления центра сертификации из резервной копии необходимо опубликовать вручную список отозванных сертификатов *(см. следующий раздел)*. В противном случае использование сертификатов будет невозможно до того момента, когда будет произведена ближайшая автоматическая публикация отозванного списка.

База данных центра сертификации представляет собой типовую базу данных сервера Windows. Для ее ремонта и восстановления в случае необходимости вы можете использовать утилиту `esentutil`.

---

[1] Резервное копирование центра сертификации входит в состав резервного копирования состояния системы (system state) соответствующего сервера.

[2] Это влечет за собой возникновение проблем с ранее выданными (по старой паре ключей) сертификатами.

[3] Этот сертификат сохраняется в папке резервного копирования. Для его установки на сервер достаточно выбрать данный сертификат, в результате запустится мастер операций, рекомендациям которого и нужно следовать.

Отзыв сертификатов

Сертификаты имеют определенный срок действия, после завершения которого они уже не могут быть использованы в новых операциях (например, для создания электронной подписи письма), но могут применяться, например, для расшифровки ранее созданных файлов.

Возникают различные ситуации, когда необходимо запретить использование выданного сертификата, у которого еще не истек срок действия. Например, в случае кражи ноутбука с установленным сертификатом пользователя. В подобных случаях необходимо *отозвать* сертификат.

Отзыв сертификата осуществляется из консоли управления центра сертификации. Необходимо найти сертификат в списке выданных, отметить его и в меню свойств выбрать операцию отзыва. Далее следует указать причину, по которой сертификат признается недействительным.

Причины отзыва имеют, скорее, информационное значение. Пользователь сможет их увидеть, но реакция системы во всех случаях будет одна: невозможность выполнения действий с данным сертификатом. Тем не менее одна причина отзыва имеет особый статус. Если вы предполагаете *временно* отозвать сертификат по каким-либо причинам, то необходимо указывать *только* причину **Certificate Hold**. В этом случае сертификат можно "восстановить". Во всех остальных случаях выполняемая операция отзыва *необратима*.

Список отозванных сертификатов (Certificate Revocation List, CRL) публикуется центром сертификации. Выполняется это автоматически по заданному расписанию. По умолчанию ежедневно публикуются частичные списки (изменений), а раз в неделю — обновляется весь лист. При необходимости вы можете ускорить процесс публикации, если в меню свойств папки отозванных сертификатов выбрать операцию публикации.

Примечание

Если CRL недоступен по той или иной причине (например, еще не опубликован и не реплицировался в службе каталогов), то использование сертификатов будет невозможно. Если включен аудит событий входа в систему, то в файле протокола можно будет увидеть соответствующие сообщения Kerberos.

Получение цифровых сертификатов

Получение сертификатов осуществляется по правилам соответствующих удостоверяющих центров. Для центров сертификации из состава Windows 200*x* Server существуют варианты *автоматической* и *ручной выдачи* сертификатов.

- **Автоматическая выдача сертификатов.**

  Возможна только в центрах сертификации предприятия, интегрированных со службой каталогов.

  Автоматически могут выдаваться сертификаты не всех типов. Кроме того, для получения сертификатов компьютеров, сертификатов для создания IPSec-соединений и т. п. необходимо предварительно настроить центр сертификации на их выдачу (установить соответствующие шаблоны).

  Чтобы включить автоматическую выдачу сертификатов, необходимо настроить соответствующую групповую политику, разрешив автоматическую выдачу сертификатов определенного типа (рис. 12.3).

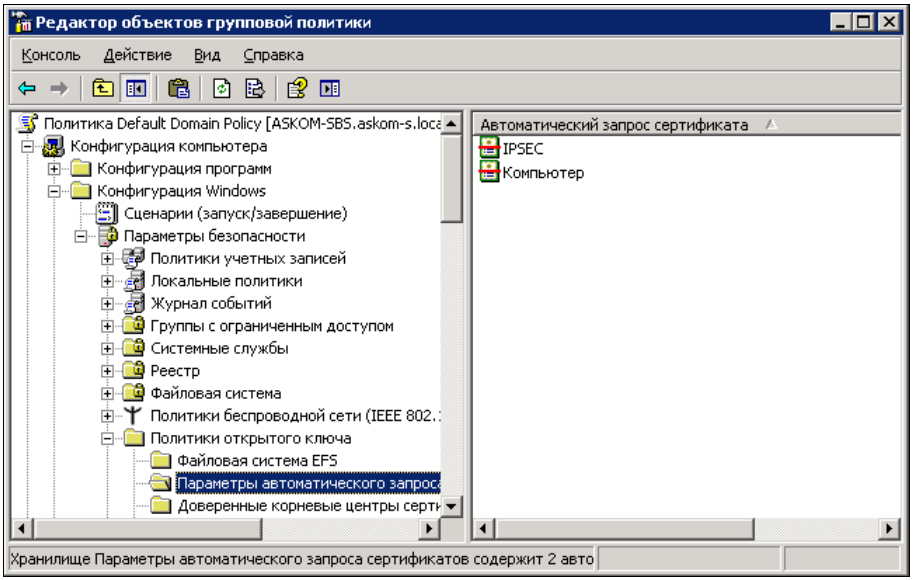


Рис. 12.3. Настройка перечня автоматически выдаваемых сертификатов

После создания и распространения такой групповой политики вы сможете проконтролировать получение сертификатов по списку окна выданных сертификатов в оснастке управления удостоверяющего центра.

- **Получение сертификатов после подтверждения администратора.**

  Если удостоверяющий центр автономен, то автоматическая выдача сертификатов невозможна. В этом случае пользователь (компьютер), желающий получить сертификат, выполняет операции по запросу сертификата и отсылает заявку (запрос) на выдачу сертификата.

  Запросы на выдачу сертификатов отображаются в оснастке управления удостоверяющего центра. Чтобы выдать сертификат, администратор цен-

тра должен найти соответствующий запрос и в его меню выбрать операцию выдачи сертификата.

По истечении некоторого времени, отведенного на обработку заявки в центре, пользователь должен вновь обратиться к удостоверяющему центру и проверить наличие выданного сертификата (выполняется с помощью той же программы, которой был сформирован первоначальный запрос). При наличии сертификата пользователь имеет возможность установить его на компьютер.

- **Получение сертификатов пользователем.**

  Существует две технические возможности получения сертификатов пользователем. Первая — это использование оснастки управления сертификатами, а вторая — через обозреватель Интернета[1].

  Чтобы открыть оснастку управления сертификатами, необходимо вызвать консоль управления (`mmc`) и добавить оснастку управления сертификатами (для получения пользовательского сертификата выбирается опция **пользователь**), после чего можно, выделив папку сертификатов, выполнить из ее меню команду запроса нового сертификата. Данная операция не требует от пользователя административных прав на персональном компьютере.

  Если у пользователя есть локальные административные права, то он может получить сертификат через Web-интерфейс. Для этого следует открыть в MS Internet Explorer страницу **http://<*имя_сервера_сертификатов*>/CertSrv** и "пройти" по страницам мастера выдачи сертификатов, не забыв согласиться на установку модулей ActiveX.

Примечание

Если сертификат запрашивается с удостоверяющего центра предприятия[2], то он будет выдан сразу же в процессе запроса. Если центр сертификации установлен автономно, то пользователь только сформирует запрос на получение сертификата. Для установки сертификата необходимо — после его ручной выдачи — вновь повторить операцию, выбрав в меню пункт проверки выдачи сертификатов.

Как уже было сказано, срок действия сертификата ограничен. При его завершении удобно воспользоваться оснасткой управления сертификатами и запросить продление срока действия текущего сертификата. Выполнять эту операцию желательно *до момента окончания срока действия сертификата*. В противном случае можно будет получить только *новый* сертификат.

---

[1] Выдача сертификатов с использованием обозревателя Интернета является опцией установки центра сертификации. Обычно такую возможность не отключают.

[2] При использовании шаблонов сертификатов версии 2 (доступны для центров сертификации на Windows 2003 Enterprise) администратор имеет возможность установить необходимость ручного подтверждения выдачи сертификата и при использовании центра сертификации предприятия.

Получение коммерческих сертификатов

Сертификат можно получить и в коммерческих центрах. Перед получением такого сертификата необходимо зайти на сайт центра (его адрес можно увидеть в свойствах сертификата центра; список сертификатов основных коммерческих центров можно просмотреть в свойствах обозревателя MS Internet Explorer) и ознакомиться с процедурой получения сертификата.

Часть центров предоставляет возможность получения ограниченных бесплатных личных сертификатов. Эти сертификаты могут быть использованы для создания электронной подписи и шифрования электронной переписки. Процедура запроса такого сертификата достаточно проста. Никто не запрещает вам представиться любым именем, единственный контролируемый параметр в этом случае — это адрес электронной почты, для которого создается сертификат.

Примечание

Облегчить поиск центра сертификации может помочь ссылка, включенная в настройки программ MS Office. При открытии окна настройки сертификатов в электронной почте можно нажать на кнопку **Получить удостоверение** и система откроет страничку с рекомендуемым списком центров сертификации. Так, центр **www.verisign.com** предоставляет бесплатные сертификаты на 60 дней, **www.thawte.com** и **www.trustcenter.de** — на год, и т. п.

Сертификаты для локального пользования

При установке высокого уровня безопасности для программ MS Office становится невозможным запускать не только сторонние макросы и сценарии, но и коды собственной разработки. Для тех пользователей, которые применяют макропрограммирование и не имеют либо коммерческих сертификатов, либо сертификатов организации, предусмотрена возможность создания *индивидуальных сертификатов*.

Индивидуальные сертификаты создаются с помощью специальной программы, включенной в состав MS Office (SelfCert.exe). Если установка этого пакета на компьютере не содержит компонента **Цифровой сертификат для проектов VBA**, его придется установить отдельно — он доступен через дополнительные параметры настройки установки. С его помощью формируются сертификаты, которые подписаны *самим пользователем*. Такие сертификаты можно применять для создания электронной подписи собственных кодов. Однако при попытке запуска сценария или макроса на другом компьютере эти сертификаты будут отклонены, поскольку к органу, выдавшему сертификат, отсутствует доверие.

Корпоративная политика управления сертификатами

В условиях корпоративной среды часто возникают ситуации, когда необходимо восстановить закрытый ключ сертификата того или иного пользователя. Например, в случае замены компьютера или увольнении сотрудника для получения доступа к зашифрованным этим сотрудником служебным документам. Для этого функционал центров сертификации предприятия обычно включает в себя возможность *восстановления* всех параметров личных сертификатов. Подобная возможность присутствует в опциях центра сертификации сервера Windows 2003, но только для редакции Enterprise.

Включая функцию хранения сертификатов корпоративного сервера в службе каталогов, многие администраторы даже и не подозревают о необходимости выполнения ряда дополнительных операций, описанных ниже, без которых восстановление закрытых ключей не осуществимо.

Примечание

Предоставлять право восстановления личного сертификата необходимо *только специально назначенным сотрудникам*. Бесконтрольное использование данной функции дискредитирует все усилия по обеспечению безопасности информации организации на основе внедрения сертификатов.

Настройка хранения закрытых ключей пользователей

Для настройки опции восстановления ключей сертификатов необходимо:

1. Настроить и выдать сертификат восстановления ключей (key recovery agent).
2. Выполнить настройки центра сертификации, указав пользователя (пользователей), которые будут иметь право восстановления ключей.
3. Опубликовать в центре сертификации шаблоны, которые включают в себя возможность централизованного хранения ключей.

Получение сертификата восстановления ключей

Сертификат восстановления ключей выдается на основе соответствующего шаблона, который присутствует только в версии Windows 2003 Enterprise. По умолчанию право выдачи такого сертификата предоставлено только администраторам домена или предприятия. В случае необходимости эту настройку можно еще более ужесточить, сменив разрешения доступа к данному шаблону.

Шаблон восстановления предполагает ручную выдачу сертификата. Это наиболее оптимальный вариант, позволяющий обеспечить необходимый уровень

безопасности. Кроме того, при получении сертификата целесообразно сохранить возможность экспорта ключей, чтобы сохранить копию, например, на дискете.

В остальном процедура публикации нового шаблона и получения сертификата стандартна. Следует выполнить публикацию нового шаблона (так, как было описано выше) и затем обычным образом сформировать запрос на сертификат, выбрав в настройках вариант сертификата восстановления. Естественно, что публикация шаблона и запрос могут быть успешными только в том случае, если они выполняются пользователем, обладающим необходимыми для этих операций правами.

Настройка центра сертификации

После выдачи хотя бы одного сертификата восстановления ключей можно указать в настройках центра сертификации пользователя, которому будет разрешена операция восстановления.

Для этого достаточно в свойствах центра сертификации указать на соответствующий сертификат.

Настройка сертификатов, выдаваемых пользователям

По умолчанию сертификаты, выдаваемые пользователям центром сертификации сервера Windows 2003, не содержат возможности восстановления ключей. Поэтому необходимо заменить шаблон, на основе которого выдаются сертификаты, на версию 2.

Примечание

В качестве криптопровайдера данного типа сертификатов поддерживается только алгоритм Rivest-Shamir-Adleman (RSA). Использование алгоритмов DSS или Diffie-Hellman не поддерживается. Поэтому если для закрытого ключа будет выбран не RSA-алгоритм, то такой ключ не будет сохранен в службе каталогов.

Публикация шаблона производится обычным образом. Опубликованный по умолчанию шаблон первой версии лучше удалить.

Для просмотра сертификатов, имеющих сохраненные в службе каталогов закрытые ключи, достаточно добавить в число отображаемых столбцов в перечне выданных сертификатов позицию **Архивированный ключ**. У тех сертификатов, для которых в данном поле стоит 1, ключи хранятся в службе каталогов.

Естественно, что после публикации нового шаблона вам следует позаботиться о том, чтобы пользователи запросили новые сертификаты. В противном случае процесс перехода на централизованное хранение ключей может затя-

нуться до года (срок жизни выданного сертификата пользователя по умолчанию).

Порядок восстановления закрытых ключей

Процедура восстановления закрытого ключа состоит из двух шагов. На первом этапе информация о закрытом ключе запрашивается из службы каталогов и сохраняется в виде файла, зашифрованного ключом сертификата агента восстановления. Следующим шагом производится дешифрование ключа и сохранение информации в pfx-файл, который затем может быть использован для установки сертификата с восстановленным ключом. Этот файл можно тем или иным безопасным способом передать пользователю, для которого производится восстановление данных.

После этого можно продолжить пользоваться сертификатом в полном объеме. Никаких дополнительных операций (обновления сертификата и т. п.) производить не требуется.

Запрос информации о ключе

Запрос параметров личного ключа производится по следующей команде:[1]

```
certutil -getkey –v SearchToken RecoveryBlobOutFile
```

В этой строке `SearchToken` означает любой возможный критерий идентификации сертификата. В качестве таковых могут быть использованы название сертификата или его номер (эти параметры легко скопировать из списка выданных сертификатов), а также имя учетной записи пользователя в виде domain\user или user@domain.

Параметр `RecoveryBlobOutFile` определяет имя файла, в который утилита запишет данные по восстанавливаемому ключу.

Восстановление ключа из зашифрованного файла

Восстановление личного ключа выполняется следующей командой:

```
certutil -recoverkey -pPassword RecoveryBlobInFile PFXOutFile
```

В этой команде `RecoveryBlobInFile` — название файла, в котором хранится зашифрованная информация (это тот самый файл `RecoveryBlobOutFile`, который был получен на предыдущем шаге). `PFXOutFile` — имя файла, в который будут записаны данные ключа. Файл создается в формате PKCS #12. С этим

[1] Утилита входит в состав операционной системы. Мы не приводим полного списка ключей этой команды. Пользователь легко сможет ознакомиться с соответствующим описанием.

типом файлов ассоциирован мастер импорта сертификатов, так что для установки восстановленного ключа достаточно будет выбрать данный файл.

В качестве `Password` вы должны указать тот пароль, которым будет зашифрован pfx-файл. Поскольку этот файл содержит личный ключ пользователя и, возможно, вам придется передавать его по каналам связи, в данной операции следует обязательно включать парольную защиту.

Электронная подпись

"*Электронная цифровая подпись* — реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе", — гласит уже упомянутый Закон РФ "Об электронной цифровой подписи".

С технической точки зрения, *электронная подпись* — это цифровой блок, который добавляется к электронному документу и подтверждает целостность (неизменность после момента подписания) документа и его авторство. Иными словами, когда мы ставим электронную подпись, программа добавляет к документу определенное количество символов. В них содержатся данные о том, кто подписал документ, и присутствует контрольная информация о документе и авторе.

Как происходит формирование электронной подписи? Сначала с помощью специальных функций, называемых *хэш-функциями*, на основе содержимого документа формируется фиксированная последовательность символов. Независимо от объема документа эта последовательность всегда имеет один размер. Особенность хэш-функций состоит в том, что изменение даже одной буквы в документе приводит к существенному изменению получаемой последовательности. Причем хэш-функции созданы так, что восстановить документ по контрольной последовательности невозможно: изменили документ — изменилась контрольная последовательность.

После получения контрольной последовательности она шифруется с помощью закрытого ключа пользователя. Расшифровать такой контрольный блок может любой пользователь, поскольку открытый ключ шифрования автора документа доступен всем.

Чтобы проверить целостность документа и его авторство, другому пользователю достаточно повторить описанные операции. Если контрольная последовательность, полученная пользователем, совпадает с последовательностью,

зашифрованной в электронной подписи, то, значит, документ не изменен и его авторство[1] подтверждается.

Если кто-то захочет изменить документ, то для новой редакции будет сформирована совершенно иная хэш-последовательность. Злоумышленник не сможет заменить эту последовательность в электронной подписи, поскольку он не сможет зашифровать ее с помощью чужого сертификата. Злоумышленник может только использовать свой сертификат, но тогда в электронной подписи появятся иные данные об авторе документа.

Как видно из описанной технологии, доверие к электронной подписи определяется двумя факторами: стойкость использованного метода шифрования и доверие к цифровому сертификату пользователя, поскольку именно сертификат устанавливает принадлежность открытого ключа данному конкретному пользователю.

Шифрование документов

Шифрование документов имеет некоторые особенности. Поскольку операции с симметричным ключом выполняются существенно быстрее, то сам документ шифруется с помощью случайного симметричного ключа, после чего этот ключ шифруется личным ключом пользователя на открытом ключе того человека, которому предполагается передать документ на ознакомление. В результате "медленные" операции (шифрование на основе двух ключей) выполняются только над малым объемом данных, что повышает скорость выполнения операций.

Электронная подпись документа MS Office

В версии Word 2003[2] предусмотрена возможность электронного подписания документа. Для этого необходимо в меню **Сервис** выбрать команду **Параметры**, на вкладке **Безопасность** нажать кнопку **Цифровые подписи**, после чего выбрать тот сертификат, который будет использован при подписании документа.

Данный вариант электронной подписи не является сертифицированным, поэтому такая электронная подпись не может признаваться официально. В то же время организации могут внутренними распорядительными документами "признать" ее правомочность (рис. 12.4).

---

[1] Возможность расшифровки с помощью открытого ключа пользователя одновременно свидетельствует об его авторстве.

[2] В офисе 2007 документ подписывается через вставку строки подписи (меню **Вставка** | опция **Строка подписи** в блоке **Текст**).

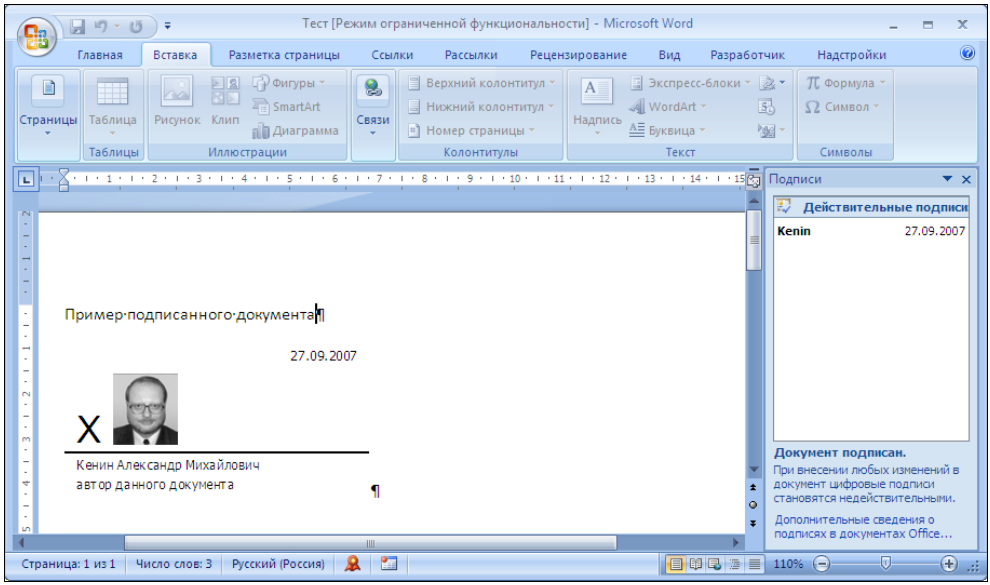


Рис. 12.4. Подпись в документе программы Microsoft Word 2007

Для использования при создании подписи к документу программа позволяет выбрать любой сертификат пользователя, даже не предназначенный для подобной операции, в том числе и вариант автоподписи (сертификат, выданный самому себе).

Возможность подписания сообщения электронной почты существует (для программ из пакета MS Office), начиная с версии Outlook 98. Для создания подписи необходимо иметь соответствующий сертификат, выданный одним из удостоверяющих центров. Для внутренней переписки можно использовать сертификаты удостоверяющего центра предприятия, для внешней почты — только сертификаты доверенных удостоверяющих центров.

Настройка опций безопасности сообщений в MS Office 2003 осуществляется через опции меню **Сервис | Параметры |** вкладка **Безопасность**. Нажав кнопку **Параметры**, следует выбрать подходящий сертификат и установить параметры безопасности для сообщений по умолчанию.

Электронные подписи программных кодов

Электронные подписи на основе открытого ключа стали активно использоваться и для подтверждения авторства программных продуктов. Была создана технология, которая позволила добавлять к программным кодам электронные подписи. Эти подписи формируются по тем же принципам, что описаны выше.

При установке такого программного продукта система проверяет верность электронной подписи. Если код кем-то изменен, то система обнаружит нарушение подписи.

Такая проверка применяется с версии Windows 2000 для программ, которые оказывают влияние на стабильность работы системы. Это, прежде всего, драйверы оборудования и системные файлы. Такие продукты должны содержать электронную подпись фирмы Microsoft. Новые драйверы тестируются в лабораториях корпорации и при отсутствии обнаруженных ошибок снабжаются электронными подписями. Программа установки проверяет наличие подписи. В случае ее отсутствия (фирма-разработчик не передавала драйвер на тестирование) обычно выдается запрос, предупреждающий об отсутствии тестирования. Пользователь, желающий установить драйвер, должен понимать определенную опасность такого шага и может согласиться с риском, возникающим при установке данного программного обеспечения. Политика организации относительно возможности установки программного обеспечения, не содержащего цифровой подписи, определяется администратором системы. Соответствующие возможности следует определить в групповой политике: блокировать установку или запрашивать согласие. Вариант игнорирования и автоматической установки не рекомендуется выбирать по причинам безопасности.

Технология подписания программных кодов используется при загрузке и автоматической установке программных модулей Internet Explorer. Современные обозреватели Интернета позволяют автоматически подключать дополнительное программное обеспечение, которое разработчики сайтов создали для повышения привлекательности своей информации. Это так называемые ActiveX, Java-апплеты и т. п. Понятно, что в этой операции таится большой риск приобретения дополнительных, скрытых от вас функций: какие еще операции будет выполнять на вашем компьютере программа, созданная неизвестными программистами? Поэтому модули стали снабжать электронной подписью их изготовителя.

Однако ситуация с электронной подписью таких модулей в корне отлична от подписания драйверов для системы. Если драйверы подписываются только фирмой Microsoft — разработчиком самой операционной системы, то загружаемые из Интернета модули ActiveX могут быть разработаны и подписаны любым пользователем. Иными словами, электронная подпись подтверждает только то, что данный модуль изготовлен неким (часто никому неизвестным) автором. При получении запроса на установку такого модуля следует внимательно ознакомиться с сертификатом. Принимать предложения на установку программ следует только от надежных источников, как бы ни напоминала сама программа о такой необходимости.

Пользователь имеет возможность в любой момент пересмотреть ранее принятые решения и, например, удалить установленные из Интернета модули или отказать в доверии тем фирмам, для которых было принято решение о доверии не программе, а изготовителю. Чтобы отказаться от доверия к фирмам-изготовителям ПО для страниц Интернета, следует в программе Свойства обозревателя через вкладку **Содержание** открыть окно **Сертификаты**. В этом окне на вкладке **Доверенные издатели** будет отображен список тех организаций, для которых при установке их программ был поставлен флажок **Всегда доверять содержимому, полученному от...**. Вам нужно отключить эту опцию.

Создание подписей к макросам MS Office

Достаточно легко можно поставить электронную подпись для файлов проектов (макросов) MS Office. Для этого следует установить соответствующий модуль дистрибутива данного пакета и получить сертификат, предназначенный для подписания кодов.

Примечание

Начиная с MS Office 2003, в программу включена возможность подписания собственных кодов *без получения специального сертификата*. Такие проекты могут быть использованы только самим пользователем.

Для подписания кода нужно открыть редактор Visual Basic, вызвать команду создания электронной подписи, выбрать нужный сертификат и сохранить проект. Такой проект будет исполняться и при установке высокого уровня безопасности, если соответствующему сертификату установлено необходимое доверие.

Создание подписей к файлам сценариев

Электронные подписи могут быть созданы и для файлов сценариев. Это позволяет повысить уровень безопасности сети, разрешив исполнение во всей организации только подписанных кодов.

При создании электронной подписи сценария и при ее проверке применяются те же процедуры, что и в случае использования других программных кодов с цифровой подписью. Для исполняемого кода вычисляется хэш, который шифруется с помощью закрытого ключа пользователя. При запуске кода программа вычисляет хэш заново и сравнивает его с дешифрованным хэшем файла. В случае возможности расшифровки и совпадения хэшей электронная подпись считается действительной.

Для подписания сценариев используется специальный объект (из Windows Scripting Host v.5.6) — `Signer` и его метод создания подписи `SignFile`:

```
Set Signer = CreateObject("Scripting.Signer")
Signer.SignFile "имя файла", "имя сертификата", "имя хранилища сертификатов"
```

Имя хранилища сертификатов можно опустить. В этом случае будут использованы значения по умолчанию для текущего пользователя. Если в системе отсутствует установленный сертификат[1], предназначенный для подписания программных кодов, то метод не будет выполнен (сообщит об ошибке).

При удачной операции создания электронной подписи к концу файла сценария будет добавлен специальный блок вида:

```
'' SIG '' Begin signature block
'' SIG '' MIID0AYJKoZIhvcNAQcCoIIDwTCCA70CAQExDjAMBggq
...
'' SIG '' 9KijgIITdlynkXo/5ff0Y5LE+zklRgY=
'' SIG '' End signature block
```

Настройка уровня безопасности при работе с файлами сценариев устанавливается через групповую политику. Фактически при этом задается следующий параметр:

```
HKCU\SOFTWARE\Microsoft\Windows Script Host\Settings\TrustPolicy
```

Если значение этого параметра (тип его `REG_DWORD`) равно 0, то разрешается запуск всех сценариев, если равно 1 — пользователь запрашивается в случае наличия электронной подписи центра сертификации, к которому не установлено доверие; неподписанные сценарии не запускаются. При значении параметра, равном 2, система выполняет *только сценарии, подписанные с помощью сертификатов доверенных центров*.

Pretty Good Privacy

Технология Pretty Good Privacy (PGP) была разработана в начале 1990-х годов Филом Циммерманом (Phil Zimmerman). PGP быстро завоевала популярность пользователей. Впервые разработчики использовали профессиональные алгоритмы шифрования данных и предоставили исходные коды программ для всеобщего ознакомления. Любой пользователь мог самостоятельно проанализировать все алгоритмы, убедиться в отсутствии "запасных входов" и откомпилировать исполняемые файлы. Причем PGP-программы обеспечивали во много раз более высокий уровень защиты данных, чем коммерческие утилиты, поскольку в то время действовали экспортные ограничения на продукты, использующие криптографические алгоритмы.

---

[1] В практике автора метод не позволял сформировать электронную подпись, если имя сертификата содержало символы кириллицы.

PGP-клиент первоначально распространялся на свободной основе, коммерческими были отдельные продукты, предоставляющие дополнительный сервис пользователю. С 1997 года права на коммерческое распространение технологии приобрела корпорация Network Associates. Технология была включена в продукты компании McAfee.com, принадлежащей Network Associates. Однако коммерческие акции не имели поддержки в Сети, и компания в 2002 году продала технологию PGP фирме PGP Corp.

Поддержка OpenPGP включена во многие продукты, в том числе такие, как популярная почтовая программа The Bat!, применяемая многими российскими пользователями. Существуют и бесплатные почтовые серверы, которые позволяют пересылать зашифрованные письма с использованием данной технологии.

Защищенные каналы связи

В компьютерных сетях обычно используются незащищенные каналы передачи информации. Это значит, что обладающий некоторым опытом и имеющий доступ к сети передачи данных злоумышленник может прочесть сведения, передаваемые между компьютерами. Немного потрудившись, злоумышленник способен "вмешаться" в работу и "на ходу" подменить часть данных своими значениями.

Для предупреждения подобных инцидентов на практике используют различные способы организации защищенных каналов связи.

Secure Sockets Layer

Протокол SSL (Secure Sockets Layer) разработан фирмой Netscape Communications Corporation для обеспечения безопасной передачи конфиденциальной информации по открытым каналам связи. Протокол во многом был оптимизирован для использования при передаче данных между серверами Интернета. В дальнейшем при активном участии других организаций была создана следующая версия данного протокола (SSL 3.0), которая стала фактическим стандартом в области защиты данных Web-серверов и клиентов (обозревателей) в Интернете.

SSL — протокол "уровня приложения". Это означает, что для использования SSL прикладная программа должна быть соответствующим образом спроектирована. Программа должна "уметь" создавать защищенное соединение и передавать по нему данные.

В программах просмотра Интернета поддержка SSL реализована по умолчанию. На практике находят применение различные версии протокола SSL:

TLS (Transport Layer Security), который часто называют SSL 3.1; WTLS (Wireless TLS), используемый при передаче данных на мобильные телефоны и пейджеры, и т. п.

Протокол SSL обеспечивает аутентификацию как сервера, так и клиента (опционально) перед началом обмена конфиденциальными данными, а у информационного сервера требует обязательного наличия цифрового сертификата.

Что гарантирует SSL? Во-первых, при создании защищенного канала связи происходит аутентификация сервера. То есть вы убеждаетесь, что будете передавать свои данные не кому-либо, а конкретному лицу, личность которого подтверждается имеющимся у него цифровым сертификатом. Во-вторых, после создания защищенного канала данные по нему будут передаваться в зашифрованном виде, что исключает их перехват посторонним лицом. При этом могут применяться различные методы шифрования, требуемые для обеспечения конфиденциальности. Соответствующий выбор определяется программным обеспечением, которое создает защищенный канал связи.

Secure Channel

Защищенным каналом называют совокупность протоколов передачи данных (Transport Layer Security (TLS), Secure Sockets Layer (SSL), Private Communications Technology (PCT)), которые обеспечивают аутентификацию клиента и сервера и безопасную зашифрованную передачу данных.

Защищенный канал используется при передаче данных в Интернете. Запрос клиента по защищенному каналу обычно оформляется с префиксом HTTPS, например **https://www.example.com/**.

Проверка защищенного канала связи

Бывают случаи, когда клиент не может осуществить соединение по защищенному каналу связи. Обычно это связано с ошибками в конфигурации сетевых устройств или блокировке пакетов на различных брандмауэрах.

Проверить, "виноват" ли в отсутствии связи канал передачи данных или есть проблемы в программном обеспечении сервера, можно, выполнив несколько простых операций.

Проверим сначала наличие ответа сервера, с которым требуется установить защищенный канал связи, по порту, используемому для его организации (по умолчанию 443). После набора такой команды:

```
telnet <имя_сервера> 443
```

должен появиться пустой экран с мигающим курсором. Это свидетельствует, что сервер ожидает получения данных. Если нажать любую клавишу (или

подождать несколько секунд), то сессия будет разорвана и на экране появится надпись:

```
Connection to host lost.
```

Если сессия создается, а работа по защищенному каналу связи невозможна, то следует выяснить причины у разработчика программного обеспечения, которое применяется на данном информационном сервере.

Если соединиться с сервером не удается, то нужно проверить все узлы, через которые проходит соединение. Эту цепочку можно вычислить с помощью утилиты `tracert`:

```
tracert <имя_сервера>
```

На экране должна появиться информация, аналогичная нижеприведенной:

```
tracert www.microsoft.com -d
1 20 ms 10 ms 10 ms 24.25.66.1
2 20 ms 10 ms 10 ms 24.93.65.149
3 39 ms 10 ms 23 ms 24.93.66.145
4 10 ms 10 ms 10 ms 24.93.66.178
5 20 ms 20 ms 20 ms 64.240.245.81
6 20 ms 20 ms 20 ms 208.30.202.5
7 20 ms 20 ms 20 ms 144.232.8.229
8 40 ms 30 ms 30 ms 144.232.18.33
9 40 ms 30 ms 40 ms 144.232.26.1
10 40 ms 30 ms 30 ms 144.232.26.6
11 80 ms 71 ms 70 ms 144.232.18.49
12 70 ms 70 ms 70 ms 144.232.6.89
```

Теперь нужно проверить каждый узел описанным выше способом, чтобы найти ту точку, которая не пропускает данные. При попытке организовать канал с таким узлом будет сообщаться следующая информация:

```
Could not open a connection to host on port 443: Connect failed
```

При получении подобного ответа следует выяснить причины таких настроек у администратора соответствующей системы. Обычно это связано с не вполне корректной настройкой фильтрации пакетов на брандмауэре.

Internet Protocol security

Использовать описанные выше протоколы защищенной передачи данных может только программа, которая умеет самостоятельно создавать такой защищенный канал и передавать по нему данные. Начиная с Windows 2000, в операционную систему встроена возможность создания защищенных каналов связи на уровне транспортных протоколов. Это означает, что защищенный канал создается средствами операционной системы, а прикладная программа

использует его, даже не подозревая о наличии защиты. При таком подходе защищенным способом могут передаваться данные любой, а не только специально спроектированной программы. Достаточно только предварительно настроить соответствующее подключение.

Создание такого защищенного канала передачи данных описывается целым набором стандартов, политик и протоколов, объединяемых названием Internet Protocol security (IPSec). Использование IPSec позволяет быть уверенным в том, что данные передаются именно между этими компьютерами (компьютеры аутентифицируются перед передачей данных), что данные целостны (в них не внесены изменения) и недоступны злоумышленнику (зашифрованы). Как уже говорилось, использовать IPSec может любая программа (любой протокол IP), никаких дополнительных функций от прикладного программного обеспечения не требуется.

Примечание

Шифрование данных в IPSec, используя ресурсы процессора, неизбежно сказывается на суммарной производительности системы (по некоторым оценкам до 10%). Поэтому включение IPSec целесообразно только на участках с повышенными требованиями к защите и целостности данных.

Следует отметить, что, как и другие методы обеспечения безопасности, IPSec не является панацеей и не может защитить, например, от сетевых атак, от других действий злоумышленников, если они используют разрешенные IPSec способы "общения".

Настройка IPSec требует от администратора компьютерной сети выполнения ряда операций. Перед тем как включать IPSec, необходимо задать правила, которые будут использованы при передаче данных с его использованием. Эти правила объединены в *политику IPSec*.

По умолчанию в системе присутствуют три политики: *клиента*, *сервера* и *защищенного сервера* (рис. 12.5). Вы можете применять эти политики, но предпочтительнее настроить собственные правила, которые, например, снизят нагрузку на сервер, поскольку будут требовать шифрования только конкретных данных, а не всего потока.

Для создания собственной политики откройте локальную[1] политику безопасности, выберите раздел **Политики безопасности IP** и в его меню отметьте пункт создания новой политики. В результате выполненных действий запустится мастер политики IP-безопасности. После ввода названия следует определить, будет ли использовано правило по умолчанию при запросе безопас-

[1] Для определения политик IPSec в рамках предприятия необходимо задавать соответствующие параметры в групповых политиках домена и подразделения.

ного соединения. Обычно следует согласиться. Далее необходимо определить способ, которым будет проводиться аутентификация компьютеров. При работе в составе домена обычно используют его способ проверки безопасности — Kerberos. Вариант сертификатов выбирают тогда, когда есть сложности с аутентификацией по Kerberos (например, установление связи не с компьютером домена), но имеется возможность установить специальный сертификат[1]. При настройке указывают только тот центр сертификации, чьими сертификатами будет пользоваться программа. Это безопасный способ проверки, но требует предварительного обмена сертификатами. И наконец, можно определить некоторый пароль, который должен быть введен на каждом компьютере при настройке IPSec. Способ самый быстрый, но и самый небезопасный.

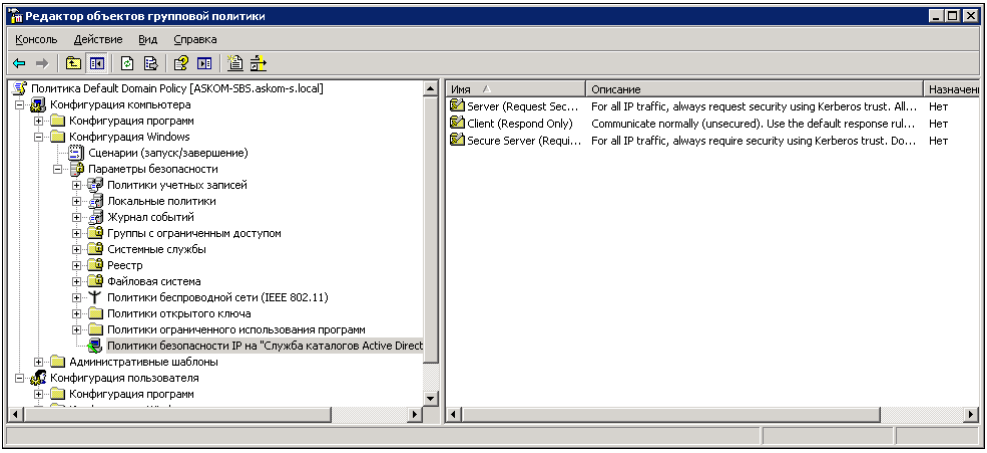


Рис. 12.5. Политики IPSec по умолчанию представлены в групповой политике по умолчанию, но не назначены для применения

На этом мастер завершает работу, создав правило с единственным параметром — правилом для установки соединений по умолчанию.

Теперь необходимо добавить в созданную политику те правила, которые будут описывать конкретные требования. Для этого в свойствах политики на вкладке **Правила** выбирается кнопка **Добавить**. Первым запросом мастера будет выбор необходимости создания *туннеля* IPSec.

Туннель IPSec создается в случае необходимости пересылки данных между двумя компьютерами, разделенными маршрутизаторами, в случаях, если, например, предполагается передавать данные через сеть Интернет. В этом слу-

[1] Необходимо использовать сертификат только соответствующего шаблона, предназначенного для IPSec.

чае описываются параметры начала и конца туннеля, тогда как в открытой сети такая информация передается прозрачно для промежуточных систем[1].

Если IPSec предполагается применять в локальной сети при связи со всеми компьютерами, то следует выбрать опцию **Это правило не определяет туннель.**

Следующим шагом можно выбрать типы подключений, к которым будет применено правило: все, или только локальные, или удаленные. Далее мастер покажет окно, в котором и нужно задать желаемые правила путем добавления или редактирования *фильтров*. По умолчанию предлагается только два фильтра — для всего трафика и для трафика ICMP (пакеты ping и т. п.). Обычно на этом этапе следует создать собственный фильтр, который будет описывать желаемые требования.

Примечание

Если фильтр создается для *передачи* данных, то обычно аналогичный фильтр (с "зеркальными" настройками) нужно создать для входящих соединений. Поэтому мастер создания фильтров предлагает создавать такие "пары" сразу (опция **Отраженный**).

В качестве источника пакетов можно указать различные варианты: адрес данного компьютера (мой IP-адрес), все адреса, DNS-имя, другой IP-адрес или целую подсеть, использовать динамические сведения (адреса WINS, DHCP, DNS и т. п. серверов, имена которых могут меняться). После выбора адреса назначения предлагается определить тип протокола, для которого будет применяться правило, а затем задать конкретные параметры выбранного протокола. Например, для TCP или UDP можно указать используемые порты.

Примечание

Выбор протоколов и их параметры (при наличии) целиком определяются решаемой задачей.

После завершения работы мастера и создания фильтра вы можете запустить мастер снова и добавить второй, третий и т. д. фильтры, которые в комплексе будут описывать конкретные параметры IPSec. Затем можно продолжить работу мастера правил безопасности.

На следующем шаге мастера правил безопасности необходимо выбрать, какой вариант обработки будет применен. По умолчанию предлагается три варианта: запросить безопасность, разрешить небезопасные и требуется безопасность. Можно создать собственные правила, но они будут принципиально

[1] Возможность пропуска пакетов IPSec через серверы с трансляцией адресов (NAT) имеется только с версий для Windows 2003 Server и Windows XP SP1.

отличаться от этого перечня только применяемыми методами шифрования данных и проверки их целостности. При отсутствии специальных требований следует согласиться с одним из предложений по умолчанию.

Определив метод аутентификации, вы завершите работу мастера.

Для ввода в действие созданных правил соответствующую политику безопасности нужно *применить*. Для этого достаточно выбрать соответствующее меню ее свойств.

Исключения IPSec

Реализация IPSec предусматривает наличие разрешений[1] на передачу следующих типов информации.

- **Широковещательный трафик.**

  Пропускаются пакеты на широковещательный адрес подсети и на диапазон адресов с 224.0.0.0 по 239.255.255.255[2].

- **Resource Reservation Protocol (RSVP).**

  Протокол используется для настройки приоритетов TCP/IP-трафика в сети (Quality Of Service — QoS, использует TCP порт 46).

- **Internet Key Exchange (IKE).**

  Протокол применяется для согласования параметров защищенного трафика (использует UDP порт 500).

- **Kerberos.**

  Протокол служит для аутентификации в IPSec (TCP и UDP порты 88).

Поскольку эти разрешения могут быть использованы для сетевых атак, то, начиная с версии Windows 2000 SP1, предусмотрена возможность их отключения. Для этого необходимо добавить в ветку реестра системы `HKLM\SYSTEM\CurrentControlSet\Services\IPSEC` параметр `NoDefaultExempt` типа `REG_DWORD`. Возможные значения зависят от операционной системы: для Windows 2000 и Windows XP возможны только 0 или 1 (по умолчанию 0), для Windows Server 2003 — от 0 до 3 (по умолчанию 3). Допустимые значения данного параметра и соответствующие им уровни разрешений приведены в табл. 12.1.

Примечание

Начиная с Windows 2000 SP4 и Windows XP SP2, по умолчанию разрешения отключены (значение параметра `NoDefaultExempt` равно 1).

---

[1] Перечисленные пакеты пропускаются, даже если администратор не указал разрешения для них явным образом в примененной политике.

[2] Broadcast- и multicast-трафик.

Таблица 12.1. *Значения параметра* `NoDefaultExempt`

Значение	Описание
0	Перечисленные выше протоколы исключаются из фильтрования IPSec
1	Из фильтрования исключаются широковещательные протоколы и IKE; Kerberos и RSVP включены
2	RSVP, Kerberos и IKE исключены из фильтрации; широковещательный трафик фильтруется
3	Из фильтрации исключается *только* трафик IKE

Если администратор решит защитить контроллеры домена с помощью IPSec, то следует явно разрешить пропуск трафика Kerberos и UDP 389 со всех контроллеров домена. Понятно, что распространять такие требования удобно только с помощью групповой политики.

IPSec при загрузке системы

Поскольку IPSec является одной из служб системы, то политика безопасности начинает применяться только после запуска данной службы. В результате в течение некоторого периода времени после включения компьютера фильтрация трафика не обеспечивается. В связи с этим в последних версиях операционных систем предусмотрен специальный режим (stateful filtering) IPSec, действующий во время загрузки компьютера. В этом режиме по умолчанию блокируется весь входящий трафик; исходящий трафик разрешается; пропускаются пакеты, направленные в ответ на исходящие пакеты, а также трафик DHCP. Администратор может, используя статические фильтры, настроить иной режим, используемый при загрузке системы.

Примечание

Настройка этого режима может быть выполнена только с помощью команды `netsh`.

Выбор режима, используемого при старте системы, производится командой:

```
netsh ipsec dynamic set config <bootmode>
```

Возможные варианты — `stateful`, `block`, `permit`. Кроме того, можно использовать исключения режимов при помощи команды

```
netsh ipsec dynamic set config <bootexemptions>
```

При этом исключения должны представлять собой список протоколов и портов: `Protocol:SrcPort:DstPort:Direction`

Фильтрация пакетов средствами IPSec

Рассмотрим некоторые рекомендации применения фильтрации с помощью политик IPSec.

Во-первых, необходимо определить методы, используемые при аутентификации компьютеров, передающих данные.

Во-вторых, нужно выбрать правильную политику защищенного соединения. По умолчанию в системе представлены три политики защищенного IP-соединения. Это *клиент* (используется нешифрованное соединение во всех случаях, когда другой участник не запросил иного), *сервер* (защищенное соединение запрашивается, но, если клиент не может его поддерживать, передача данных осуществляется в открытом режиме) и *защищенный сервер* (данные передаются только в защищенном режиме; если клиент не может установить такое соединение, связь рвется). Ни одна из этих политик не активизирована по умолчанию.

IPSec поддерживается в операционных системах только начиная с Windows 2000. Если для каких-либо компьютеров применена политика передачи данных, *требующая* установления защищенного канала IPSec, то взаимодействовать с такими компьютерами системы на основе Windows 9*x*/ME/NT 4.0 не смогут.

Администратору системы необходимо определить, какие протоколы будут использовать защищенное соединение, в каких случаях его необходимо применять обязательно, а в каких — только запрашивать, но продолжать соединение в случае отсутствия у клиента возможности поддерживать шифрование и т. п. Эта настройка выполняется созданием фильтров, вариантов действий по ним и внедрением собственной политики IPSec.

В общем случае настройка IPSec является достаточно ответственной операцией и требует от администратора определенного уровня знаний сетевых протоколов. Кроме того, при настройке IPSec с удаленными компьютерами следует убедиться в отсутствии фильтрации трафика IPSec (брандмауэров) на хостах, обеспечивающих передачу пакетов информации.

Тестирование IPSec

Для наблюдения за работой IPSec и его настройками могут быть использованы различные методы. Например, существует утилита `netdiag`, входящая в состав средств Support Tools, которые могут быть добавлены с установочного компакт-диска операционной системы. Команда

```
netdiag /test:ipsec
```

позволяет увидеть активные политики IPSec на компьютере. Так, если ни одна политика не активна, то будет получено сообщение:

```
IP Security test . . . . . : Passed IPSec policy service is active, but
no policy is assigned
```

С ключом `/debug` эта команда выводит на экран подробную информацию.

Для управления IPSec в Windows 2000 может использоваться утилита `ipsecpol`, которую необходимо установить из пакета Resource Kit (свободно доступна для загрузки).

Еще одна утилита — Ipsec Monitor (оснастка консоли управления). Она позволяет отобразить используемые на компьютере политики IPSec, фильтры, статистику IPSec.

В Windows XP/2003 основным средством управления IPSec становится команда `netsh`. С помощью этой утилиты можно как исполнять заранее подготовленные сценарии, так и менять конфигурацию в интерактивном режиме. Утилита позволяет осуществить настройку любых параметров сетевых соединений.

Программа `netsh` позволяет добавлять динамические и статические фильтры. Статические фильтры сохраняются после перезагрузки системы. Динамическая фильтрация осуществляется только на некоторый период (либо до явной ее отмены с помощью соответствующей команды, либо до момента перезагрузки системы). Обычно динамическая фильтрация используется на практике в случаях установки каких-либо обновлений, тестирования решений и т. п.

Рекомендации по использованию IPSec

Применять IPSec следует осознанно, учитывая, что такие операции, как шифрование трафика и т. п., увеличивают нагрузку на процессор. Не следует защищать IPSec весь трафик локальной сети, тем более ограничивать какими-либо политиками трафик между членами домена и контроллерами[1]. При использовании IPSec для мобильных клиентов нужно учитывать, что перемещение клиента между точками доступа будет приводить к блокированию трафика.

Необходимо учитывать, что для защиты данных клиентов удаленного подключения надо использовать не каналы IPSec, а создание виртуальных частных сетей VPN.

Служба управления правами (RMS)

Для Windows 2003 Server разработана *служба управления правами* (Windows Rights Management Services, RMS), с помощью которой можно ограничивать

[1] Это связано с тем, что в данном процессе используются различные протоколы. Применение политики при наличии только "общего понимания" может привести к проблемам в функционировании систем.

права пользователей по распространению документов MS Office 2003. Служба предназначена для предотвращения обычным пользователем несанкционированного распространения (печати на принтер, копирования на жесткий диск, рассылки по электронной почте, копирования через буфер и т. п.) документов MS Office 2003.

Примечание

Служба RMS должна приобретаться *дополнительно* к серверу Windows 2003 и клиентским лицензиям доступа к нему (на момент подготовки книги стоимость одной лицензии RMS составляла $37).

Принципы работы службы управления правами

Для реализации данной службы используется шифрование документов. Шифрование производится обычным способом: содержание документа шифруется при помощи случайного симметричного ключа, который, в свою очередь, шифруется открытым ключом сервера RMS. Полученный файл дополняется данными о назначении прав и сохраняется. Раскодировать такой файл можно только закрытым ключом сервера RMS.

При попытке доступа к документу, защищенному с использованием данной технологии, производится обращение к серверу RMS, который проверяет аутентификацию пользователя. Если пользователю предоставлено право работы с документом, сервер RMS дешифрует симметричный ключ, которым зашифрован документ, и вновь шифрует его открытым ключом пользователя из сертификата[1], выданного сервером RMS. Получив эти данные, пользователь дешифрует симметричный ключ и в итоге получает доступ к документу. Также вместе с ключом сообщаются данные о правах доступа, которые используются программой клиента для контроля работы над документом. При необходимости автономной работы эти данные могут быть сохранены в самом файле документа, что позволит осуществлять работу с ним при временном отсутствии подключения к серверу RMS.

Примечание

Назначать права доступа можно не только сотрудникам организации, но и внешним клиентам. Для этого необходимо приобретение специальной лицензии для внешнего доступа к серверу RMS и обязательная регистрация такого клиента в службе каталогов данного предприятия или в службе, которой установлено доверие на сервере RMS (например, Microsoft Passport или продукты третьих фирм).

[1] Если пользователь открывает документ на различных компьютерах, то ему выдаются различные сертификаты (поскольку они содержат данные лицензии компьютера), но имеющие одинаковые пары закрытый/открытый ключ.

Установка сервера RMS

Дистрибутив сервера RMS может быть загружен с сайта изготовителя. Для его функционирования необходимо наличие сервера баз данных (MS SQL Server 2000 с SP3).

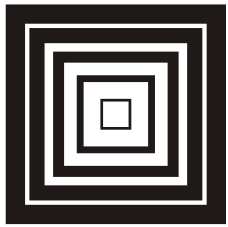
Клиентское программное обеспечение также распространяется с сайта разработчика (планируется, что оно войдет в новую версию операционной системы). После его установки клиентская часть должна получить лицензию (lockbox), а затем на компьютер будет автоматически установлен сертификат RMS. В настоящее время программами, которые могут использовать технологию RMS, являются компоненты MS Office 2003. Кроме того, с сайта разработчика можно загрузить дополнительный модуль к MS Internet Explorer, который позволяет открывать документы, защищенные RMS, в режиме *только для чтения*.

При настройке параметров сервера RMS администратор имеет такие возможности, как задать группу пользователей, которые *всегда* будут иметь доступ к документам, определить параметры для автономной работы с документами (разрешить или нет) и т. п. Самое главное, что в RMS можно создать шаблоны политик прав доступа, которые могут использоваться авторами при назначении комплекта прав на документ.

Ограничения RMS

Хотя RMS позволяет ограничить пользователя в распространении полученного документа, данная технология не обеспечивает, строго говоря, полную безопасность документа. Например, стандартные средства копирования экрана при работе с документом RMS отключены, но если у пользователя установлены программы-"грабберы" третьих фирм, то он может получить копию документа. Конечно, можно зафиксировать перечень запускаемых на компьютере программ, но в итоге окажется проще использовать стандартный комплекс защиты конфиденциальной информации, чем настраивать подобную систему.

Иными словами, RMS имеет, прежде всего, психологическое воздействие на пользователя, показывая ему, что данный документ по правилам организации не может быть скопирован и передан другому лицу.



ГЛАВА 13

Средства управления системами

Деятельность по управлению компьютерной информационной системой нуждается в инструментах, которые помогут администратору выполнять многие рутинные операции. В текущей работе администратору информационной системы обычно нужно:

- ❒ знать состав информационной системы;
- ❒ контролировать состояние функционирования отдельных ее компонентов;
- ❒ иметь централизованные средства управления.

Инвентаризация

Если у администратора нет полной инвентаризации — начиная от расположения кабелей, назначения портов коммутационных панелей и заканчивая списком установленного программного обеспечения, то на устранение повреждений, от которых никто не застрахован, может потребоваться длительный промежуток времени, в течение которого предприятие будет нести убытки из-за непредоставления услуг информационной системой. Чем более подробно составлена соответствующая документация, чем тщательнее она поддерживается в актуальном состоянии, тем легче сориентироваться в аварийной ситуации.

Учет компьютеров и программ

Автоматическая инвентаризация программного обеспечения и оборудования для функционирующих систем не представляет большой сложности. Данные о параметрах оборудования и программного обеспечения доступны на программном уровне; их легко собрать централизованно при наличии прав дос-

тупа к соответствующему компьютеру[1] (рис. 13.1). Администратору доступно большое число программ, реализующих данный функционал, поэтому большое значение при выборе инструмента имеют личные предпочтения и, возможно, дополнительные особые требования, такие как необходимость периодической инвентаризации в больших организациях или требования интеграции с бухгалтерскими учетными системами.

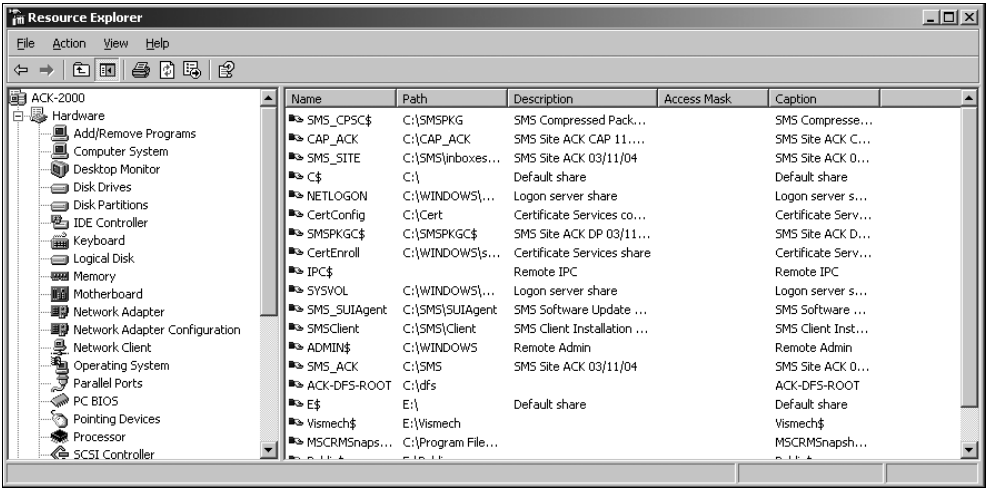


Рис. 13.1. Результаты инвентаризации ресурсов с использованием System Management Server. Собранные данные хранятся в базе, поэтому администратор легко может сформировать необходимый запрос и получить ответ, например, на скольких компьютерах используется данный программный продукт

Построение логической структуры СКС

Для устранения неисправностей СКС необходимо знать, как соединено активное оборудование, к какому порту подключен конкретный компьютер. Подобные сведения также можно собрать автоматически, если СКС построена на *управляемых* коммутаторах.

Для построения подобных схем соединения существуют различные программы. В случае "простых" схем применимы и бесплатные версии. Так, на рис. 3.3 *(см. главу 3)* представлена схема соединений реальной сети, автоматически составленная бесплатной программой 3Com Network Supervisor.

Если сеть разбита на отдельные сегменты (виртуальные сети) и в ней присутствуют резервные каналы связи и т. п., то возможностей бесплатных версий

[1] В домене с этой целью обычно используются учетные записи, включенные в группу администраторов домена. В рабочей группе придется указывать параметры учетных записей каждой системы.

оказывается недостаточно. В этом случае для составления схемы, если она не была составлена прежним администратором, можно воспользоваться триальными версиями программ, впоследствии вручную отслеживая вносимые изменения.

Simple Network Management Protocol

Для получения информации от управляемого коммутатора используется специальный протокол SNMP (Simple Network Management Protocol, простой протокол управления сетью). Устройства[1], которые допускают управление по данному протоколу, могут принимать из сети команды, выполнять их и передавать информацию о параметрах своей работы. Например, после получения сообщения о прекращении поступления электроэнергии от управляемых аварийных источников программа может запросить данные об уровне зарядки аккумуляторных батарей и отложить отключение компьютеров до момента практически полной разрядки.

Примечание

Существуют различные версии протокола SNMP (в настоящее время — первая, вторая и третья). Многие устройства, уже давно эксплуатируемые в сети, предполагают возможность управления только по версии 1.0. Данная версия не предусматривает никакой защиты, имена сообществ передаются по сети в открытом виде, что легко позволяет перехватить их снифферами. Поэтому обращайте внимание на то, что имена сообществ (community в терминологии SNMP) ни в коем случае не должны сохранять значения по умолчанию, их следует заменить на достаточно длинные и сложные названия. А интерфейсы управления такими устройствами желательно выделить в отдельную виртуальную сеть.

SNMP-управление в первую очередь используется для управления активным сетевым оборудованием: маршрутизаторами и коммутаторами, аварийными источниками питания, модемами и т. п. Например, на рис. 11.1 показана статистика работы устройства, полученная на основе SNMP-запросов.

SNMP-управление отличается относительной простотой реализации. Отправка сообщений выполняется по протоколу UDP. Для каждого устройства[2] есть фиксированный набор команд, заранее известно, какие данные можно получить от устройства и какие команды оно должно выполнить.

Сообщения, которые могут быть запрошены или получены устройством, задаются индивидуально и записываются специальным образом в так называе-

---

[1] Цена управляемых устройств выше неуправляемых конструкций, в связи с чем в малых организациях чаще используют неуправляемое оборудование.

[2] Существуют типовые описания команд для соответствующих классов устройств. Например, есть типовые команды для маршрутизаторов, которые позволяют запрашивать основные сведения об их функционировании и управлять ими независимо от типа конкретного устройства.

мый MIB-файл[1]. Хотя команды в определенной своей части стандартизованы, все же MIB-файлы специфичны для каждого конкретного устройства.

Обработка SNMP-сообщений "вручную" практически нереальна, поэтому для взаимодействия с SNMP-устройствами необходимы специализированные программы. Обычно разработчики оборудования выпускают программы для управления собственными изделиями. Комплексы, которые позволяют управлять разнородными устройствами сетевой инфраструктуры, часто весьма дороги, и позволить себе использовать их могут только крупные организации.

Инвентаризация физических каналов связи

Инвентаризация кабельной инфраструктуры является одной из самых сложных задач при наличии разветвленной сети предприятия. В лучшем случае у администратора есть кабельные журналы, в которых приведен перечень кабелей и списки соединений, выполненных на коммутационных панелях. Часто эти списки не актуальны, а реальные подключения знает только сам администратор.

Существуют специальные программы, ведущие учет рабочих мест, соединительных кабелей и другого оборудования, которые позволяют в случае необходимости быстро вывести всю информацию о пути соединения точки А и точки Б: номер розетки, кабель, номера коммутационных панелей и портов, на которые разделены кабели, и другую информацию. Первоначальный ввод данных в такие программы — размещение на чертежах рабочих мест, коммутационного оборудования, занесение данных о соединении портов и т. п., производится вручную на основании реализованного проекта СКС.

В последнее время производители оборудования СКС начинают предлагать различные решения *автоматизированного* управления кабельной инфраструктурой. Эти решения основаны, как правило, на внедрении дополнительного служебного *(девятого)* проводника в коммутационных шнурах. Коммутационные панели оснащаются дополнительными контактными площадками, специальные модули осуществляют сбор сведений о фактических подключениях и передают их в отдельную систему контроля (решения PatchView компании RiT Technologies, технология Itracks, система iPatch Real Time Infrastructure Management от Systimax и др.). Такой подход позволяет построить схему подключений в автоматическом режиме и, самое главное, отслеживать ее изменения в реальном режиме времени.

Стоимость дополнительных проводников, новых контактных площадок и другого аналогичного оборудования относительно невелика. Данные техно-

[1] Management Information Base. Сообщения получают названия вида: 1.3.46.67.98.

логии могут быть легко внедрены и в существующих проектах. Однако стоимость модулей анализаторов, сервера контроля и собственно самого программного обеспечения пока не позволяют широко использовать подобные средства интеллектуального управления СКС.

Контроль функционирования ПО

В повседневной практике для администратора очень важно своевременно получить информацию о возникновении того или иного сбоя в работе информационной системы. Еще лучше — получить предупреждение заблаговременно.

Один из наиболее просто организуемых вариантов контроля за работоспособностью серверов заключается в централизованном сборе журналов работы различных систем и последующем анализе полученных данных, глубина которого определяется администратором. В зависимости от результатов анализа система может предупреждать администратора о возникающих ошибках, таких как остановка служб. Более "интеллектуальная" обработка предусматривает некую логику обработки событий. Например, попыткой подбора пароля считается *n* ошибочных вводов пароля за короткий промежуток времени.

"Тяжелые" программы управления информационными системами обычно устанавливают на контролируемые системы специальные программы-агенты, которые ведут сбор данных в постоянном режиме (см., например, Microsoft Operation Management Server, описываемый ниже).

ПО управления серверами от вендоров

Несмотря на большое количество утилит, входящих в состав операционной системы и пакетов Resource Kit, администраторы обычно предпочитают иметь в запасе продукты третьих фирм, которые хорошо зарекомендовали себя при разрешении тех или иных проблем. Ранее уже говорилось о некоторых из таких программ:

- ERD Commander;
- программах для сканирования безопасности сети;
- программах анализа сетевого трафика;
- антивирусных корпоративных решениях

и др.

Профессиональные продукты управления большими сетями — HP Open View, Unicenter и др. — обычно недоступны администраторам малых и средних сетей из-за высокой стоимости: их базовые комплекты оцениваются в 20—30 тыс. долларов без стоимости клиентских лицензий. Поэтому в таких

организациях управление сетью строится на использовании отдельных, не интегрированных друг с другом комплектов.

Далее я приведу несколько кратких описаний ряда популярных технологий и продуктов, которые часто используются при управлении компьютерными сетями. Естественно, что каждый системный администратор будет иметь свой взгляд на данные решения и применять только те продукты, оптимально подходящие для конфигурации его парка оборудования[1].

Службы технической поддержки производителей

В помощь пользователям своих программных продуктов и оборудования разработчики обычно создают инфраструктуру служб технической поддержки. Службы технической поддержки создателей наиболее распространенных продуктов, таких как оборудование от Hewlett-Packard, программные решения от Oracle и т. п., предлагают потребителям возможность заключить договоры на обслуживание с различным уровнем сервиса и гарантирующих ту или иную помощь в течение фиксированного периода времени.

Пакеты технической поддержки с высоким уровнем сервиса обычно недоступны для малых организаций, поскольку стоимость таких услуг весьма высока. В то же время имеется возможность заключения договоров на техническую поддержку, которые обещают участие специалистов и какое-то решение вопроса.

Незначительный опыт общения автора с подобными службами местных представительств является, к сожалению, скорее отрицательным. Например, работая в компании, которая являлась сертифицированным партнером одного софтверного гиганта, автор имел возможность использовать обращения в службу поддержки, положенные по данному статусу. Итоги двух обращений, реакция на которые, мягко говоря, была неоперативной и нерезультативной, не вызывают более никакого желания повторить попытки. Возможно, что это объясняется непереломленными традициями отношения нашего сервиса к рядовым пользователям, недостатками формализованной кадровой политики при наборе специалистов в такие организации или еще какими-либо причинами.

Примечание

Подобная ситуация, конечно, не является стандартом. Например, хочу отметить высокий уровень работы с пользователями специалистов службы Hewlett-

[1] Читатель должен понимать, что в объеме одной книги невозможно даже привести перечень всех таких продуктов. Автор пытается показать, прежде всего, спектр таких программ, основываясь на некотором опыте работы с ними.

Packard, Intel, 3Com, весьма инициативно и оперативно решавших проблемы, с которыми автор обращался к их представителям.

Хочется надеяться, что ситуация изменится с развитием служб поддержки, хотя она во многом зависит в том числе и от активности потребителей. Поясню небольшим примером. Автор вынужден был обратиться в одну из служб поддержки по поводу проблем аутентификации пользователей конкретным аппаратным устройством, возникших после обновления операционной системы с Windows 2000 Server на Windows 2003. Ответ от российского представительства не был получен и пришлось обратиться в головную организацию. Буквально через несколько часов автор получил сначала обвинения от российских представителей о неполучении ими такой заявки, а после предъявления SMTP-журналов, подтверждающих прием сообщения почтовым сервером, — извинения и конкретные советы.

Intelligent Platform Management Interface

Достаточно часто у системных администраторов возникает задача получить удаленное управление над сервером. Традиционно используемые методы: подключение к удаленному рабочему столу, программы, аналогичные VNC или R-Admin *(см. разд. "Утилиты удаленного управления компьютером" далее в этой главе)* бессильны в случае зависания операционной системы.

В подобных ситуациях администратору помогут специальные средства управления, которые присутствуют в современных серверных системах. Их возможности описаны в спецификации IPMI (Intelligent Platform Management Interface). Серверы, удовлетворяющие данной спецификации, могут управляться удаленно с независимой консоли. В число действий, доступных администратору, входит:

- удаленное включение, выключение и перезагрузка сервера независимо от состояния операционной системы;
- обновление BIOS;
- просмотр параметров состояния сервера (температура, уровни напряжения, состояние датчиков, установленных на сервере), в том числе получение автоматического оповещения о событиях в работе системы по сети.

Подключение к серверу для удаленного администрирования может быть осуществлено как через последовательный порт (обычно с использованием модема[1]), так и по компьютерной сети. Если вы реализуете удаленное управ-

[1] Использование модема позволяет подключиться к серверу даже в случае полного отказа инфраструктуры. Стоимость же данного решения (модем плюс один внутренний номер на АТС предприятия) весьма невысока.

ление через сеть, то для большей надежности целесообразно выделить такое управление в отдельный независимый сегмент передачи данных. В этом случае рекомендуется устанавливать самое простое (и, как следствие, самое надежное) активное оборудование вплоть до концентраторов на 10 Мбит/сек.

Подсистема удаленного управления не входит в состав всех платформ. В некоторых случаях такая возможность уже встроена в оборудование, в других можно дооснастить сервер специальной платой, реализующей необходимые функции.

В качестве примера на рис. 13.2 представлен интерфейс удаленного управления сервером Sun.

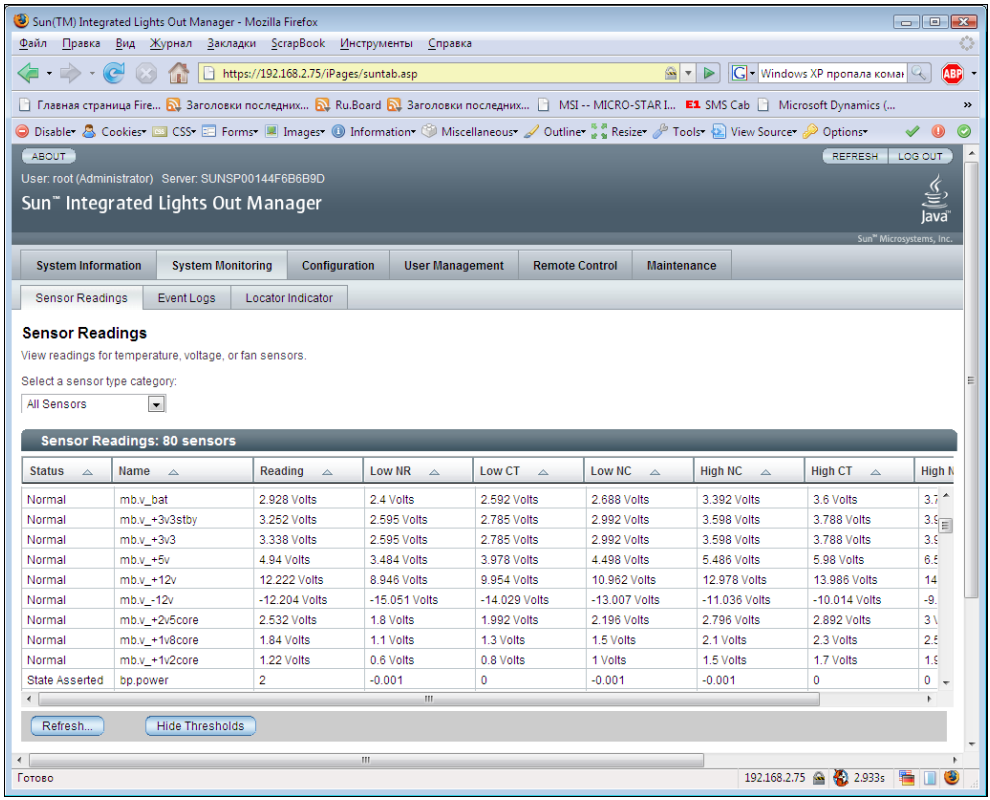


Рис. 13.2. Удаленное управление серверной платформой.

На рисунке представлено одно из окон программы удаленного управления серверной платформой — Integrated Lights Out Manager. Программа представляет собой Java-приложение и позволяет удаленно по безопасному каналу (https) контролировать работу сервера. В число возможностей программы входят мониторинг сенсоров платформы (на рисунке), управление электропитанием (в том числе присутствует функция как корректного выключения с сохранением данных средствами операционной системы, так и простое отключение питания), а также удаленный контроль системы, позволяющий подключить к серверу удаленный CD-ROM, гибкий диск или их образы

Методы управления компьютерной сетью

Если первые версии Windows предполагали управление сетью преимущественно из графического интерфейса, то каждая последующая разработка предлагает все больше возможностей автоматизации работы администратора, прежде всего за счет выполнения команд в режиме командной строки. Практически первой технологией управления Windows в режиме командной строки была утилита KIXART, включенная в состав Resource Kit для Windows 4.0, после чего были добавлены возможности исполнения сценариев Visual Basic, причем в новых версиях резко увеличено число объектов, управлять которыми можно по этой технологии. Недавно была добавлена поддержка технологии Windows Management Interface (WMI, *см. одноименный раздел далее в этой главе*).

В результате администратор сети получил инструментарий, позволяющий управлять практически всеми основными параметрами своих систем.

Windows Scripting Host

С помощью сценариев можно автоматизировать выполнение большинства административных задач управления системой. Сценарии могут быть использованы для подключения к сетевым дискам и установки принтеров, для изменения настроек системы и вывода сообщений на экран. С помощью сценариев можно изменять параметры функционирования программного обеспечения и оборудования компьютера.

В Windows возможно выполнение сценариев, написанных на таких языках программирования, как VBScript, JScript и JScript .NET. Для исполнения программного кода сценария на компьютере должна присутствовать система, которая интерпретирует этот код и обеспечивает взаимодействие с другими программами. Обеспечивает такую функциональность специальный *сервер сценариев* — Windows Script Host (WSH).

Примечание

Кроме упомянутых языков программирования администраторы могут применять и другие технологии, такие как Perl, TCL, REXX, Python и др. Для этого необходимо установить соответствующие модули интерпретаторов разработки третьих фирм.

WSH встроен в операционные системы Windows 98/ME/2000 и старше. Для Windows 95 можно бесплатно установить WSH, загрузив соответствующий файл с информационного сервера разработчика.

Каждая последующая версия WSH существенно функциональнее предыдущей, поэтому для систем, находящихся в эксплуатации, целесообразно обно-

вить эту службу до последней версии. Для сравнения, если для Windows 98/ME предназначалась версия WSH 1.0, то на момент написания книги для загрузки была доступна версия 5.7 (для Windows XP, Windows 2003 Server и Windows 2000; данная версия уже входит в состав Windows Vista).

Как правило, администраторы редко создают нужные сценарии "с нуля". Обычно ищется подходящий пример, который лишь незначительно модернизируется. Подобные коды достаточно широко представлены в Сети, а на сайте разработчика ОС можно воспользоваться для поиска подходящего решения следующей ссылкой: **http://www.microsoft.com/technet/community/scriptcenter/scresorc.mspx**. На рис. 13.3 представлено окно одной из коллекций, свободно доступных с сайта разработчика (Portable Script Center, **www.microsoft.com**).

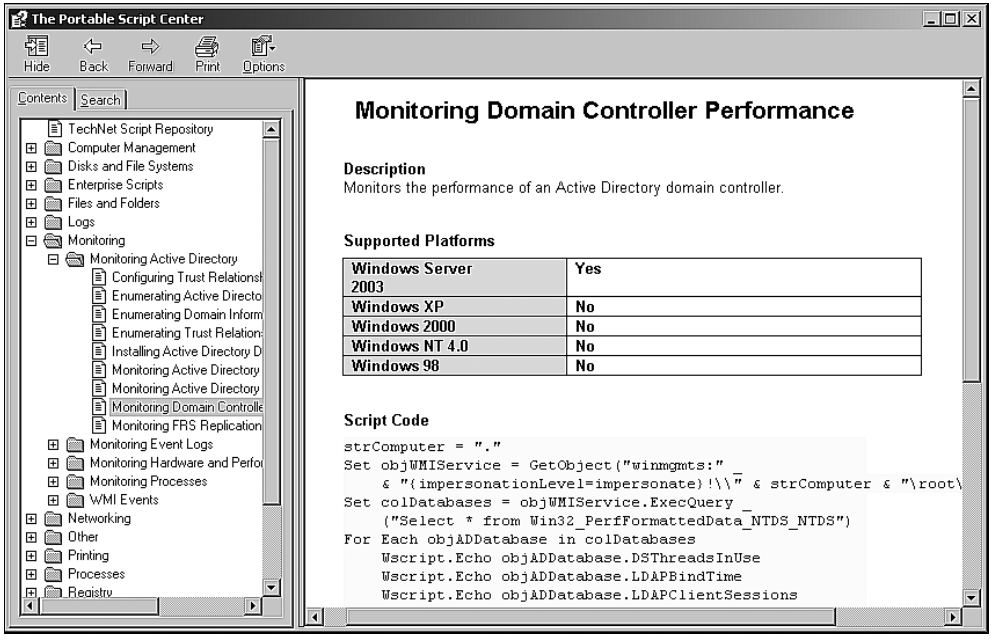


Рис. 13.3. Script Center

Многие администраторы чувствуют себя недостаточно уверенно при составлении сценариев. В то же время применение сценариев существенно облегчает администраторские функции. В таких ситуациях могут помочь специальные продукты, которые позволяют составить сценарий в визуальном режиме, просто добавляя необходимые шаги (проверки, условия, действия и т. п.) путем перетаскивания мышью и задания необходимых характеристик каждого шага.

Один из таких продуктов приведен на рис. 13.4. Это программа AutoMate от компании Unisyn Software, LLC (**www.unisyn.com**)

WMI использует технологию DCOM (distributed COM), поэтому он "работает" в локальных сетях. Хотя DCOM и относится к известным протоколам, на большинстве межсетевых экранов он блокируется администраторами. Поэтому для управления компьютерами в других сетях (Интернете) с помощью WMI следует использовать специальные расширения. Они доступны только для Windows 2003 Server Service Pack 2; Windows 2003 Server Service Pack 2 x64 Edition; Windows XP; Windows XP 64-bit (соответствующие методы уже присутствуют в Windows Vista). Загрузить их можно со страницы

http://www.microsoft.com/downloads/details.aspx?FamilyID=845289ca-16cc-4c73-8934-dd46b5ed1d33&DisplayLang=en.

После установки данных обновлений управление компьютерами будет осуществляться по протоколам HTTP/HTTPS, которые на межсетевых экранах обычно не блокированы. При этом обращение к объектам WMI должно осуществляться по следующему образцу:

```
strComputer = "mycomp.mydomain.ru"
Set objWRM = CreateObject("WSMan.Automation")
Set objSession = objWRM.CreateSession("http://" & strComputer)
strResource =
http://schemas.microsoft.com/wbem/wsman/1/wmi/root/cimv2/Win32_Service
```

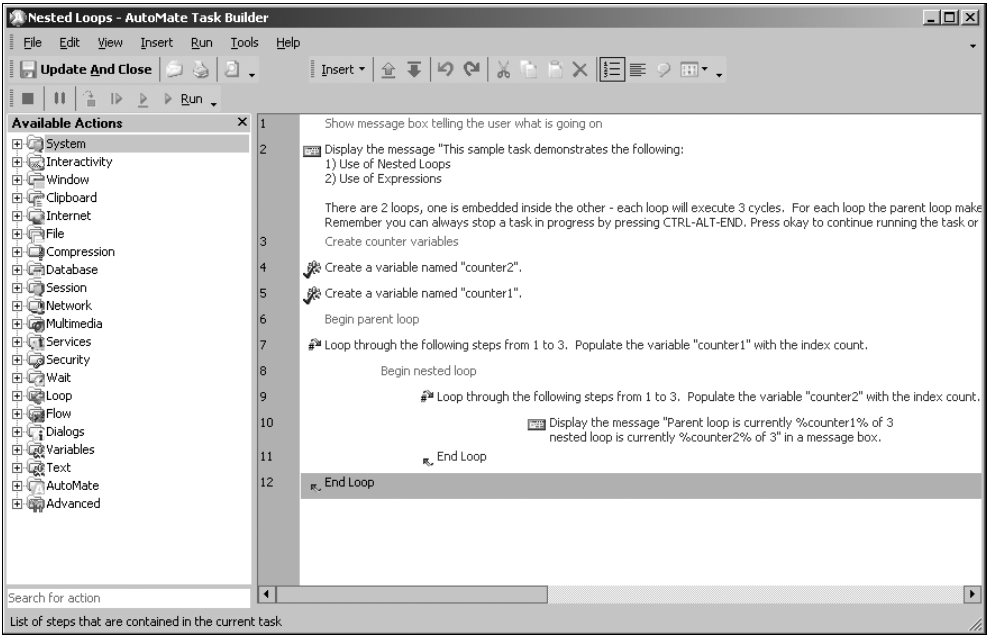


Рис. 13.4. Мастер создания автоматического сценария управления системой

Windows Management Interface

Windows Management Interface (WMI) — это технология управления Windows-компьютерами, реализующая стандарты Web-управления предприятием (WBEM, Web-based Enterprise Management[1]). WMI позволяет собирать данные с компьютеров и обеспечивать выполнение команд настройки. Как обрабатывать получаемые данные, стоит ли их хранить, какие команды подавать и т. п. — это задача другого программного обеспечения (например, описанного в последующих разделах).

WMI реализовано для всех операционных систем Windows, начиная с Windows 95. Однако устанавливается эта подсистема по умолчанию только в Windows Millennium Edition, Windows 2000, Windows XP, Windows 2003 Server и последующих операционных системах. Для других поддерживаемых версий Windows соответствующие файлы установки доступны для бесплатной загрузки.

WMI выполняет функции сбора данных и управления конфигурацией компьютера через специализированные программные модули, называемые *провайдерами* (providers). Существуют провайдеры для управления драйверами Windows, операционной системой, Internet Explorer, Office 2000/XP, службами каталогов и т. п. Этот список постоянно пополняется, и при установке на компьютер нового программного обеспечения перечень управляемых объектов может существенно расшириться.

Стандартами WBEM предусмотрена типовая схема управляемых объектов — Common Information Model (CIM). Эта схема реализована в WMI как пространство имен Cimv2. В этом пространстве имен по умолчанию выполняются WMI-команды.

Поскольку через WMI доступны многие функции управления компьютерной системой, правильной настройке прав доступа следует уделить особое внимание. Соответствующие операции выполняются через окно управления компьютером (в контекстном меню значка **Мой компьютер** нужно выбрать пункт **Управление**, рис. 13.5, *слева*). После чего следует выбрать строку **Службы и приложения | Управляющий элемент WMI** и в его меню открыть пункт **Свойства**. В появившемся окне (рис. 13.5, *справа*) можно установить желаемые права доступа к соответствующим пространствам имен службы.

WMI Query Language

При практическом использовании можно обнаружить, что пространство имен WMI напоминает базу данных, а классы WMI — отдельные таблицы этой

[1] WBEM разработан Distributed Management Task Force — **http://www.dmtf.org/**.

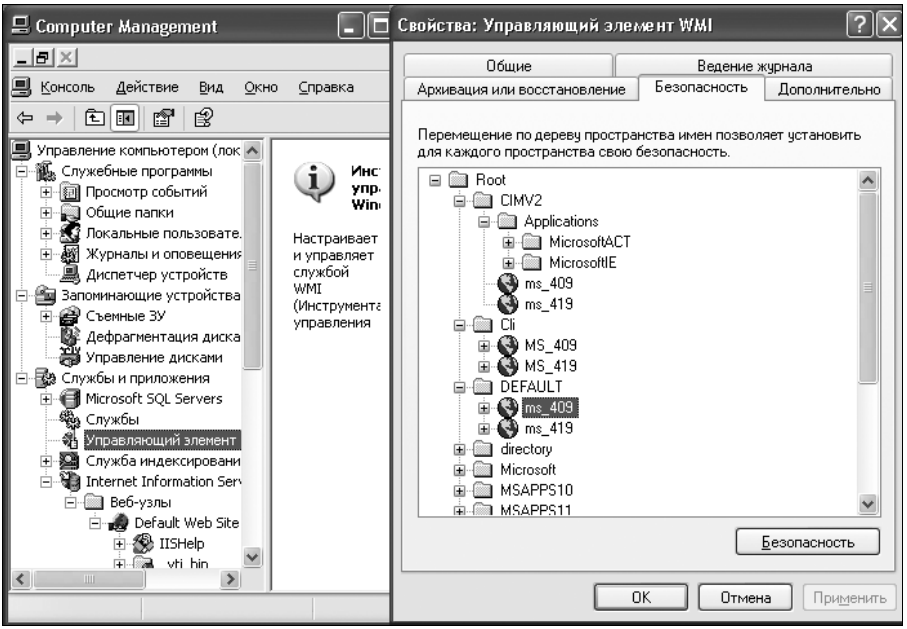


Рис. 13.5. Настройка прав доступа к WMI

базы данных. Каждый элемент (в WMI его принято называть *instance* соответствующего класса) аналогичен строке в такой таблице, а характеристики этого элемента подобны полям таблицы.

Для получения параметров устройств (например, характеристик сетевых карт или списка автоматически загружаемых при старте программ) администраторы могут использовать язык запросов — WMI Query Language (WQL). WQL является диалектом языка SQL, имеющим некоторые дополнения. Команды WQL также принято называть *запросами*, поэтому администраторы, которые имеют некоторый опыт работы с базами данных и создания различных запросов, легко смогут обучиться использованию WMI в своей практике.

Однако WQL может быть использован только для получения той или иной информации. Запросы WQL не позволяют добавить данные или изменить определенные параметры. Если вам необходимо выполнить какие-либо настройки, то сначала следует получить (выбрать) с помощью запросов WQL соответствующий объект, а затем, используя допустимые для данного элемента методы управления, провести желаемые изменения.

Варианты применения WMI

Существуют различные методы использования возможностей WMI.

Для автоматизации управления компьютерными системами доступ к WMI может быть реализован через Windows Scripting Host. Это позволяет админи-

стратору создавать сценарии управления системами. Вы можете запросить характеристики какого-либо объекта с помощью WQL и изменить значения некоторых из них, присвоив новые величины параметрам выбранного объекта.

WMI имеет свой интерпретатор, работающий в режиме командной строки, — WMIC (WMI Command-line tool). Для его запуска необходимо выполнить команду `WMIC`. В результате на экране появляется окно, аналогичное окну командной строки, в котором следует вводить необходимые команды. В этой утилите доступна объемная подсказка, вызываемая по ключу `/?`. Однако для успешной работы в этом режиме необходимо четко представлять, в каком классе находится объект, характеристики которого вы хотите получить или в настройки которого предполагается внести изменения.

Определенную помощь в представлении о структуре классов WMI может оказать программа WBEMTest.exe, имеющаяся на каждом компьютере с установленным WMI. Используя WBEMTest.exe, можно перечислить классы WMI и отобразить характеристики отдельных элементов. Утилита позволяет выполнить WQL-запрос и увидеть его результат на экране. Хотя утилита предназначена для поддержки и имеет ограниченные возможности, но она может помочь разобраться с WMI-классами.

Для тех, кто предполагает использовать управление системами через WMI, целесообразно установить на компьютер какую-либо программу просмотра WMI. Например, весьма неплохими возможностями обладает программа CIM Studio, которая может быть свободно загружена с сайта Microsoft[1] (рис. 13.6).

Для использования WMI необходимо знание иерархической структуры объектов системы. Запомнить ее практически невозможно, поэтому при составлении запросов могут помочь такие продукты, как WMI CIM Studio. С помощью данной программы администратор имеет возможность подключиться к любому пространству имен, зарегистрированному в системе, отобразить существующие классы объектов, увидеть свойства класса (характеристики, которые можно получить при исполнении запроса) и методы (параметры, которые можно установить в команде). Здесь же можно открыть окно, в котором попробовать создать собственный WMI-запрос и сразу увидеть его результаты.

Примечание

Те, кто использует в своей работе Microsoft Visual Studio .NET, могут применять входящие в ее состав утилиты. Если ни одна из перечисленных программ по

[1] **http://www.microsoft.com/downloads/details.aspx?FamilyId=6430F853-1120-48DB-8CC5-F2ABDC3ED314&displaylang=en**. Можно найти поиском по ключевым словам "WMI Administrative Tools".

каким-либо причинам вас не устраивает, то в Интернете легко можно найти и другие утилиты.

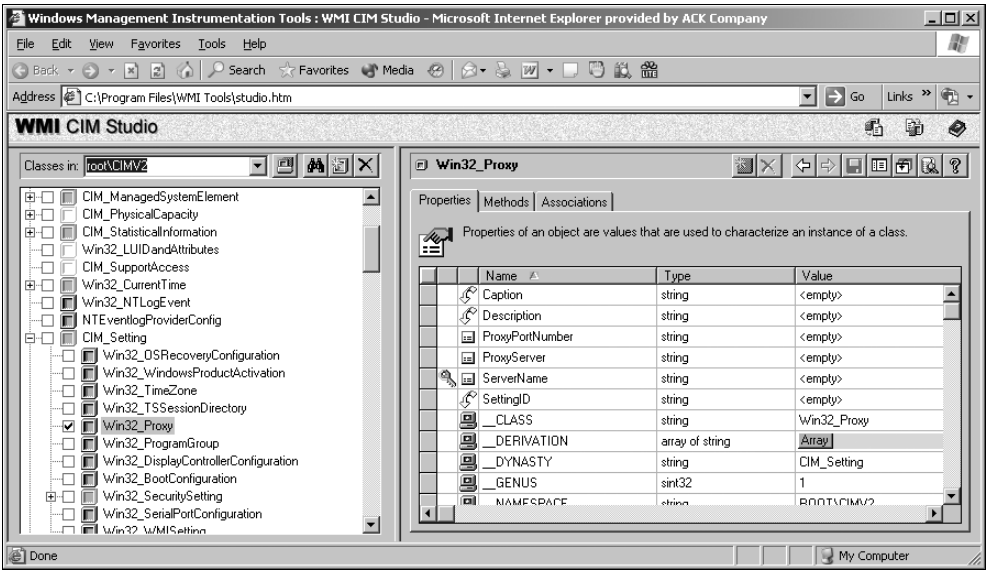


Рис. 13.6. WMI CIM Studio

Примеры

Большинство практических WMI-сценариев создается на основе того или иного примера, который найден в Интернете. Приведу несколько возможных вариантов WMI-сценариев.

- **Перечисление логических дисков системы.**

  Следующий сценарий на Visual Basic выводит на экран наименования логических дисков, присутствующих в системе.

```
for each Disk in GetObject("winmgmts:").InstancesOf _
  ("CIM_LogicalDisk")
    WScript.Echo "Instance:", Disk.Path_.Relpath
Next
```

  При выполнении цикла переменной `Disk` поочередно присваиваются все элементы класса "логический диск". Затем (третья строчка) сценарий выводит на экран сообщение с логическим именем этого диска.

- **Перезапуск остановившихся служб системы.**

  Следующий пример кода на Visual Basic может быть использован для перезапуска остановленных служб системы:

```
Set colListOfServices = GetObject("winmgmts:").ExecQuery _
("Select * from Win32_Service Where State = 'Stopped' and _
  StartMode = 'Automatic'")
For Each strService in colListOfServices
  strService.StartService()
Next
```

Первая строка кода создает коллекцию объектов, удовлетворяющих условию выборки, заданному в WQL-запросе. Этот запрос выбирает все службы, для которых установлен автоматический режим запуска и которые в настоящий момент остановлены. Пятая строка кода организует цикл, выполняющий метод запуска служб, найденных на предыдущем этапе.

Для данного сценария можно установить автоматический запуск через определенные промежутки времени, чтобы гарантировать работу всех служб компьютера[1].

Контроль функционирования систем. Microsoft Operation Management Server

Администратор компьютерной системы отвечает за функционирование всех ее составляющих. Чтобы работать не только по фактам инцидентов, а предупреждать возможные отказы, существенную часть своего рабочего времени он должен затрачивать на оценку состояния серверов системы, просмотр протоколов работы различных служб и т. п. Анализ получаемой информации обычно требует высокой квалификации администратора, являясь весьма рутинной операцией. Даже если администратор и не пренебрегает этой частью своих повседневных обязанностей, тем не менее, все эти усилия не могут гарантировать контроль функционирования компонентов в реальном режиме времени.

Существуют различные программы, призванные осуществлять те или иные функции контроля работоспособности серверов. Advanced Host Monitor от KS-Soft (**http://www.ks-soft.net/hostmon.eng/index.htm**), бесплатная программа Nagios, созданная для Linux (**http://www.nagios.org/**), MonitorMagic от Tools4ever (**http://www.tools4ever.com/**). Много других программ доступно через поисковые системы, например в Желтых страницах Yahoo и т. п. В подобных программах реализуются два подхода к контролю систем. Первый — это получение и анализ данных, доступных удаленной системе без каких-

[1] В свойствах службы есть опция восстановления, в которой можно задать параметры перезапуска службы после ее аварийной остановки. Однако если служба по тем или иным причинам не стартовала при запуске системы или была остановлена вручную, то автоматически она также не будет запущена. Приведенный в примере код позволяет автоматически находить такие службы и запускать их.

либо дополнительных операций. Так можно анализировать данные журнала протокола событий на наличие сообщений об ошибках, проверять доступность системы командой `ping`, а работоспособность службы информационного сервера — наличием ответа на HTTP-запрос и т. д. Пример подобной программы — GFI Server Monitor (**http://www.gfi.com/**).

При втором подходе на контролируемые системы устанавливаются специальные программы — *агенты*. Понятно, что в этом случае возможности контроля существенно увеличиваются. Примером такого подхода является программа Microsoft Operation Management Server.

Примечание

Данный продукт приводится в качестве примера только лишь потому, что его разработчиком является сам изготовитель операционной системы.

Microsoft Operation Management Server берет на себя рутинный контроль состояния системы, причем делает это в реальном времени. С заданной периодичностью (обычно каждые пять минут для типовых служб, но эти параметры можно настроить) проверяется функционирование основных компонентов системы. Так, почтовая система отправляет и получает тестовое письмо, Web-сервер отвечает на HTTP-запрос. MOM предупреждает о нехватке свободного места на жестком диске и о том, что сервер DNS не может загрузить копию зоны с первичного сервера; сообщает об ошибке операции резервного копирования и о большом количестве почтовых сообщений, стоящих в очереди на отправку. Одновременно с отправкой администратору сообщения о событии отображается информация из базы знаний, описывающая возможные действия персонала в данной ситуации. Кроме того, MOM осуществляет сбор и анализ записей файлов протокола систем, параметров счетчиков производительности, ведет корпоративную базу по возникшим инцидентам и т. д.

Контроль систем выполняется при помощи специальных *сценариев* для MOM-сервера, которые запускаются устанавливаемыми на компьютерах-клиентах агентами. Эти сценарии входят в состав дополнительных модулей (Administration Management Kit, AMK), часть из которых загружается бесплатно, а часть доступна в коммерческом варианте. В распоряжении администратора имеются модули для контроля работы службы каталогов, служб WINS, DHCP, DNS, серверов SQL, IIS, Exchange, Project, SMS и т. д. Есть модули для сбора информации от не управляемых агентами MOM устройств: SNMP-устройств и данных от Linux-систем (формируемых утилитой `syslog`).

Число разработок AMK постоянно растет. При этом можно легко доработать сценарии в соответствии со специализированными требованиями своей системы (сценарии написаны на Visual Basic).

Для систем, осуществляющих обслуживание пользователей, особенно важно оперативно реагировать на возникающие сообщения о потенциальных проблемах. Администратор может настроить в MOM автоматическую реакцию на возникающие события: от посылки простых предупреждений на пейджер до запуска любых программ. Очевидно, что действия, реализуемые *без участия администратора*, возможны в ответ только на события, которые уже случались и для которых есть существенная вероятность повторения в будущем, поэтому следует хорошо изучить свою информационную систему, знать, на *какие* события и *как* следует автоматически реагировать.

По результатам наблюдения можно сформировать отчеты, позволяющие администратору выполнить оценку состояния системы, запланировать точную настройку систем. В качестве примера графического представления отчета на рис. 13.7 показана загрузка процессоров нескольких серверов в заданный промежуток времени.

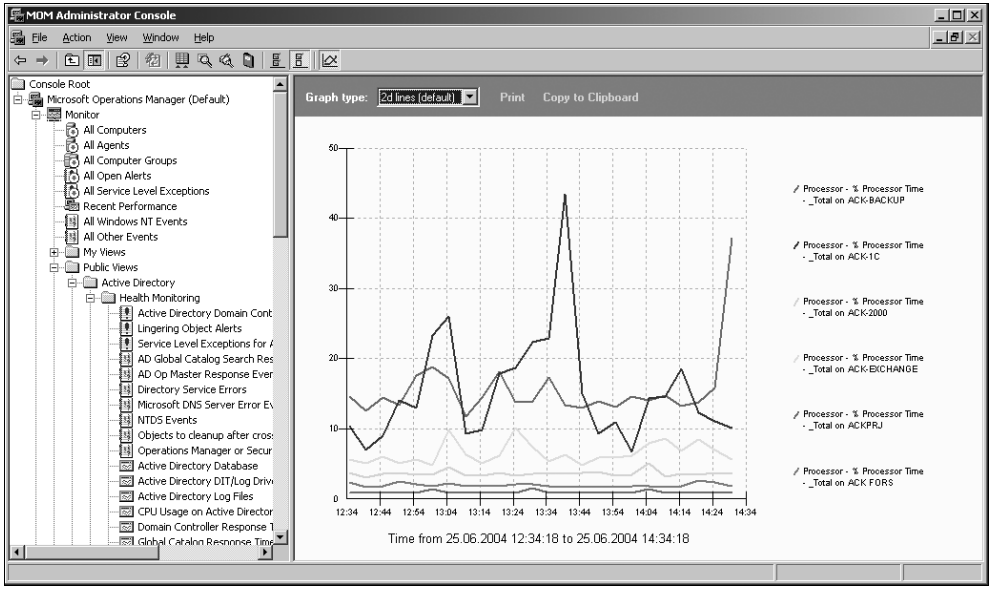


Рис. 13.7. Отчет, сформированный по результатам наблюдения за системой

Программы, аналогичные MOM, — необходимая часть информационной системы. Они берут на себя часть рутинных операций контроля за системой, однако не стоит думать, что они способны заменить опытного администратора. Во-первых, автоматизированные системы обнаруживают — по разным оценкам — только около четверти возникающих проблем. Во-вторых, разработка сценариев реагирования будет оправдана только для определенного круга постоянно возникающих проблем. Ну и в-третьих, для создания собственных

правил нужно постоянное участие как программиста, так и администратора, что сложно реализуемо в малых и средних организациях.

Контроль прикладного ПО

Описанные выше программы контролируют, прежде всего, работоспособность основных служб инфраструктуры. Однако работоспособность сервера баз данных отнюдь не означает функционирование вашей прикладной программы, которая работает с этими данными. В то же время конечный пользователь оценивает работу всей информационной системы именно по доступности конечных бизнес-задач.

Хотя разработчики программ контроля за функционированием серверов постоянно добавляют в состав функций новое поддерживаемое ПО (например,

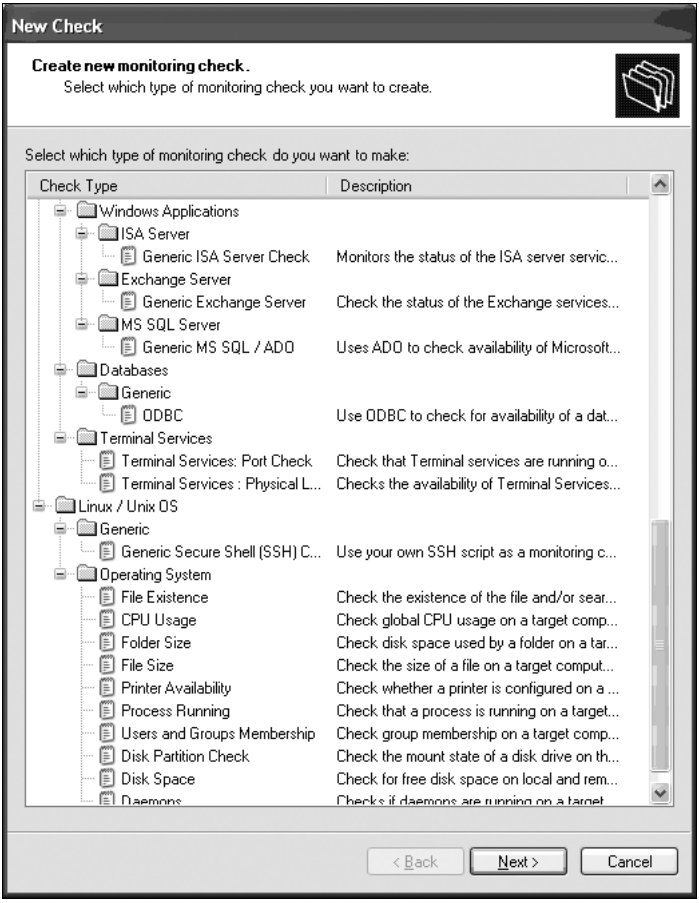


Рис. 13.8. Создание нового правила контроля

в составе GFI Server Monitor v.7 включен контроль работы антивирусных программ от Symantec и Kaspersky), надеяться на включение в этот список специализированного ПО не имеет смысла.

Обычно программы контроля имеют специальные мастера для создания пользовательских правил контроля системы. На рис. 13.8 представлено окно мастера программы GFI Server Monitor. Даже по отображаемому участку легко судить о функциональности системы контроля.

В современных компьютерах администратор может следить практически за любыми характеристиками аппаратной части и программного обеспечения, причем возможности контроля все более расширяются и начинают применяться не только на серверных платформах, но и на рабочих станциях.

Оптимальный вариант — включить реализацию соответствующего кода контроля в техническое задание на применяемые программы. Если такая возможность отсутствует, то следует собственными силами создать (модернизировать) тот или иной агент контроля. Часто такая задача доступна специалисту, имеющему даже незначительный опыт программирования.

Удаленное администрирование

Администраторам часто приходится со своего рабочего места управлять серверами и рабочими станциями. С появлением терминальных служб и возможности подключения к удаленному рабочем столу выполнение этих операций существенно облегчилось.

Примечание

Технологии, описываемые в следующих разделах, могут быть использованы только на *работоспособной операционной системе*. Если вы хотите установить новую версию ОС, изменить параметры BIOS или вывести компьютер из "подвисания", то необходимы иные решения. Так, современные модели серверов имеют модули, позволяющие удаленно видеть "картинку" и управлять клавиатурой так же, как если бы работа проводилась локально за консолью *(см. разд. "Intelligent Platform Management Interface" этой главы)*. Для обычных систем можно порекомендовать IP KVM-коммутаторы, обеспечивающие передачу изображения монитора и управление клавиатурой по IP-сети. Дополнением к данному решению могут быть устройства отключения питания компьютеров по IP-сети, которые обеспечат перезагрузку системы даже в случае отсутствия у нее реакции на команды клавиатуры.

"Удаленный помощник"

Режим удаленного подключения к рабочему столу в Windows XP предназначен в первую очередь для оказания помощи пользователю компьютера, чтобы в случае возникновения проблем в работе он имел возможность обратиться к

специалисту, а последний, подключившись к компьютеру, оперативно оказать посильную помощь. Администраторы системы могут задать в групповой политике параметры вызова помощника.

Поскольку в Windows XP Professional/Vista при подключении удаленного пользователя к компьютеру текущий пользователь не может продолжать работу[1], то в системе предусмотрен специальный механизм отправки приглашений на удаленное подключение. При подключении удаленного помощника рабочий стол виден одновременно двоим людям: самому пользователю и тому помощнику, который принял приглашение. Первоначально удаленный помощник не может управлять компьютером: ему доступно только наблюдение и возможность обмена мгновенными сообщениями.

Предоставить удаленному помощнику право на управление компьютером должен текущий пользователь, причем он может в любой момент вернуть себе управление системой.

Отправить приглашение можно с помощью почтовой программы или программы MSN Messenger. Для отправки приглашения необходимо выполнить **Пуск | Справка и поддержка** и следовать указаниям мастера отправки приглашения. Для осуществления автоматического подключения удаленный помощник должен его принять. В результате специалист сможет наблюдать удаленный рабочий стол, однако управление компьютером остается за локальным пользователем.

Примечание

В Vista появилась возможность предложить пользователю принять приглашение на удаленный контроль компьютера. Команда `msra /offerRA <имя удаленного компьютера>` позволяет запустить помощника и инициировать сессию на удаленной системе. Этот режим очень удобен для администраторов при оказании поддержки неопытным пользователям. Пользователю достаточно только дать согласие на подключение и предоставить необходимый уровень контроля над своей системой.

Если удаленному специалисту необходимо "перехватить" управление компьютером, то он может обратиться к пользователю путем обмена мгновенными сообщениями. Если пользователь даст такое согласие, то дальнейшая работа удаленного пользователя ничем не будет отличаться от обычной терминальной сессии, кроме возможности локального пользователя в любой момент вернуть себе управление компьютером.

[1] Система выдает соответствующее предупреждение и в случае отсутствия ответа по истечении заданного промежутка времени производит отключение текущего пользователя.

Удаленное управление рабочим столом

Для удаленного управления серверами предназначена возможность подключения администратора: в режиме удаленного администрирования терминальных служб в терминах Windows 2000 или подключение к удаленному рабочему столу в терминологии Windows 2003/XP/Vista. В этом режиме пользователи, имеющие права администратора компьютера, могут выполнить удаленное подключение к рабочему столу сервера и выполнять любые[1] операции по настройке системы.

Примечание

Этот режим предусматривает максимально два подключения для удаленных администраторов. Поэтому имеет смысл ввести ограничения на длительность удаленной сессии, чтобы система автоматически отключала пользователей по истечении заданного периода времени. Это позволит, например, вновь осуществить подключение к серверу в случае обрыва соединения[2].

Удаленное управление рабочим столом позволяет контролировать систему только после старта соответствующих служб. При возникновении проблем, например в процессе перезагрузки системы, администратору понадобится доступ к компьютеру непосредственно с консоли. Однако если условиями эксплуатации ставится задача удаленного управления в любой момент времени, то осуществить такое требование можно только приобретением аппаратной части, поддерживающей перенаправление данных в процессе загрузки системы.

Утилиты удаленного управления компьютером

Хотя для Windows XP присутствует возможность удаленного подключения к рабочему столу, на практике она редко используется администраторами для рабочих станций пользователей. Во-первых, соответствующие опции должны быть предварительно включены в настройках клиентского компьютера, во-вторых, при попытке удаленного подключения текущий пользователь должен завершить свою работу. Поэтому обычно применяется та или иная программа, позволяющая увидеть удаленный рабочий стол на локальном компьютере и перехватить управление клавиатурой и мышью.

Существует большое количество таких программ: как бесплатные версии (VNC), так и коммерческие (pcAnywhere[3] от Symantec, Remote Admin от

---

[1] Практически любые. Некоторые программы, например, не могут быть установлены в режиме терминальной сессии. Например, eRoom из состава Documentum и т. п.

[2] На практике не всегда удается осуществить подключение тем же пользователем к существующей сессии терминального сервера, особенно для Windows 2000 Server. Поэтому введение такого лимита не позволит "потерять" удаленное управление системой.

[3] Последняя версия программы позволяет администратору удаленно управлять как системами на основе Windows, так и Linux-компьютерами.

Famatech, Inc., NetOp Remote Control от DanWare Data и т. д.). Выбор конкретной версии определяется возможностями администратора.

В любом случае для управления удаленным компьютером программой такого класса на него должна быть установлена клиентская часть. Для систем на базе Windows NT/200*x*/XP эта операция может быть проведена централизованно, используя учетную запись администратора домена. Установка клиентского модуля на системы с Windows 9*x*/ME обычно производится с помощью модификации сценариев входа в сеть. Приведем описание возможностей некоторых программ управления удаленным компьютером.

- VNC (Virtual Network Computing, **www.realvnc.com**).

  VNC позволяет удаленно просматривать любые платформы (UNIX, Win32, Mac, мобильные клиенты и т. п.). Это кроссплатформенное приложение; имеется вариант на Java, который позволяет управлять рабочим столом из любого обозревателя Интернета.

  Коды программы открыты с 1998 года; пользователи загрузили более 20 млн ее копий. Программа включена в состав популярной операционной системы Linux. По данным ее сайта, VNC используют все компании, входящие в список Fortune 500[1].

- Hidden Administrator.

  Hidden Administrator[2] (**www.hidadmin.ru**) — бесплатная программа российского автора. Подобно другим программам она обеспечивает полный доступ к ресурсам удаленного компьютера, предоставляет администратору возможности скрытого наблюдения и управления, обмена файлами и т. п. Отметим также наличие опции удаленного включения системы (Wake on LAN).

- Remote Administrator (RAdmin).

  Еще одной часто используемой программой удаленного управления для платформы Windows является RAdmin. Она также позволяет одновременно работать с несколькими удаленными компьютерами с помощью обычного графического интерфейса. Учитывая, что эта задача разработана для Win32, она использует методы аутентификации пользователей, принятые в Windows.

  Программа позволяет осуществить копирование файлов на управляемый компьютер, поэтому ранее ее достаточно часто применяли для управления серверами Интернета.

---

[1] Периодически обновляемый список наиболее успешных компаний.

[2] Следует учитывать, что часть антивирусных программ рассматривает утилиты удаленного управления в качестве вредоносного кода. Например, антивирус Касперского таковыми считает Hidden Administrator и Remote Administrator.

Примечание

Использование программ удаленного управления в открытых сетях должно сопровождаться особыми мерами безопасности. Целесообразно внимательно следить за обновлениями программ и использовать только последние версии, поскольку каждая новая разработка обычно характеризуется более устойчивой работой и повышенной защищенностью данных сессий. Например, уязвимость в программе RAdmin была использована для DdoS-атак на компьютеры с ее инсталляциями (см. **http://www.opennet.ru/opennews/art.shtml?num=3424**).

Microsoft System Management Server

Разветвленная компьютерная система нуждается в централизованном учете и управлении программным обеспечением. Для этих целей предусмотрен специальный сервер — Microsoft System Management Server (SMS).

Прежде всего, SMS — это мощный инструмент инвентаризации системы. С его помощью централизованно собираются данные как по составу аппаратной части компьютеров, так и по установленным на них программах (причем учитываются все исполняемые файлы, которые обнаруживаются на дисках системы). SMS использует специальную технологию, позволяющую выполнять на удаленных компьютерах установку программного обеспечения. Учитывая, что в SMS содержится вся информация о составе систем, администратор получает возможность точной настройки установки программ, выбора тех систем, на которых необходимо выполнить эту операцию. Так, можно ограничить операцию только компьютерами с установленной ОС Windows 2000 при наличии SP4 и MS Office 2000 с SP2 без горячих заплаток, на которых имеется не менее 200 Мбайт свободного места на системном диске, а частота процессора более 800 МГц.

SMS берет на себя рутинную работу по распространению установочных файлов в удаленные филиалы, контроль за установленными программами (например, в случае замены системного блока и сохранения имени компьютера SMS обнаружит отсутствие программ, назначенных администратором для данной станции, и повторно их установит), распространение и установку обновлений операционной системы и MS Office.

По результатам выполнения команд система централизованно соберет информацию протокола установки, которая может быть легко проанализирована администратором. В составе SMS предусмотрена возможность предоставления информации в виде графических отчетов, причем разработчики подготовили немалое количество шаблонов для наиболее популярных анализов. В случае необходимости специалист может легко создать собственный запрос, учитывающий любые параметры как оборудования, так и программного состояния систем.

Отдельные утилиты третьих фирм

Набор имеющихся в системе утилит управления обычно не достаточен для выполнения большого объема административных задач управления системами. Администраторы весьма часто пополняют свой арсенал продуктами, выпущенными независимыми разработчиками программного обеспечения.

Приведем несколько ссылок на подобные продукты.

Утилиты от Sysinternals

По адресу **http://www.sysinternals.com/ntw2k/utilities.shtml** находится список нескольких бесплатных утилит, весьма необходимых администратору.

Прежде всего, отметим утилиту Filemon, которая позволяет отследить все файловые операции, совершаемые в системе. Утилита показывает, какие файлы создаются в системе, какие программы и к каким файлам обращаются за чтением данных или для их записи, успешны ли эти операции или завершены с ошибкой.

Аналогичная утилита следит за любыми обращениями к реестру системы и помогает узнать, какая программа и как запрашивает информацию. Существует программа, отображающая все запущенные в системе процессы с указанием их иерархии. А утилита Diskview позволяет увидеть, какой сектор занят заданным файлом (удобно для получения информации о поврежденном файле в случае появления сбойных секторов).

Список утилит достаточно велик, поэтому просто порекомендую посетить упомянутый сайт и загрузить необходимые программы.

ПО восстановления системы

Существует несколько программ, позволяющих осуществить загрузку с компакт-диска в случае краха операционной системы и выполнить ряд операций по ее восстановлению (например, правку реестра, замену файлов по сети и т. п.). Мы упоминали уже ERD Commander, отметим также диски восстановления от Acronis. Аналогичные программы достаточно распространены и обладают сходными функциями. Главное, что подобная утилита должна быть в наборе инструментов системного администратора.

ПО инвентаризации систем

Существует много программ, позволяющих проанализировать информационную систему и получить отчет о составе аппаратной части и установленном программном обеспечении. Очень часто такие программы содержат возмож-

ность анализа установленных обновлений безопасности и выдают список патчей, которые следует инсталлировать на конкретную систему. Кроме того, анализируются настройки компьютеров с точки зрения реализации базовых требований по безопасности настройки систем (например, состав групп администраторов, факт предоставления всего диска в общее пользование, возможность выполнения ряда операций от имени анонимного пользователя и т. п.) и соответствующие рекомендации также предоставляются администратору. В данном классе представлено очень много программ — от бесплатных версий до серьезных коммерческих продуктов. Читатель легко найдет соответствующие ссылки в глобальной сети.

Утилиты дефрагментации дисков

Встроенная утилита дефрагментации от фирм Microsoft Corporation и Diskeeper Corporation (прежнее название Executive Software) весьма неудобна при использовании в масштабе предприятия. Нет возможности управления запуском операции на других системах, запуск по расписанию появился только с версии для Windows XP[1] или т. п. В то же время при достаточно серьезной нагрузке систем (например, Web-серверы) дефрагментация может повысить производительность весьма существенно (до 10—15%).

Внешний вид консолей управления различных дефрагментаторов мало отличается друг от друга. Основные функциональности, которые добавляют серверные версии таких программ, — это возможность выполнения операций по заданному графику, автоматическая установка агентов на компьютеры сети и создание распределенных заданий по дефрагментации дисков. Естественно, что администратору доступна информация о результате выполнения заданий по каждой включенной в операцию машине (итоги работы, итоговый процент фрагментации по каждому диску и т. п.).

Существуют различные корпоративные решения. Прежде всего, это серверная версия Diskeeper Server, O&O Defrag (O&O Software GmbH, **www.oosoftware.com**), дефрагментатор от Winternals (**www.winternals.com**) и др. Функциональность программ почти одинакова. Администратор может использовать любой вариант в зависимости от своих возможностей.

Снифферы

Хотя администратору и не нужно разбираться в тонкостях сетевых протоколов, но он должен уметь на базовом уровне использовать тот или иной вари-

[1] При создании расписания запуска штатной программы следует не забыть вручную указать имя дефрагментируемого диска (см. KB555098).

ант программы сетевого анализатора *(сниффера)*. Ранее уже упоминалось, как применять сниффер для оценки основных параметров функционирования сети: процента использования полосы пропускания, оценки используемых протоколов, количества пакетов с ошибками и т. п. Кроме того, сниффер позволяет обнаружить отклонения в работе устройств: избыточное количество пакетов того или иного типа, что может быть признаком заражения какой-либо системы вирусом или готовящейся атаки.

Также сниффер незаменим для настройки работы брандмауэра со специализированными недокументированными приложениями (обнаружение реально используемых приложением портов). Программы-анализаторы сетевого трафика обычно имеют развитые средства его анализа; это позволяет автоматически выявлять те или иные отклонения в работе сетевых устройств (рис. 13.9). Очень интересен открытый проект Ethereal (**http://www.ethereal.com**). Эта свободно распространяемая программа имеет такие возможности, как восстановление по перехваченным пакетам, например, всего телефонного разговора или всех переданных во время сеанса telnet данных и т. п.).

Окно экспертного анализа сниффера выделяет пакеты, предположительно свидетельствующие о недостатках в работе системы. Так, на приведенном рис. 13.9 система автоматически выделила поздний отклик удаленного компьютера, слишком большое число повторов передачи пакетов и т. п. Администратору достаточно отметить нужный пункт, и программа автоматически покажет связанные с данным выводом пакеты данных. Таким образом, можно

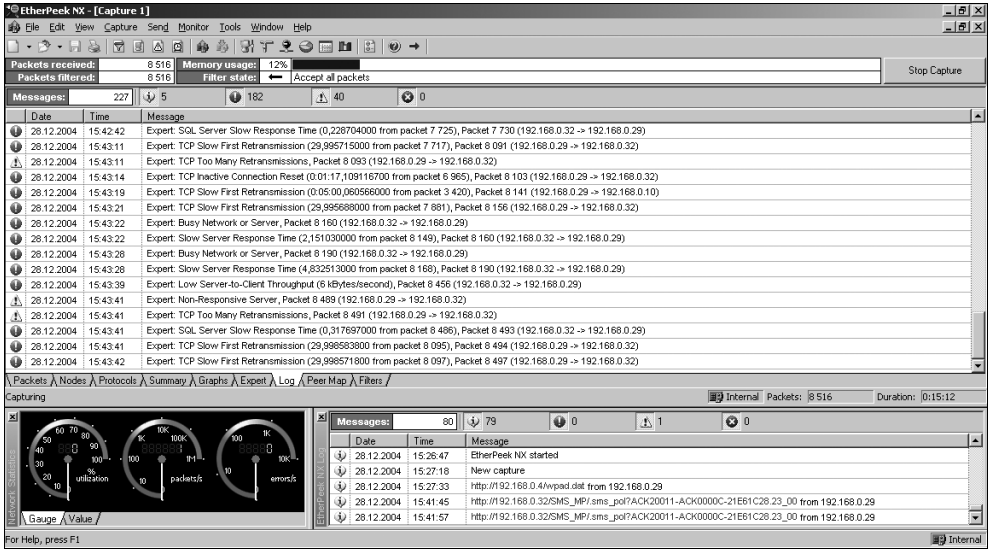


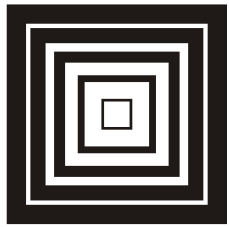
Рис. 13.9. Окно анализатора сетевых пакетов EtherPeek NX (**http://www.wildpackets.com/**)

оценить достаточное число параметров работы системы, не обладая глубокими знаниями протоколов передачи информации.

Я советую установить ту или иную программу анализа и мониторинга сетевого трафика и проанализировать трафик систем при обычных условиях. Это позволит приобрести некоторый опыт, чтобы в случае необходимости оперативно оценить, откуда идут пакеты, отфильтровать ненужный для анализа в конкретном случае трафик, поставить триггер на запуск анализатора по конкретным событиям и т. д.

Программы очистки диска

Программы для безопасного удаления информации с диска обычно входят в те или иные коммерческие дистрибутивы. Но вы можете использовать и бесплатную версию (на основе открытой лицензии), загрузить которую можно по ссылке **http://www.tolvanen.com/eraser/**.



ГЛАВА 14

Автоматизация установки программного обеспечения

Системному администратору постоянно приходится вводить в эксплуатацию новые рабочие места, модернизировать существующие. Время выполняемых при этом операций (установка операционной системы, прикладного программного обеспечения, обновлений и т. п.) можно существенно сократить, если использовать тот или иной вариант автоматизации своих действий.

Автоматизация процесса установки

При установке операционной системы приходится вводить много ответов, начиная от часового пояса, параметров сети, желаемого разрешения экрана и т. д. В составе дистрибутива операционной системы (архив deploy.cab в папке \Support\Tools) присутствует программа setupmgr, которая позволяет сформировать файл ответов, который может быть использован при автоматической установке (рис. 14.1).

Программа снабжена подробной справочной системой и не нуждается в дополнительном описании.

Установка прикладного ПО

Существенную часть затрат рабочего времени администратора составляет работа по установке программного обеспечения на рабочие станции пользователей: добавление новых программ, обновление существующих, распространение "заплаток" и т. п. Автоматизация этих операций позволяет уменьшить объем рутинных операций системного администратора, повысить качество обслуживания организации.

При внедрении автоматизированной установки прикладного ПО администратору приходится решать две проблемы: внедрения системы распространения

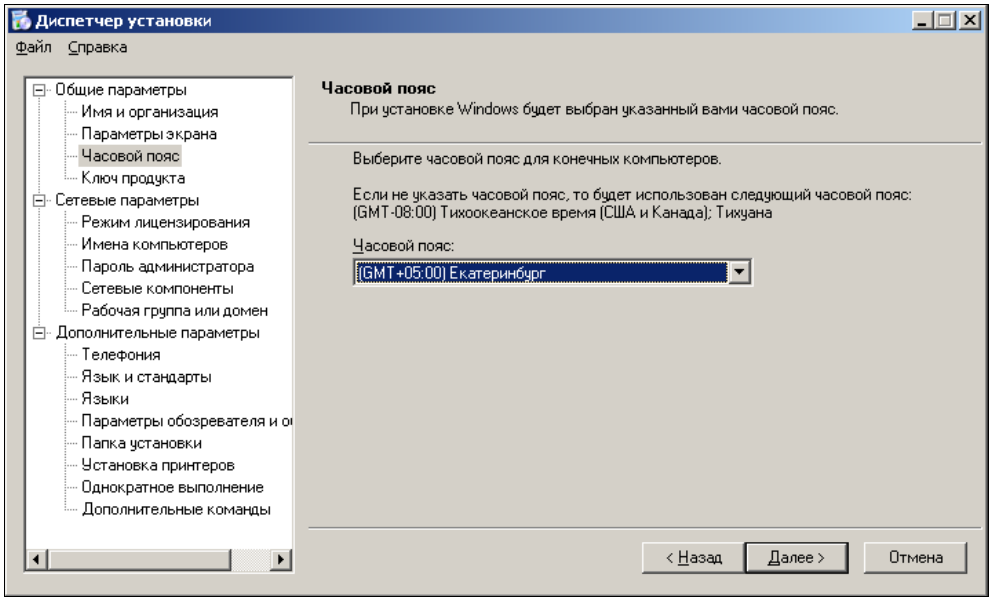


Рис. 14.1. Программа формирования файла ответов для автоматизированной установки

ПО и отработки технологии модификации установочных файлов для получения "тихой" инсталляции.

Сценарии разворачивания ПО (при входе в домен)

Существует большое количество коммерческих продуктов, предназначенных для развертывания ПО в компьютерной сети. Это решения от IBM (Tivoli), Computer Associates International, NetSupport, Microsoft, Novell и т. д. Как правило, они ориентированы на большие сети и экономически не оправданы при незначительном числе компьютеров в организации.

Однако последние версии Windows включают различные технологии, которые могут быть применены для запуска программ на клиентских компьютерах, что может быть использовано для установки и настройки ПО. Во-первых, это назначение сценариев, запускаемых при входе в сеть. Этот способ применим ко всем системам, настроенным для работы в домене Windows. Во-вторых, в доменах Active Directory можно использовать групповые политики для установки ПО на системы с Windows 200*x*/XP/Vista. В-третьих, можно создать сценарии для удаленного выполнения программ[1].

[1] Для систем Windows 9*x* в этом случае может понадобиться предварительная установка Windows Scripting Host *(см. главу 13, разд. "Windows Scripting Host")*. Существуют и другие языки макропрограммирования, которые могут быть использованы администратором для таких операций. Обычно это зависит от предыдущего опыта администратора, от знания им конкретного языка.

Можно использовать возможности имеющихся программ сетевого управления. Так, автору известен случай, когда для установки ПО применялся MOM-сервер *(см. разд. "Контроль функционирования систем. Microsoft Operation Management Server" главы 13)*: для выполнения сценариев были использованы агенты MOM клиентских компьютеров.

Безусловно, специализированные продукты предоставляют администратору существенно больше возможностей. Так, с помощью SMS можно пересылать установочные файлы в удаленные офисы в период минимальной загрузки канала, контролируя при этом использование его полосы пропускания; при выборе систем для установки легко использовать различные критерии отбора: версии программ, свободные объемы жестких дисков, конкретные модели установленных в компьютер устройств и т. д. SMS автоматически собирает информацию о ходе распространения ПО и отображает ее в удобном виде. В то же время многие функции подобных систем в малых организациях остаются невостребованными.

Сценарии входа в сеть позволяют устанавливать любое ПО на системы с Windows 9*x*; в случае Windows NT будут успешно выполнены те задания, для которых достаточно прав учетной записи входящего на компьютер пользователя. Распространение программ с помощью групповых политик позволяет предоставить пользователю на время установки дополнительные права[1], но такое решение применимо только для систем с Windows 200*x*/XP/Vista.

С помощью индивидуального сценария можно выполнить удаленно программу на системах с Windows NT/200*x*/XP/Vista. Кроме того, в Интернете несложно найти программы, которые упрощают многие настройки при разработке подобных сценариев. В любом случае выбор оптимального варианта определится особенностями конкретной организации.

Одной из проблем распространения ПО является анализ результатов установки. Специализированные серверы (SMS, Tivoli и т. п.) позволяют администратору получить информацию о результатах установки программ. В иных случаях администратору следует настраивать установку ПО на использование протоколирования, а затем собирать и анализировать файлы протоколов.

---

[1] Технология повышения уровня привилегий (elevated privilegies) используется в случае *управляемых установок*. В их число входят установки с помощью групповых политик и SMS 2003. В этом случае учетная запись пользователя, запустившего такую установку, получает для необходимых операций права локальной системной учетной записи. Реализуется это путем взаимодействия процесса msiexec, запущенного от имени пользователя, с процессом msiexec, выполняющимся от имени учетной записи системы.

Варианты запуска программы установки

Административная установка

В организациях часто используют *административную установку*. Административная установка подразумевает перенос дистрибутивных файлов продукта на какую-либо сетевую папку с одновременным внесением настроек, специфичных для данной организации. Так, многие программы имеют функцию установки отдельных компонентов "по требованию" (при первом обращении). Вы можете включить в административную установку указание на несколько сетевых путей, где будут храниться файлы дистрибутива. В результате при попытке добавления компонента инсталлятор проверит несколько сетевых папок и не сообщит об ошибке, если одна из них недоступна в текущий момент. Вы также можете включить в установку, например, указание параметров подключения почтового клиента к серверу Exchange. Таким образом пользователи, первый раз запускающие Outlook, автоматически увидят свой почтовый ящик без необходимости промежуточных шагов настройки подключения.

Административная установка выполняется с помощью ключа `/a`. При этом следует применять файлы трансформаций, описание которых приведено далее.

"Тихая" установка

"Тихой" (silent) называют такую установку, которая не требует от пользователя ввода каких-либо данных в процессе инсталляции. Поэтому тихая установка может быть полностью выполнена в автоматическом режиме.

Для исключения ответов пользователя можно применять различные подходы: специальные ключи командного файла, предварительно подготовленные файлы ответов, переупаковку программы установки.

Ключи командных файлов установки

Если иное не предусмотрел разработчик программы, то установочные файлы обычно имеют ключи командной строки, позволяющие выполнить установку в тихом режиме. В этом случае используются настройки установки по умолчанию. К сожалению, синтаксис командных строк инсталляторов различных разработчиков отличается друг от друга.

Примечание

Если в процессе установки возникла ситуация, требующая введения пользователем дополнительной информации, то программа покажет соответствующее диалоговое окно.

Стандартным для установочных файлов программ Windows является формат MSI. Формат инсталлятора подробно описан разработчиком и фактически является открытым стандартом. Для файлов в этом формате предусмотрен ключ тихой установки `/q`. При этом следует использовать следующий синтаксис запуска[1]:

```
msiexec /i <имя_файла_дистрибутива.msi> /qn
```

Если стандартный MSI-дистрибутив запускается файлом setup.exe, то следует использовать такую строку:

```
setup.exe /s /v"/qn"
```

Дистрибутивы, подготовленные с помощью популярного продукта InstallShield, имеют ключ тихой установки `/s`. Тихая установка требует наличие файла ответов. Если он отсутствует в составе дистрибутива, то пользователь может создать его самостоятельно, записав свои действия в качестве варианта ответов во время тестовой установки продукта. Для этого необходимо использовать режим записи ответов[2] с ключом `/r`:

```
setup.exe /r /f1
```

По умолчанию файл ответов должен иметь имя setup.iss и располагаться в той же папке, что и setup.exe. В противном случае при запуске тихой установки (с ключом `/s`) следует указать путь к нему в ключе `/f1`.

Примечание

Программа инсталлятора может закрыться раньше, чем установка продукта будет полностью завершена. Если вы используете последовательность сценариев установки, то это может привести к ошибке их выполнения. В такой ситуации следует добавить ключ `/sms`, который заставляет программу инсталлятора ждать полного окончания установки продукта.

В последнее время приобрели популярность так называемые PackageForTheWeb-дистрибутивы (PFTW). Эти пакеты представляют собой один самораспаковывающийся файл, который после разархивирования автоматически запускает программу setup.exe, содержащуюся в этом архиве. PFTW допускают использование двух ключей. Ключ `/s` осуществляет "тихое" разворачивание дистрибутива, а ключ `/a` "передает" последующие ключи программе setup.exe. Например, вы можете использовать запуск PFTW с ключами `/s /a /r` для того, чтобы создать файл ответов.

---

[1] В примере использован также ключ `/n`, наличие которого позволяет выполнить установку скрыто, без интерфейса пользователя.

[2] Ключ `/f1` можно не указывать в командной строке. В этом случае файл ответов будет записан по умолчанию в папку Windows и иметь имя setup.iss. Аналогично, если вы не используете для файла ответов имя по умолчанию, то его необходимо указать с ключом `/f1` при запуске тихой установки.

Примечание

Большая база рекомендаций по развертыванию популярных продуктов (возможные ключи запуска и трансформаций, советы по переупаковке и т. д.), доступна на сайте AppDeploy (**http://www.appdeploy.com/packages/index.asp**).

Файлы ответов

Наиболее корректным вариантом подготовки дистрибутива к тихой установке является формирование файлов ответов (или *трансформаций*, transform, MST-файлы). Преимущество использования MST-файлов состоит в том, что исходный продукт не подвергается каким-либо изменениям в процессе подготовки к развертыванию. При этом файлов трансформаций может быть создано сколь угодно много — для любого варианта установки продукта.

Подробными описаниями синтаксиса файлов ответов снабжены основные продукты Microsoft (операционная система, продукты MS Office и т. д.). Некоторые программы, например MS Office 2003 (в составе Resource Kit), имеют специальные мастера, которые позволяют настроить файлы трансформации установки. Администратору достаточно выбрать в графическом режиме желаемые параметры установки, чтобы создать файл трансформации для тихой установки продукта. Но, к сожалению, большинство программ, с которыми приходится сталкиваться на практике, не имеют такого описания или мастера создания ответов.

Если не удается найти инструкции по составлению трансформаций у изготовителя продукта, то можно воспользоваться программами для редактирования установочных файлов[1] (рис. 14.2). Как правило, эти программы либо записывают ответы пользователя во время тестовой установки, либо позволяют отобразить структуру файла MSI, назначить необходимые параметры, скрыть диалоговые окна и т. п.

Примечание

Если в процессе подготовки файлов трансформаций не были заданы все параметры, то могут возникнуть ситуации, когда программа выведет диалоговое окно для получения дополнительной информации установки. Если установка должна выполняться скрытно и не от имени учетной записи текущего пользователя, то подобная ситуация может привести к сохранению остановившейся программы в памяти системы сколь угодно долго.

Кроме файлов ответов можно использовать программы, моделирующие нажатие клавиш и движения мыши.

[1] Не забывайте, что есть программы, преобразующие исполняемые файлы установки (setup.exe) к виду *.msi.

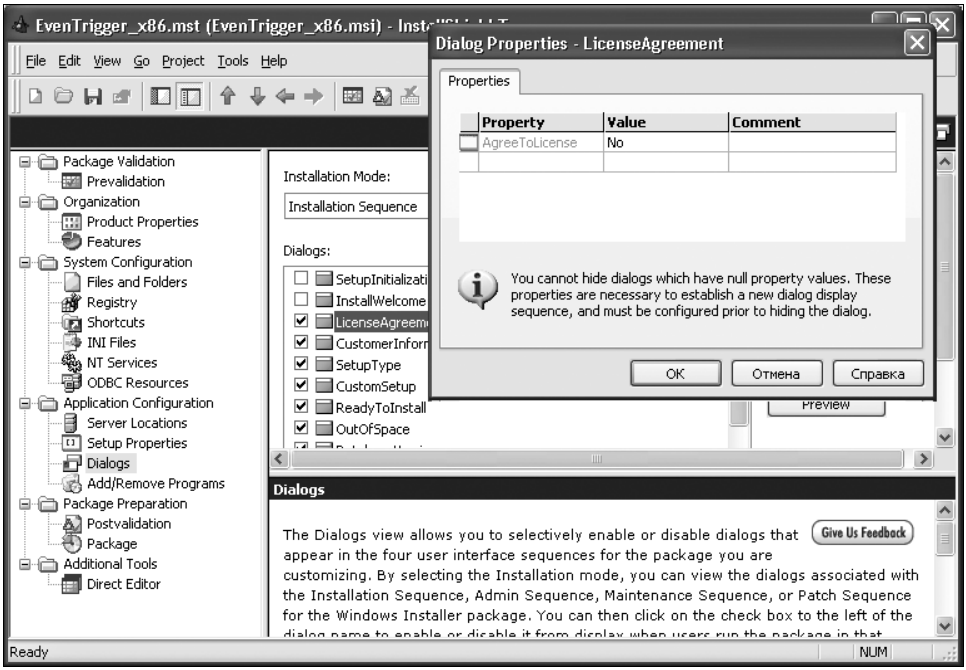


Рис. 14.2. Редактирование установочного файла с помощью специализированной программы

Переупаковка

Первой технологией, предназначенной для массового развертывания программ, была *переупаковка* (repackages).

Технология переупаковки заключается в том, что специальная программа контролирует изменения, вносимые установкой на тестовый компьютер: следит за изменениями файловой системы, ветвями реестра, другими параметрами. После чего сравнивается состояние системы *до* установки программы и *после*. Все обнаруженные различия анализируются и создается *новая* программа установки.

Существует и вторая технология, используемая для переупаковки. Это мониторинг процесса инсталляции. Специальная программа следит за всеми действиями процесса установки; например, ею будет замечено любое обращение к реестру системы с целью проверки существования какого-либо параметра. Мониторинг позволяет создать более точный файл переупаковки, но эта технология содержится только в коммерческих версиях программ.

Допустимые для переупаковки продукты

Не все дистрибутивы допускают переупаковку. Во-первых, нельзя переупаковывать сервис-паки, горячие заплатки и другие продукты, вносящие изме-

нения в операционную систему (например, DirectX). Такие программы могут выполнять специальные процедуры, например, прямое редактирование двоичных файлов, которые не могут быть верно воспроизведены процедурой переупаковки.

Во-вторых, переупаковка продуктов, устанавливающих драйверы устройств, сетевые протоколы и другие системные агенты, часто не приводит к успеху. В-третьих, переупакованный дистрибутив не сможет заменить файлы, защищаемые технологией Windows File Protection. Такие изменения "разрешены" только для программ изготовителя операционной системы.

Конечно, не имеет смысла переупаковывать продукты, содержащие мастера настройки (как упомянутый MS Office) или Internet Explorer и т. п.

Преимущества процесса переупаковки

Переупаковка достаточно просто реализуется при помощи бесплатных утилит. В этом процессе от администратора требуется меньшее вмешательство: достаточно проконтролировать зафиксированный перечень изменений и отказаться от шагов, которые могли быть вызваны фоновой активностью системы (рис. 14.3).

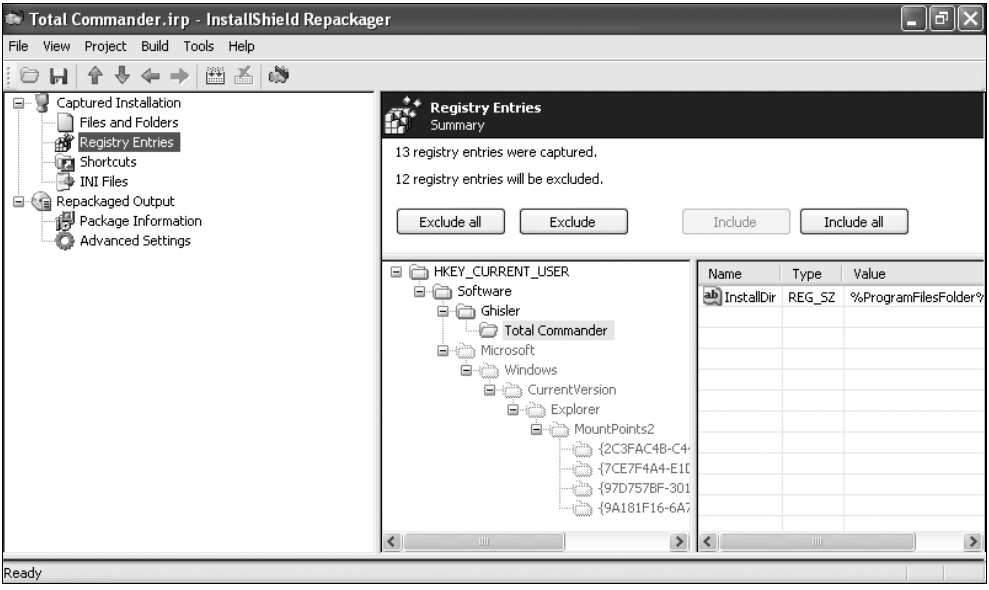


Рис. 14.3. Программа показывает изменения, которые вносит программа установки в настройки системы

Переупаковка позволяет включить в один дистрибутив несколько последовательно устанавливаемых продуктов. Достаточно запустить до второго скани-

рования системы необходимое число программ. Кроме того, с помощью переупаковки легко выполнить пользовательские настройки. Для этого необходимо до начала анализа запустить на тестовом компьютере установленную программу, настроить ее и сохранить изменения. Все эти изменения войдут в переупакованный дистрибутив.

Продукты для подготовки установочных файлов

Очевидно, что для выполнения упомянутых операций редактирования, настройки, преобразования, переупаковки и других операций с файлами дистрибутива администратору необходимы специализированные средства.

В составе дополнительных утилит для Windows 2000 есть программа WinINSTALL, которую можно использовать для переупаковки. В дистрибутиве Windows 2003 Server она отсутствует, но новую ее версию, которая также бесплатна, легко найти в Интернете: программа WinINSTALL LE 2003 (фирма OnDemand Software) доступна для загрузки по адресу **http://www.ondemandsoftware.com/**. WinINSTALL LE 2003 предназначена для создания и редактирования пакетов установок; с ее помощью можно редактировать не только файлы MSI, но и пакеты обновлений, установки MSM (Merge Modules) и т. п.

Если администратор использует SMS, то он может бесплатно загрузить специальную[1] версию InstallShield AdminStudio:
http://www.microsoft.com/downloads/details.aspx?familyid=925412e6-5350-455b-a973-fabec35462e5&displaylang=en.

Полная версия InstallShield AdminStudio, на взгляд автора, является самой функциональной среди аналогичных продуктов, с которыми ему пришлось столкнуться.

Бесплатную программу от Wise (Wise InstallTailor) можно загрузить по следующей ссылке: **http://www.wise.com/installtailor_formframe.asp**.

Обратите внимание, что программами для редактирования своих установочных файлов часто снабжаются корпоративные версии ПО. Например, для настройки параметров установки Adobe Acrobat можно использовать специальную утилиту изготовителя InstallShield Tuner:
(**http://www.adobe.com/support/downloads/detail.jsp?ftpID=2709**).

Можно применить и коммерческие версии соответствующих продуктов редактирования, ссылки на которые легко найти на упомянутых выше страницах.

---

[1] Некоторое неудобство представляет объем загрузки — около 300 Мбайт. Фактически копируется полная версия; варианты (ограниченная SMS или полная версия) отличаются только вводимым серийным номером при установке продукта.

Тестирование сценариев установки

Переупаковку можно использовать только для установки продукта на сходные системы. Желательно, чтобы на тестовом компьютере стояла "чистая" операционная система: не было никаких других программ, кроме требуемых для инсталляции переупаковываемого продукта, и не исполнялись никакие фоновые процессы. Если в системе, на которой производился анализ процесса установки, остались "следы" каких-либо предыдущих установок, то соответствующие изменения могут быть не обнаружены и не включены в переупакованный файл. Например, если некая программная библиотека ранее была установлена другим продуктом, то программа установки "увидит" ее в системе и не будет добавлять. В результате на другой системе без этой библиотеки продукт, установленный с переупакованного таким образом дистрибутива, работать не будет.

Ограничения устанавливаемого ПО

Для развертывания в организации подходят не все программы. Например, если программа требует индивидуального серийного номера для каждого компьютера, то массовая ее установка становится существенно затрудненной. Поэтому для организаций применяются так называемые *корпоративные версии*.

Обычно корпоративные версии оптимально приспособлены для массового развертывания[1]. Программы установки имеют необходимые ключи тихого выполнения, для всех компьютеров применяется единый серийный номер, программа после установки не требует активации и т. п. Упомяну такие корпоративные продукты, как Windows XP/2003, Microsoft Office, Symantec AntiVirus и т. д.

Понятно, что в некоторых ситуациях административное развертывание программы невозможно. Обычно это касается программ с той или иной защитой. Например, если для завершения установки необходим индивидуальный ответ от изготовителя ПО, формируемый на основе сообщаемых данных конкретной системы.

Клонирование рабочих станций

Клонирование представляет собой процесс воспроизведения данной системы на другом рабочем месте. Клонированная станция будет иметь аналогичную версию операционной системы, те же установленные (и соответствующим

[1] Весьма часто опции развертывания такого ПО на клиентские компьютеры входят в меню серверной части программы.

образом настроенные) прикладные программы пользователей и т. п. К клонированию обычно прибегают при обновлении аппаратной части рабочего места (новый системный блок), при восстановлении "упавшего" компьютера, при создании типовых рабочих мест и т. д.

Существуют различные способы клонирования. Это и простое дублирование структуры жесткого диска, и тот или иной вариант удаленной установки (Remote Installation Service, Automated Deployment Services), и перенос настроек с одного компьютера на другой. Администратор выбирает тот вариант, который оптимальным образом подходит для его системы.

Перенос информационной системы на новое оборудование

Модернизация рабочей станции может быть выполнена с использованием операций резервного копирования и последующего восстановления системы на новом системном блоке. Для этого следует вначале выполнить операцию резервного копирования системы. Затем для компьютера с новым системным блоком нужно установить аналогичную операционную систему с минимальным набором опций. После этого можно восстановить на нее данные и состояние системы из файлов резервного копирования. В этом случае операция восстановления *сохранит* новые драйверы.

Примечание

Восстановление должно проводиться на такую же конфигурацию логических дисков, что и в исходной системе. Так, если первоначально в системе присутствовало два жестких диска, то в новой системе следует разбить диск на два логических и дать им соответствующие имена.

Способ не оптимален по затрачиваемому времени, поскольку фактически предполагает установку "с нуля" и последующую инсталляцию всех прикладных программ. Однако он позволяет штатными средствами модернизировать оборудование компьютерной системы.

Перенос настроек на новые системы

При замене или обновлении компьютера обычно возникает задача переноса на новую систему всех старых пользовательских настроек, документов и т. п. Задача не вполне тривиальная, поскольку эта информация хранится в различных папках (не всегда в предусмотренных по умолчанию), пользователь использует уникальное ПО и т. п.

В составе Windows XP имеется встроенное средство для копирования пользовательских данных с одного компьютера на другой. Это мастер переноса файлов и программ. Данная программа копирует содержимое пользователь-

ской части реестра и специальных папок (таких как Мои документы). Если подобную операцию необходимо выполнить либо удаленно, либо одновременно для нескольких систем, то следует загрузить с сайта разработчика версию данной утилиты для администраторов. Она позволяет запускать операцию из командной строки с указанием соответствующих параметров.

Можно использовать в данных целях и утилиты третьих фирм. Например, программы для переноса настроек при миграции домена или при создании образов операционных систем (версии для предприятия программы GHost и т. п.).

Дублирование жесткого диска

Наиболее простой вариант создания копии данной системы заключается в дублировании структуры жесткого диска. Существует несколько программ, с помощью которых можно выполнить подобную операцию. Наиболее популярна программа GHost от Symantec, часто используют также утилиты от Acronis (**http://www.acronis.ru/**).

Структуру жесткого диска можно копировать непосредственно с диска на диск как на одном компьютере, так и на различных системах при подключении через COM-, LPT-, USB-порты или сеть. Можно сохранить образ диска в виде файла и использовать этот файл для последующего создания копий дисков.

Поскольку при шифровании данных применяется уникальный идентификатор безопасности, который заменяется программами дублирования диска, то для сохранности информации *все зашифрованные файлы необходимо расшифровать перед клонированием*.

Удобно осуществлять подключение к другим системам с помощью загрузочных дисков, подготовленных в корпоративных версиях соответствующих программ (рис. 14.4). Замечу, что корпоративные версии программ позволяют использовать как возможности загрузки стартовой дискеты по сети (для сетевых адаптеров, поддерживающих PXE-стандарт), так и предлагают иные специальные варианты выполнения операции. Например Symantec GHost CE позволяет автоматически создавать виртуальные разделы (DOS или PS DOS), после загрузки с которых программа дублирования получает полный доступ как к жесткому диску, так и к различным сетевым устройствам с файлами-образами дисков.

Если дублирование диска проводится для замены одного жесткого диска на другой, то никаких проблем не возникает. Если же жесткий диск перенести из одного компьютера в другой, то обычно успешно загрузиться новому компьютеру не удастся.

Рис. 14.4. Мастер создания загрузочного диска.
Мастер помогает создать дискету, после загрузки с которой можно осуществить дублирование жесткого диска с подключением к другому компьютеру. В случае необходимости создается индивидуальный образ с использованием драйверов сетевого адаптера от изготовителя оборудования

Для систем на базе ядра Windows NT простая перестановка жесткого диска обычно заканчивается "голубым экраном смерти" (BSOD). Происходит это, в основном, по причине отличающихся драйверов доступа к жестким дискам и различия библиотек доступа к оборудованию компьютера — HAL (Hardware Abstraction Layer)[1]. Рекомендуемый способ действий в этих случаях — подготовка дисков с помощью программы `sysprep` *(см. разд. "Использование утилиты sysprep" далее в этой главе)*, но на практике к успеху часто приводят и варианты, описанные далее.

Замена IDE-драйверов на стандартные

Если BSOD при установке жесткого диска в новый системный блок связан с различающимися IDE-драйверами, то часто самым быстрым способом подготовки диска к установке на новом компьютере является замена таких драйверов на стандартные.

Для этого перед переносом жесткого диска на другой компьютер следует заменить драйвер IDE-контроллера в Диспетчере устройств на стандартный и

[1] Выделяют три основных типа компьютеров, которым требуются отличающиеся HAL. Это Standart PC, ACPI PC, ACPI Uniprocessor PC. Кроме того, HAL отличаются для одно- и многопроцессорных систем. Компьютерные бренды могут иметь собственные коды, поставляемые производителями.

удалить все драйверы, специфичные для данной материнской платы. Затем установить диск в новый блок и попытаться загрузить систему.

Замена HAL

Разработчик не предусматривает никаких средств для смены HAL[1]. В общем случае необходимо выполнить чистую установку операционной системы. В то же время на форумах Интернета можно встретить следующую рекомендацию. Скопируйте в системный каталог (из дистрибутива) файлы HAL для различным систем и модифицируйте меню загрузки[2] следующим образом:

```
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS ="Standart PC" /fastdetect
/hal=halstd.dll
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS ="ACPI PC" /fastdetect
/hal=halacpi.dll
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS ="ACPI Uniprocessor PC"
/fastdetect /hal=halmacpi.dll
```

После чего можно попытаться выбрать различные варианты загрузки и, в случае успеха, соответствующим образом модифицировать выбор по умолчанию.

Утилита *sysprep*

Рекомендуемый вариант подготовки жесткого диска к установке на другом компьютере (клонированию) состоит в использовании утилиты `sysprep`[3], поставляемой в составе дистрибутива системы. Утилита находится в папке Support\Tools\ установочного компакт-диска системы в архиве deploy.cab.

Программа `sysprep` предназначена для подготовки жесткого диска к клонированию. Практически она "возвращает" программу установки на несколько шагов назад, при этом допустимо использовать все возможности автоматизации инсталляции: создать файл ответов, добавить новые, отсутствующие в дистрибутиве драйверы устройств, выполнить после завершения процесса определенные программы и т. д.[4] Установленные на исходном компьютере

---

[1] Допустима только замена определенных типов HAL на другие. Эта операция проводится при помощи Диспетчера устройств. См. KB309283.

[2] В конкретном случае, может быть, придется исправить параметры системной партиции (`multi(0)disk(0)rdisk(0)partition(1)`) и сервис-паки установки Windows (в случае других путей установки системы).

[3] Версии утилиты отличаются для различных операционных систем. При возможности следует всегда использовать наиболее свежие версии. Например, начиная с версии 1.1, добавлена возможность обнаружения при завершении установки новых драйверов IDE-дисков. Проверить наличие новых версий необходимо на сайте изготовителя.

[4] Читатель может самостоятельно ознакомиться с возможностями программы, описанными в файле deploy.chm.

прикладные программы остаются работоспособными после операции клонирования.

Создание установочного образа системы при помощи утилиты *sysprep*

Для создания установочного образа системы при помощи утилиты `sysprep` выполните следующие действия:

1. Установите на типовой компьютер нужную версию операционной системы, последние обновления безопасности, все прикладное программное обеспечение (офис, антивирусное ПО, обозреватели Интернета третьих фирм и т. п.).
2. Создайте на диске (в корне) папку SYSPREP, запишите в нее утилиты Sysprep.exe и Setupcl.exe (эта папка после установки системы будет автоматически удалена).
3. Чтобы исключить запросы дополнительной информации после переноса диска на новый компьютер (например, запроса серийного номера Windows), создайте в папке SYSPREP файл ответов. Проще всего воспользоваться программой диспетчера установки (Setupmgr.exe). После генерации файла ответов желательно просмотреть его и включить дополнительные параметры, если это необходимо.
4. После сохранения файла ответов запустите программу `sysprep`[1]. По завершению ее работы можно перенести жесткий диск в новую систему и включить компьютер. Обычно через несколько минут система завершит процесс установки и будет полностью работоспособна.

Подготовка диска для существенно отличающейся системы

Описанными выше действиями создается образ системы, который можно развернуть на *аналогичные* конфигурации компьютеров, если после завершения работы утилиты `sysprep` сохранить образ жесткого диска в виде файла.

Однако комплектации рабочих станций в организации часто существенно отличаются друг от друга, а драйверы используемых в них устройств *не входят* в состав дистрибутива операционной системы. В этом случае необходимо специальным образом подготовить жесткий диск перед операцией клонирования[2].

---

[1] Если предполагается наличие не PnP-устройств, то используйте при запуске ключ `-pnp`. Это позволит обнаружить такие устройства на новом компьютере, но может существенно (до 20 минут) увеличить процесс установки.

[2] Можно воспользоваться утилитами редактирования файла образа диска, добавить в него необходимые папки и изменить соответствующим образом файлы настроек.

1. Чтобы sysprep "заставила" программу установки протестировать на новой системе все типы жестких дисков, следует включить в файл ответов такие строки:

```
[Sysprep]
BuildMassStorageSection = Yes
[SysprepMassStorage]
```

2. Чтобы добавить новые драйверы устройств, которые отсутствуют в дистрибутиве Windows, внутри[1] папки SYSPREP создайте папку с названием, например, Drivers. Для удобства можно сделать структуру папки разветвленной, например создать папки Drivers\Video, Drivers\Net и т. п. Скопируйте в эти папки OEM-драйверы устройств компьютеров вашей сети.

Примечание

По умолчанию драйверы должны содержать цифровую подпись изготовителя. В противном случае их установка будет отложена до первого входа администратора в систему. Если необходимо разрешить установку драйверов без цифровой подписи, то следует включить в секцию [Unattended] файла ответов строку DriverSigningPolicy = Ignore (как при использовании sysprep, так и RIS).

3. Дополните файл ответов Sysprep.inf в разделе [Unattended] ссылками на папку с драйверами по следующему образцу:

```
OemPnPDriversPath = <путь_к_папке_драйверов>;<путь_к_папке_драйверов>
```

Папки должны быть перечислены через точку с запятой. Например:

```
OemPnPDriversPath = "sysprep\Drivers\net; sysprep\Drivers\Video"
```

Желательно включить в образ максимальное число драйверов, чтобы обеспечить его универсальность.

После завершения этих операций запустите утилиту sysprep.

Создание файлов образов клонируемого диска

Сразу же после завершения работы программы sysprep следует с помощью одной из программ копирования диска создать его образ. Этот образ диска можно записать на сетевой ресурс, на несколько компакт-дисков и т. п. Впоследствии с данного образа можно клонировать жесткие диски для новых систем неограниченное количество раз. Причем, как уже говорилось выше,

[1] Можно разместить драйверы и в другом месте, соответственно подправив путь к ним в файле ответов. Например, в корневой папке жесткого диска. Причина размещения драйверов именно в папке SYSPREP — это автоматическое ее удаление после завершения установки системы.

при использовании корпоративных версий программ клонирования, данный образ можно восстанавливать по сети и на компьютер с отсутствующей операционной системой.

Клонирование компьютеров-членов домена

Членами домена Windows являются не только пользователи, но и компьютеры с операционной системой на основе Windows NT. Поэтому дублирование дисков не может проводиться для создания копий рабочих станций, являющихся *членами домена*, т. к. в домене не может быть двух идентичных учетных записей[1]. Необходимо сначала перевести компьютер в рабочую группу, после чего клонировать диски и добавить новые станции в домен.

Примечание

Программа `sysprep` автоматически меняет идентификатор компьютера. В случае использования программы при операции *модернизации* аппаратной части данного компьютера ее следует запускать с ключом `-nosidgen`.

Обратите внимание, что некоторые программы имеют специальные функции для клонирования дисков со станций, являющихся членами домена. Например, упоминавшаяся ранее программа Symantec GHost CE. При установке такой программы учетная запись, от имени которой она будет запускаться, наделяется правом добавления рабочих станций в домен. В результате появляется возможность клонирования диска и последующего автоматического добавления системы в домен за одну операцию. Пользователем данная операция воспринимается как клонирование станции-члена домена.

Автоматическая удаленная установка систем Microsoft

В составе Windows имеется два штатных средства для удаленной установки операционных систем. Это служба Remote Installation Service (RIS) и служба Automated Deployment Services (ADS).

Служба ADS предназначена для разворачивания серверов Windows 200*x*. Она устанавливается[2] только на Enterprise-версию Windows 2003 Server. В отличие от ADS, служба RIS позволяет устанавливать как серверные операционные системы Windows 200*x*, так и рабочие станции на основе Windows 2000/XP. Служба RIS входит в состав дистрибутива серверных операционных

[1] За исключением контроллеров домена, которые имеют одинаковый идентификатор SID.

[2] Установочные файлы не входят в состав дистрибутива и должны быть загружены с сайта разработчика.

систем Windows 200*x*[1]. Устанавливается она после выбора соответствующей опции в числе компонентов системы.

Примечание

Для установки Windows Vista используется новая версия системы. Мы не будем ее описывать, поскольку групповое разворачивание операционных систем Vista не стало актуальным и корпоративные пользователи весьма сдержанно внедряют эту версию в производственные условия.

Установка RIS

Служба RIS устанавливается только в домене Windows. Для ее работы необходим сервер DHCP (обычно используется на одном компьютере со службами RIS).

Для инсталляции RIS требуется логический диск, *отличный* от того, на котором установлена система. Кроме того, следует позаботиться о достаточном месте на этом диске, поскольку на нем будут храниться установочные файлы операционных систем.

Примечание

При установке RIS на компьютер добавляется специальная служба, которая исключает хранение двух копий одного и того же файла. Этим также экономится дисковое пространство. Следствием этого является необходимость использования для сервера RIS программы резервного копирования, совместимой с данной технологией (например, штатной программы `backup`).

Возможности RIS

RIS позволяет установить операционную систему в качестве члена домена вместе с прикладными программами, осуществив загрузку *по сети*. Поэтому для использования RIS необходимо наличие в компьютере либо сетевой карты, поддерживающей сетевую загрузку[2], либо одной из карт[3], для которой предусмотрено наличие специальной программы для загрузки с дискеты.

---

[1] Желательно использовать службы последних версий ОС. В противном случае необходимо ознакомиться со статьями онлайновой базы данных, поскольку после установки без дополнительных обновлений служба RIS из состава Windows 2000 Server недостаточно функциональна.

[2] Если драйверы такой карты не входят в состав дистрибутива операционной системы, то они должны быть как включены в состав OEM-драйверов, так и скопированы в папку i386 существующего образа установки.

[3] Перечень таких карт выводится программой подготовки такой загрузочной дискеты от компании 3Com — `rbfg` (программа копируется в папку RemoteInstall\Admin\i386 сервера RIS). Это в основном модели сетевых адаптеров известных производителей — 3Com, Intel, Realtek, SMC. Необходимо использовать версию `rbfg` из состава Windows 2003 Server, поскольку она поддерживает большее количество сетевых адаптеров. В Сети можно найти также аналоги этой утилиты, поддерживающие несколько увеличенный список сетевых карт. Но это уже коммерческие версии программы.

Служба RIS работает следующим образом. При попытке сетевой загрузки клиент получает от сервера DHCP IP-адрес и адрес TFTP-сервера, с которым пытается соединиться. После этого с сервера TFTP на компьютер загружается программа, которая проверяет параметры пользователя (его права на установку системы) и производит копирование данных образа операционной системы (при необходимости сформированного вместе с установленными прикладными программами) на локальный диск. После завершения копирования осуществляется обнаружение PNP-устройств и завершение установки.

Добавление образов операционных систем в RIS

Образы операционных систем добавляются в службу двумя способами. Первый — это размещение в RIS дистрибутивов "чистой" операционной системы[1]. Операция выполняется с помощью консоли управления службой RIS и не представляет никакой сложности.

В оснастке управления RIS можно добавить новый образ установки непосредственно с дистрибутива. Это нужно выполнить только один раз для каждой версии операционной системы.

Права на установку с помощью RIS могут быть предоставлены только отдельным пользователям. При этом пользователь будет видеть в своем списке установок только те варианты, которые ему разрешил администратор. Для этого фактически осуществляется назначение прав доступа к файлу конфигурации. Это можно сделать как из данной программы, так и любым другим способом редактирования прав доступа к файлу.

Второй способ предусматривает размещение в RIS образа системы *вместе со всем установленным прикладным программным обеспечением*: программами офиса, антивирусным ПО, прикладными утилитами и т. п. Чтобы создать в RIS такой образ, необходимо:

1. Разместить (так, как описано выше) установочный образ операционной системы на том же языке.
2. Установить на эталонный компьютер эту операционную систему и все прикладные программы.
3. Создать образ данной установки и скопировать его на сервер RIS.

Создание образа системы и копирование его на сервер осуществляется с помощью программы Riprep.exe. Достаточно просто запустить ее (лучше сде-

[1] Желательно, конечно, предварительно встроить в дистрибутив последний сервис-пак. Эта операция выполняется запуском сервис-пака с ключом `/s:`*`путь`*, где *`путь`* — путь к папке с исходным дистрибутивом (обычно i386). Кроме того, в образ можно добавлять впоследствии и новые исправления (hotfixes), которые будут автоматически устанавливаться в завершении процесса (подробности можно изучить в *разд. "Предварительная установка исправлений"* файла deploy.chm).

лать это непосредственно с сервера RIS — программа находится в папке \\<*имя_RIS-сервера*>\Reminst\Admin\I386) и ответить на все вопросы мастера создания образа. Для сохраненных образов администратор может налагать права доступа с целью разрешить установку соответствующих версий только конкретным пользователям домена.

Примечание

Параметры установки операционной системы определяются значениями, заданными в файле ответов — Ristndrd.sif (это название такого шаблона в случае использования RIS). Фактически это аналог файла ответов unattended.txt, и вы можете воспользоваться соответствующими описаниями для точной настройки процесса установки. Например, можно ввести серийный номер Windows или удалить все имеющиеся на диске разделы и создать один логический диск с желаемым типом файловой системы.

Подготовка образов для RIS

Во-первых, для использования RIS администратор должен создать образ установки для каждого типа систем: выполнить все инсталляции и сохранить образы для Standart PC, ACPI PC и ACPI Uniprocessor PC. И если в организации используется несколько вариантов установок, то их количество, соответственно, должно быть утроено — для каждого варианта аппаратной части должен быть создан *свой образ системы*.

Во-вторых, подготовленные образы должны быть дополнены драйверами всех тех устройств, которыми комплектуются новые компьютеры. Так, в обязательном порядке следует добавить драйверы сетевых устройств, которые используются при загрузке по сети, если они не включены в состав дистрибутива.

Примечание

Установка видеоадаптеров часто выполняется с помощью программы установки. Такую операцию придется производить вручную после загрузки операционной системы (или включить ее в число автоматически запускаемых после установки программ).

Добавить драйверы новых устройств в установочный образ наиболее удобно редактированием RIS-установки:

1. Создайте папку oem\$1[1] на том же уровне, что и папка i386 (на сервере RIS) установки соответствующего варианта ОС.

[1] Это имя одной из специальных папок, используемых во время установки системы. См., например, описание "Distribution Folder Structure" на **http://www.microsoft.com/resources/documentation/Windows/XP/all/reskit/en-us/prbc_cai_zrlx.asp**.

2. Создайте в \$oem\$\\$1 необходимую структуру папок с драйверами (\$oem\$\\$1\Drivers\Net и т. п.) и укажите путь к ним в файле Ristndrd.sif в секции `[Unattended]`. Кроме того, включите опцию необходимости использования дополнительных драйверов (`OemPreinstall = Yes`). В результате секция `[Unattended]` должна начинаться таким образом:

```
[Unattended]
OemPreinstall = Yes
OemPnPDriversPath = "Drivers\net; Drivers\Video"
```

Примечание

Не забывайте про строчку `DriverSigningPolicy = Ignore` в случае отсутствия электронной подписи у драйвера устройства *(см. примечание в разд. "Подготовка диска для существенно отличающейся системы" ранее в этой главе)*.

Есть одна особенность добавления драйвера новой сетевой карты для RIS-установки. Чтобы система могла осуществить загрузку по сети с помощью неизвестного сетевого устройства, его драйверы нужно скопировать не только в папку \$oem\$ данной установки, но и в папку I386 соответствующего образа операционной системы (того, который добавлен из консоли управления RIS непосредственно с дистрибутива Windows; часто называют flat-образом).

Внесенные таким образом изменения в образы установок операционных систем начинают действовать после перезапуска службы BINL (`net stop binlsvc` и потом `net start binlsvc`).

Сравнение различных вариантов клонирования систем

Если сравнивать время операций, то установка с использованием RIS происходит медленнее, чем клонирование образа жесткого диска, прежде всего, за счет копирования по сети большого количества отдельных файлов.

Кроме того, RIS работает с достаточно ограниченным списком сетевых адаптеров, не поддерживает многие адаптеры ноутбуков[1], тогда как корпоративные программы клонирования позволяют использовать любые сетевые карты — в крайнем случае допустима загрузка с дискеты или компакт-диска.

Поскольку образы дисков можно хранить на сетевых устройствах, то особых проблем с их редактированием не возникает (структура установок RIS доступна непосредственно, образы дисков можно редактировать специальными

[1] При этом можно использовать один и тот же адаптер не более двух раз для установки станций-членов домена, иначе установка будет просто "зависать" после предложения нажать клавишу <F12>.

утилитами). В то же время объем хранимых данных в случае RIS существенно меньше, тогда как средний образ клонируемого диска будет занимать порядка 1,8 Гбайт.

Клонированием диска можно воспользоваться практически в любой ситуации (независимо от наличия домена, сервера RIS и т. п. — достаточно образа на компакт-диске и программы клонирования, умещающейся на одной дискете). В то же время установка станции с использованием RIS не требует участия системного администратора, достаточно предоставить права на установку тем или иным пользователям.

Кроме того, RIS входит в состав дистрибутива серверных систем, а корпоративные программы клонирования необходимо приобретать за отдельную плату.

Примечание

При практическом использовании RIS автор встретил несколько случаев, когда после копирования по сети установочных файлов система не могла загрузиться с локального жесткого диска. Описания причин такой неисправности в свое время не были найдены на сайте разработчика, причем последующее копирование образа диска с установленными программами с помощью Ghost создавало нормальную работоспособную систему.

Я описал некоторые отличия программ клонирования. Конечно, у каждого администратора будут свои причины выбора предпочтительного варианта установки.

Приложение

Обязанность контроля функционирования информационной системы влечет за собой выполнение ряда рутинных операций. Их состав специфичен для каждого предприятия. Однако я попытаюсь привести примерный шаблон, на основе которого может быть составлен конкретный план периодических мероприятий. Удобно, если этот план будет выполнен в виде соответствующего перечня, выполнение каждого пункта которого будет отмечаться в этом же документе.

Примечание

В данном плане приводятся только позиции, которые следует проверить администратору. Естественно, что обнаружение каких-либо ошибок предполагает соответствующие действия администратора по ликвидации проблемы.

Ежедневные операции

Ежедневные операции направлены, в первую очередь, на контроль текущего состояния информационной системы. Каждая позиция данного шаблона должна быть дополнена конкретными операциями проверки.

- **Оценка внешнего состояния серверов и окружающей среды.**

  Администратору необходимо оценить температуру вокруг серверов, проверить отсутствие внешних признаков вскрытия корпусов, состояние кабельной системы и т. д.

- **Проверка функционирования основных служб информационной системы.**

  Администратор обязан проверить состояние всех основных служб системы: работоспособность канала Интернета, возможность приема и отправки сообщений электронной почты, отклики от информационного сервера Интернета предприятия и т. д. Объем подобных операций зависит от состава информационной системы.

- **Оценка показаний датчиков аппаратного контроля.**

  Серверные платформы оснащены датчиками, позволяющими контролировать температурный режим внутри корпуса, параметры электропитания, частоту вращения вентиляторов, состояние RAID-контроллеров. Администратору необходимо убедиться, что соответствующие показания находятся в допустимых диапазонах.

- **Проверка результатов выполнения операций резервного копирования.**

  Следует убедиться, что *все* операции резервного копирования завершились успешно и без каких-либо сообщений об ошибках. Особо хочется обратить внимание, что контролю подлежат все операции резервного копирования: выполняемые как системными средствами, так и внутренними операциями прикладного программного обеспечения.

- **Проверка результатов обновления антивирусных баз.**

  Несмотря на то, что по умолчанию многие антивирусные программы предлагают недельный график обновления, автор советует запланировать данную операцию на каждый день и регулярно проверять ее итоги.

- **Проверка результатов иных плановых операций в системе.**

  В информационной системе могут существовать иные операции, выполняемые по специальным графикам. Например, мероприятия по оптимизации баз данных SQL-сервера, формирование отчетов статистики использования Интернета и т. п. Администратору следует проверить итоги выполнения таких операций.

- **Проверка содержимого протоколов работы серверов.**

  Администратор должен просмотреть и проанализировать протоколы работы всех серверов информационной системы, в первую очередь обращая внимание на протоколы системы безопасности и на сообщения об ошибках или предупреждения. Следует отметить, что и чисто информационные сообщения могут существенно помочь опытному администратору в предупреждении аварии.

- **Проверка доступного объема жестких дисков.**

  Необходимо проверить наличие на основных производственных серверах[1] достаточного свободного объема дискового пространства, которое позволит продолжить нормальное выполнение бизнес-операций.

---

[1] Это требование относится к тем серверам, объем информации на которых может меняться. Например, почтовый сервер (прием большого числа сообщений), файловый сервер (пользователи перенесли на него существенный объем данных), сервер баз данных (разработчики изменили структуру информации, вследствие чего размер баз существенно вырос) и т. п. Естественно, что для серверов, выполняющих такие функции, как маршрутизация сетей и т. п., данный контроль не актуален.

- **Проверка работы служб систем.**

  Администратор должен проверить, что все автоматически запускаемые службы[1] *всех* серверов информационной системы находятся в состоянии *"работает"*.

Еженедельные операции

В группе еженедельных операций представлены задачи, которые администратор должен выполнять несколько раз в месяц. Конкретная периодичность — раз в неделю или раз в две недели — должна быть определена в зависимости от специфики информационной системы.

- **Формирование отчета.**

  Хотя это чисто организационное предложение, наличие периодического отчета системного администратора, с одной стороны, стимулирует самого администратора, с другой — позволяет держать руководителя в курсе состояния информационной системы.

- **Очистка фильтров вентиляторов охлаждения.**

  Практика показывает, что в условиях обычного учреждения воздушные фильтры "забиваются" уже через одну-две недели. В связи с этим следует еженедельно очищать фильтрующие элементы как всего помещения, так и на корпусах оборудования (конечно, если соответствующие фильтры предусмотрены).

- **Проверка производительности серверов.**

  Администратору необходимо проверить параметры производительности серверов системы и проанализировать их изменения по сравнению с прошлыми периодами. В случае снижения параметров — принять меры по поддержанию необходимого уровня обслуживания пользователей.

Плановые операции другой периодичности

Администратору не следует забывать и о тех работах, выполнять которые ему приходится достаточно редко. Следующие работы можно запланировать, например, в квартальном или полугодовом планах.

- **Установка обновлений.**

  Администратор должен периодически проверить наличие обновлений для всего программного обеспечения, используемого в организации. Даже

[1] Существуют службы, которые автоматически запускаются и впоследствии останавливаются. Но я не буду особо заострять на этом внимание.

если в организации реализована система текущего обновления безопасности, необходимо убедиться в отсутствии обновлений, которые не охватываются ею.

- **Очистка оборудования от пыли.**

  Обычно данную операцию совмещают с проведением на оборудовании тех или иных работ, поскольку при этом обычно предполагается отключение электропитания. Периодичность работ определяется качеством окружающей среды, и при отсутствии специальных мер по фильтрации воздуха данная операция должна выполняться не реже одного раза в два-три месяца.

- **Выполнение комплекса работ по полному восстановлению системы.**

  Крайне важно, чтобы специалист мог оперативно выполнить комплекс работ по полному восстановлению информационной системы после аварийной ситуации. Поэтому в организации должны быть запланированы работы по восстановлению тестовой системы на основе тех резервных копий, которые создаются в плановом порядке.

- **Планирование развития.**

  По итогам загруженности информационной системы за некоторый период администратор может предположить о дополнительных ресурсах, которые могут потребоваться для дальнейшего нормального функционирования системы (например, приобретение дополнительного жесткого диска). Соответствующие предложения должны быть направлены руководителю.

План-отчет операций

На основе приведенного выше плана мероприятий следует составить список конкретных текущих операций администратора. При этом каждая позиция должна быть пооперационно развернута в соответствии со спецификой информационной системы примерно в следующем виде, позволяющем непосредственно в бланке отмечать результаты проверки каждого пункта (табл. П1).

Заполненный администратором отчет будет являться документом, по которому можно оценить как работу специалиста, так и объективно проанализировать состояние системы.

Таблица П1. *Список конкретных текущих операций администратора*

Отчет о проверке					
Администратор:	*Иванов*		Дата:	*23.08.2008*	
...					
Операция: проверка параметров производительности сервера					
Сервер	**Счетчик**		**Измеренное значение**		**Время измерения**
server1	% Processor Time		16%		09.30
	...		...		...
...					
Операция: проверка наличия обновлений программного обеспечения					
1. Проверить наличие обновлений для Windows 2003					
2. Проверить наличие обновления для Office 2007					
...					
...					

Предметный указатель

A

Access control list (ACL) 107
Account Lockout and Management Tools 191, 386
Active Directory (AD) 165, 454
ADSI Edit 456
Advanced Host Monitor 510
AutoMate 505
Automated Deployment Services (ADS) 539
Automated System Recovery (ASR) 335

B

BitLocker 377
◊ включение без TPM 378
◊ режим восстановления 380
Black DNS 250
Boot threshold 132
Bridge Protocol Data Units (BPDU) 78
Bridges 76
Browser Helper Object (BHO) 351

C

CDP 342
Certificate Revocation List (CRL) 470
Check Point 269
Common Information Model (CIM) 506
Continuos Data Protection 342
CWDM 60

D

Default gateway 104
Demilitarized zone (DMZ) 262
DetachOL 247
DHCP Relay Agent 131
Dynamic Host Configuration Protocol (DHCP) 101, 107
◊ отказоустойчивая конфигурация 134
Diaul-up-подключение 119
DiffServ 86
Diskview 519
Distinguished Names (DN) 171
Distributed File System (DFS) 186
Domain Name System (DNS) 135
◊ split 143
◊ имя 111
◊ зона 135
◊ отказоустойчивая конфигурация 149
◊ сервер 114

E

Extensible Authentication Protocol (EAP) 94
Easy Recovery 419, 432
Enroll agent 388
ERD Commander 390, 425, 428, 519
EtherChannel 80
eToken 390
Event log 433
EvenTrigger 435

Exploit 356
Extended Security Update Inventory Tool 366

F

Filemon 519
Firewall 264
Flexible Single Master Operation role (FSMO) 169
Fully qualified domain name (FQDN) 112

G

Gateway 104
GetDataBack 419, 432
GHost 534, 539
Global catalog (GC) 170
Group Policy Management 231
GVRP 73

H

Hardware Abstraction Layer (HAL) 535
Hidden Administrator 517
Hop-count threshold 132
Hot fix 356

I

Insight for Active Directory 456
InstallShield AdminStudio 531
InstallShield Tuner 531
Internet Authentication Service (IAS) 290
Internet Engineering Task Force (IETF) 99
Internet Information Server (IIS) 208
Internet Protocol security 486
Intrusion Detection Systems (IDS) 268
Intrusion Prevention Systems (IPS) 268
IP:
◊ адрес 100
  ▫ динамический 108
  ▫ статический 141
◊ маска адреса 102
◊ порт 109
◊ шлюз 104
IP Multicast Addressing 101
Ipsec Monitor 492
iptables 46
IPv6 99

K

KVM-коммутатор 514

L

Link Aggregation Control Protocol (LACP) 80
Late collision 416
LDAP Interchange Format (LDIF) 180
Lightweight Directory Access Protocol (LDAP) 164
Linux 23
LogParser 438
Lotus Notes 244

M

MAC-адрес 110
◊ программная смена 320
Management Information Base (MIB) 498
Microsoft Baseline Security Analyzer (MBSA) 358
Microsoft Exchange Server 244
Microsoft Operation Management Server 455
Microsoft System Management Server (SMS) 518
MLT 80
MonitorMagic 510
Multi Spanning Tree Protocol (MSTP) 79
Multi Router Traffic Grapher 415
Multimaster replication 340
MX-запись 233, 245

N

Nagios 510
NetBIOS-имя 111
Network Access Protection (NAP) 269
Network Address Translator (NAT) 261, 263
Network Monitor 450
Nobody 44

O

Observer 414
Offline NT Password Editor 390
Open Relay DataBase (ORDB) 250
Open Shortest Path First (OSPF) 74
Organization Unit (OU) 166

P

Performance Monitor 443
Power over Ethernet (PoE) 63
Port Knocking 54
Postfix 54
Pretty Good Privacy (PGP) 482
Provider 506
Proxy 117
Public Key Infrastructure (PKI) 463

Q

Quality of Service (Qos) 85, 489

R

RAID 332
Rainbow-таблица 383
Rapid Spanning Tree Protocol 78
Real-time Spam Black Lists (RBL) 250
Recovery consol 421
Relative Distinguished Names (RDN) 171
Remote Administrator 517
Remote Installation Service (RIS) 539
Remote Procedure Call (RPC) 238
Repackages 529
Resource records 139
Rights Management Services (RMS) 492
RIP 74
Routing 104
Routing and Remote Access Server (RRAS) 76, 131
RSTP 78
ruToken 390

S

Samba 37
Security Configuration Manager (SCM) 231, 319
Server Performance Advisor 452
Service pack 356
Sites 168
Spanning Tree Protocol 78
Squid 52
SSL 483
STP 78
Strict Priority Queuing (SPQ) 89
Stub-зона 138
SUSE Linux Openexchange Server 244
System Management Server (SMS) 365
System Policy Editor 216

T

The Bat! 242, 483
ToS 85
Traffic shaping 90

U

Update sequence numbers (USN) 340

V

Vi 31
Virtual local area network (VLAN) 70
Virtual Network Computing 517
Virtual Private Network (VPN) 285
◊ соединение 285
Virtual Routing Reduntance Protocol (VRRP) 81
VLAN 70
◊ tagged 72
◊ untagged 72
◊ маршрутизация 74
VMware:
◊ общая папка в Linux 37
Volume Shadow Copy (VSC) 331, 429
VWware Tools, настройка в Linux 36

W

Web-based Enterprise Management (WBEM) 506
Weighted Round Robin (WRR) 89
Wi-Fi Protected Access (WPA) 93
WinAntiSpam 252

Windows Fundamentals for Legacy PCs (WinFLP) 154
Windows Management Interface (WMI) 503, 506
◊ фильтр 219
Windows Script Host (WSH) 503
Windows Update Services (WUS) 363
WINS 126
Wired Equivalent Privacy (WEP) 93
Wireless Access Point (AP) 91
Wise InstallTailor 531
WMI Query Language (WQL) 507

А

Агент ретрансляции DHCP 131
Администрирование, удаленное 514
Адрес:
◊ динамический 102
◊ самостоятельное назначение 108
◊ электронный 233
Антивирусная защита 343
◊ почтовых сообщений 246
◊ служб 348
◊ установка 345
Антивирусная программа 344
Атрибут 178
Аудитор 163
Аутентификация 386
◊ протокол 386

Б

Безопасность:
◊ информации 311
◊ операционной системы 361
◊ паролей 381
◊ прикладного ПО 329
Безопасность клиента 95
Брандмауэр 109, 122, 246, 261, 264

В

Вентилятор 418
Виртуальная машина 393
Виртуальный компьютер 393
Вирус 236, 246
◊ лечение 347
◊ мистификация 347
◊ троянский конь 251, 265, 349
◊ червь 268, 348
Владелец объекта 199
Восстановление:
◊ данных:
▫ с жестких дисков 419
▫ с помощью утилит 431
◊ удаленных файлов 428
◊ центра сертификации 469

Г

Группа пользователей:
◊ DHCP Administrators 212
◊ DHCP Users 212
◊ HeplSevicesGroup 211
◊ Network Configuration Operators 212
◊ Print Operators 212
◊ Remote Desktop Users 211
◊ WINS Users 212
◊ Администраторы (Administrators) 210
◊ Все (Everyone) 212
◊ Гости (Guests) 211
◊ Операторы резервного копирования (Backup Operators) 210
◊ Опытные пользователи (Power Users) 210
◊ Пользователи (Users) 210
◊ специальная 212
◊ универсальная 194

Д

Делегирование прав 182
Домен 164
◊ Windows 155
◊ вложенный 166
◊ второго уровня 112
◊ имя 111
◊ первого уровня 112
◊ создание 172

Ж

Журнал 433

З

Запись ресурса 139
Заплатка 356
Запрос 507
Защита данных от копирования 372
Защищенный доступ в сеть 269

К

Кабели:
◊ оптические многомодовые 58
◊ оптические одномодовые 58
Канал связи:
◊ защищенный 483, 484
◊ незащищенный 483
Каталог 163
◊ схема 164
Клонирование рабочих станций 532
Ключ шифрования 460
◊ закрытый 461
◊ открытый 461
Команда:
◊ arp 111
◊ change logon 301
◊ chkdsk 419, 422
◊ csvde 176
◊ dcdiag 456, 457
◊ dcgpofix 222
◊ dcpromo 173
◊ diskperf 449
◊ dnsdiag 148
◊ dsadd 176
◊ dsget 176
◊ dsmod 176
◊ dsmov 176
◊ dsquery 176
◊ dsrm 176
◊ enable 422
◊ esentutil 469
◊ EVENTTRIGGERS 437
◊ fixboot 422
◊ fixmbr 422
◊ gpupdate 220
◊ ipconfig 108, 120
◊ ipsecpol 492
◊ ipv6 100
◊ ldifde 180
◊ listsvc 422
◊ logoff 302
◊ MSG 302
◊ MSTSC 301
◊ nbtstat 116
◊ netdom 155
◊ netsh 126, 134, 212, 490, 492
◊ netstat 109
◊ nslookup 142, 146, 234, 457
◊ ntdsutil 169
◊ pathping 124
◊ ping 111, 120, 511
◊ portqry 122
◊ query 302
◊ regsvr32 231
◊ reset session 302
◊ route 76, 105
◊ SHADOW 301
◊ telnet 236, 238
◊ tracert 105, 123, 485
◊ TSPROF 302
◊ TSSHUTDN 302
◊ winipcfg 108
Консоль восстановления 421
Контроллер домена 164
Концентратор 65
Корзина 429

Л

Лес 167

М

Маршрутизатор 73
Маршрутизация *См.* Протоколы автоматической маршрутизации
◊ статическая 74
Маска адреса 102
Межсетевой экран (МСЭ) 261
Мост 76

О

Обход перекрестной проверки 200
Ограничение полосы пропускания 90
Отказоустойчивая конфигурация:
◊ на основе протоколов второго уровня 78
◊ на основе протоколов третьего уровня 81
◊ топология сети 77
◊ шлюз по умолчанию 81
Очередь 89
Очистка кэша 137

П

Патч-корд 62
Переупаковка 529
Подразделение 166
Подсеть 102
Политика:
◊ IPSec 486
◊ безопасности 437
◊ групповая 160, 167, 215, 345, 349, 368, 372, 480
◊ обновлений 364
◊ ограниченное использование программ 224
◊ по установке программного обеспечения 222
◊ подключений 289
Пользователь, удаленный 284
Порог ожидания 132
Порт 109
◊ well-known 109
◊ сканирование 110
Почта:
◊ внутрикорпоративная 242
◊ Интернета 233
Провайдер 506
Программа:
◊ ADSI Edit 177
◊ Cain & Abel 384
◊ Poledit.exe 216
◊ Riprep.exe 541
◊ SelfCert.exe 473
◊ WBEMTest.exe 508
◊ агент 511
Производительность, программа 444
Прокладка силового кабеля 63
Прокси-сервер 117
Пространство имен 166
Протокол:
◊ Address Resolution Protocol (ARP) 111
◊ Hypertext Transfer Protocol (HTTP) 237
◊ Internet Control Message Protocol (ICMP) 99
◊ Internet Message Access Protocol (IMAP) 237
◊ Internet Protocol security (IPSec) 486
◊ NetBEUI 96, 151
◊ NetBIOS Frame Protocol (NBFP) 96
◊ NWLink IPX/SPX 96
◊ Open Shortest Path First (OSPF) 76
◊ Post Office Protocol 3 (POP3) 237
◊ Routing Information Protocol (RIP) 76
◊ Secure Sockets Layer (SSL) 483
◊ Simple Mail Transfer Protocol (SMTP) 236
◊ Simple Network Management Protocol (SNMP) 497
◊ Transmission Control Protocol (TCP) 96, 99
◊ User Datagram Protocol (UDP) 99
◊ автоматической маршрутизации 74
◊ сетевой 96
Протоколирование работы системы 433

Р

Разделение DNS 143
Разрешение:
◊ безопасности 197
◊ имен 116
◊ общего доступа 196

Резервное копирование 330
◊ данных:
  ▫ DNS-сервера 341
  ▫ реестра системы 342
  ▫ состояние системы 334
  ▫ типы операций 333
◊ центра сертификации 469
Ресурс, административный 157
Ресурсы о безопасности 313

С

Сайт 168
Сервер:
◊ BIND 172
◊ DHCP 127, 341
◊ DNS 341
◊ MDaemon 244
◊ Postfix 250
◊ RRAS 284
◊ VPN 287
◊ WINS 114, 126
◊ глобального каталога 170
◊ индивидуальная настройка 318
◊ лицензий 297
◊ почтовый 233
◊ прокси 267
◊ сценариев 503
◊ терминальный 295
◊ удаленного доступа и маршрутизации 284
◊ установка 141
Сервис-пак 356
Сертификат восстановления 374
Сеть:
◊ безопасность 93
◊ виртуальная 70
  ▫ частная 261, 285
◊ домашняя 151
◊ локальная 100
◊ одноранговая 153
Система:
◊ контролирующая содержание 268
◊ предотвращения атак 268
Служба:
◊ DHCP 142, 341
◊ IAS 290
◊ WINS 114
◊ автоматического обновления 363
◊ каталогов 142, 165, 454
◊ маршрутизации и удаленного доступа 76
◊ сертификации 469
◊ терминальная 295
◊ управления правами 492
Смарт-карта 290, 388
Сниффер 416, 497, 521
Сообщение:
◊ DHCPACK 133
◊ DHCPDISCOVER 132
◊ DHCPOFFER 132
◊ DHCPREQUEST 133
Спам 236, 242, 244, 248
Список отозванных сертификатов 470
Стек протоколов TCP/IP 99
Структурированные кабельные сети (СКС) 57
Сценарий 503
◊ входа в систему 159
Счетчик 444

Т

Таблица маршрутизации 104
Теневое копирование 331
Технология:
◊ SmartDefense 269
◊ трансляции адресов 263
Точка:
◊ восстановления 425
◊ доступа 90
Трансляция адресов 101
Туннель IPSec 487

У

Установка ПО 523
◊ административная 526
◊ ограничения 532
◊ тихая 526
Устройства хранения данных 332

Утилита:
◊ ALTools.exe 386
◊ dcpromo 172
◊ dhcpexim.exe 134
◊ LDP.exe 178
◊ ldp.exe 456
◊ LockDown 363
◊ netdiag 491
◊ ntbackup 173
◊ ntdsutil.exe 340, 456
◊ Scanreg.exe 342
◊ Scanregw.exe 342
◊ Setpwd.exe 340
◊ syslog 511
◊ sysprep 536
Учетная запись:
◊ HelpAssisstant 207
◊ IUSR_ имя_компьютера 208
◊ IWAM_имя_компьютера 208
◊ Local Service 209
◊ Network Service 209
◊ SUPPORT_номер 208
◊ Администратор (Administrator) 203, 207
◊ блокировка 385
◊ Гость (Guest) 207
◊ доменная 191
◊ локальная 191
◊ Система (Local System) 209

Ф

Файл:
◊ Adsutil.vbs 208
◊ Config.pol 216
◊ deploy.chm 424
◊ hosts 115
◊ lmhosts 115
◊ networks 115
◊ Ntconfig.pol 216
◊ rqs_setup.bat 293
◊ sceregvl.inf 231
◊ txtsetup.oem 424
◊ wpad.dat 119
◊ wuau.adm 364
◊ автономный 306
Файловая структура, распределенная 186
Формат CSV 176

Х

Хаб 65
Хост 111
Хэш 225, 258
◊ функция 477

Ц

Центр сертификации 463
◊ доверенный 464
◊ корневой 466
◊ подчиненный 466
Цифровой сертификат 459, 462
◊ индивидуальный 473
◊ отзыв 470
◊ получение 470

Ш

Шаблон 467
◊ compatws.inf 206
◊ административный 230
Шифрование 93
◊ диска 376
◊ документов 478
◊ с помощью двух ключей 461
◊ сообщения 258
◊ симметричное 460
Шлюз 104
◊ по умолчанию 73

Э

Электронная подпись 257, 477
◊ документа MS Office 478
◊ программного кода 479